



**This electronic thesis or dissertation has been
downloaded from Explore Bristol Research,
<http://research-information.bristol.ac.uk>**

Author:

Diepenbroek, Martine L M

Title:

Myths and Histories of the Spartan scytale

A comprehensive review and reassessment of the extant sources describing the cryptographic Spartan device known as the scytale to challenge the view promoted by modern historians of cryptography that denies the scytale its deserved status as a vehicle for secret communication in the ancient world

General rights

Access to the thesis is subject to the Creative Commons Attribution - NonCommercial-No Derivatives 4.0 International Public License. A copy of this may be found at <https://creativecommons.org/licenses/by-nc-nd/4.0/legalcode>. This license sets out your rights and the restrictions that apply to your access to the thesis so it is important you read this before proceeding.

Take down policy

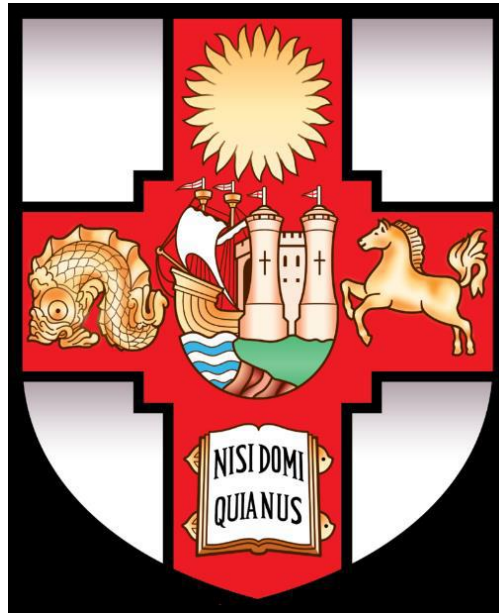
Some pages of this thesis may have been removed for copyright restrictions prior to having it been deposited in Explore Bristol Research. However, if you have discovered material within the thesis that you consider to be unlawful e.g. breaches of copyright (either yours or that of a third party) or any other law, including but not limited to those relating to patent, trademark, confidentiality, data protection, obscenity, defamation, libel, then please contact collections-metadata@bristol.ac.uk and include the following information in your message:

- Your contact details
- Bibliographic details for the item, including a URL
- An outline nature of the complaint

Your claim will be investigated and, where appropriate, the item in question will be removed from public view as soon as possible.

Myths and Histories of the Spartan *scytale*

A comprehensive review and reassessment of the extant sources describing the cryptographic Spartan device known as the *scytale* to challenge the view promoted by modern historians of cryptography that denies the *scytale* its deserved status as a vehicle for secret communication in the ancient world



Martine Loekie Mariska Diepenbroek

A dissertation submitted to the University of Bristol in accordance with the requirements for the award of the degree of Doctor of Philosophy in the Faculty of Arts

School of Humanities

Department of Classics and Ancient History

Date of submission: January 2020

Word count: 69.727 (excluding footnotes, references, and appendices)

Abstract

The current study is a comprehensive review and reassessment of the extant sources describing the cryptographic Spartan device known as the *scytale*, to challenge the view promoted by modern historians of cryptography that denies the *scytale* its deserved status as a vehicle for secret communication in the ancient world. Modern historians of cryptography see the *scytale* essentially as a simple ‘stick’ that would have served little practical use as a vehicle for secret communication. Yet, this study seeks to demonstrate that the cryptographic principles employed in the Spartan *scytale* show an encryption and coding system that is no less complex than some 20th century transposition ciphers. It will be shown that, contrary to the accepted point of view, *scytale* encryption is as complex and secure as other known ancient ciphers. The study will draw salient comparisons with a selection of modern transposition ciphers (and their historical predecessors), and offer a detailed review and comprehensive new analysis of the surviving classical sources that similarly reveal the potential of the *scytale* as an actual cryptographic tool in ancient Sparta in order to illustrate the relative sophistication of the Spartan *scytale* as a practical device for secret communication. This helps to establish the conceptual basis that the *scytale* would, in theory, have offered its ancient users a potentially secure method for secret communication – particularly over long distances. The study will be complemented by two appendices to the work in which an overview is given of all surviving ancient literary sources on cryptography and steganography as well as an overview of all extant medieval, Renaissance, and modern sources referring back to these classical sources, making this study the most comprehensive collection of Greek and Roman cryptographic and steganographic sources created so far – and thereby making an original and significant contribution to the current scholarship on the ancient history of cryptography.

Dedication and acknowledgements

My thanks and appreciation to my supervisors at the University of Bristol. First, many thanks to Professor Neville Morley, who supervised me during my first year, and who helped me to start the research, and to create a plan to make it possible to finish the research and dissertation within the duration of the course. Secondly, many thanks to Dr. Genevieve Liveley who became my supervisor at the end of the first year, and who helped me to get through my upgrade process. Your enthusiasm, support, and valuable comments have been a major help throughout the duration of the course. It certainly improved my writing and research skills in many ways. My thanks also go to Dr. Isabella Sandwell for acting as my second supervisor throughout the duration of the course, to Professor Patrick Finglass for proofreading various drafts of the dissertation and especially for his invaluable suggestions on Herodotus. I also thank Dr. Amy Coker for being my upgrade assessor at the end of the first year. Many thanks and appreciation also to Dr. John Black, an independent historian and researcher, for acting as my advisor and for proofreading parts of the dissertation throughout the time it took me to complete this research and to write the dissertation.

Finally, on a more personal note, I would like to thank everyone at the Bristol International Student Centre (BISC) with whom I worked during my Ph.D. years in Bristol next to my studies. Thank you all for being great friends who always supported me, and for often enquiring after my research and my personal well-being! Special thanks go to Eve Scott for proofreading the final draft and for being a great friend over the years. And most importantly, this dissertation is dedicated to my parents who have always been extremely supportive in countless ways, since I was a little girl. You have always believed that studying Classics and Ancient History was an excellent choice for me, and I agree. Therefore, this work

is for you. I am very grateful for the support and help that I have received from every one of you. Otherwise, I would not have been able to complete my research degree.

Author's declaration

I declare that the work in this dissertation was carried out in accordance with the requirements of the University's *Regulations and Code of Practice for Research Degree Programmes* and that it has not been submitted for any other academic award. Except where indicated by specific reference in the text, the work is the candidate's own work. Work done in collaboration with, or with the assistance of, others, is indicated as such. Any views expressed in the dissertation are those of the author.

The prologue of the thesis is based on a publication on part of the research: Diepenbroek, M. L. M. (2019). From Fire Signals to ADFGX. A case study in the Adaptation of Ancient Methods of Secret Communication. *KLEOS - The Amsterdam Bulletin of Ancient Studies and Archaeology*, 63-76. References to the publication are also made in chapters 3 and 5.

SIGNED:

DATE:

Table of Contents

Abstract.....	2
Dedication and acknowledgements.....	3
Author's declaration.....	5
Table of Contents.....	6
List of tables and illustrative material.....	9
Introduction.....	11
Working definitions: steganography and cryptography	15
Overview.....	17
Review of literature.....	19
Research methodology.....	32
Prologue	35
Chapter 1: Ancient steganography: Herodotus' contributions	51
1.1: Ancient cryptography and steganography	52
1.1.1: Bellerophon's tablet.....	54
1.2: Secret communication in Herodotus' <i>Histories</i>	60
1.2.1: Herodotus' views towards non-Greek secret communication	62
1.2.2: Harpagus to Cyrus: the message in the hare	66
1.2.3: Histiaeus to Aristagoras: the tattooed slave	68
1.2.4: Correspondence between Timoxenus and Artabazus: letters on arrows.....	70
1.2.5: Demaratus' letter to the Spartans: a message hidden under the wax of a wax tablet.....	71
1.2.6: Analysing instances of secret communication in Herodotus' work.....	73
Chapter 2: The <i>scytale</i>	79
2.1: Spartan society according to non-Spartan sources.....	80
2.2: Literacy in Spartan society.....	85
2.3: The <i>scytale</i> in non-Spartan sources.....	95
2.3.1: Archilochus of Paros (7 th century BCE)	95
2.3.2: Pindar (5 th century BCE).....	98
2.3.3: Aristophanes (late 5 th / early 4 th century BCE)	99
2.3.4: Nicophon (4 th century BCE)	103
2.3.5: Thucydides (2 nd half 5 th century BCE).....	104
2.3.6: Xenophon (late 5 th / early 4 th century BCE).....	106
2.3.7: Aristotle (4 th century BCE)	108
2.3.8: Theophrastus (4 th century BCE).....	109
2.3.9: Ephorus (4 th century BCE).....	110

2.3.10: Plutarch (late 1 st /early 2 nd century CE)	112
2.4: The <i>scytale</i> in practice	122
Chapter 3: Cryptography and steganography in Aeneas Tacticus' <i>How to Survive Under Siege</i>	135
3.1: Reasons for the absence of the <i>scytale</i> in <i>How to Survive Under Siege</i>	138
3.2: Aeneas Tacticus' methods for cryptography and steganography	141
3.2.1: Methods for steganography.....	144
3.2.2: Methods for cryptography.....	150
3.2.3: Combinations of cryptography and steganography	152
Chapter 4: Roman views towards the Spartan <i>scytale</i>	161
4.1: Secrecy and Roman letter writing.....	163
4.1.1: Ovid (43 BCE-17/18 CE) and Pliny the Elder (23-79 CE).....	163
4.1.2: Cicero (1 st century BCE).....	167
4.1.3: Ausonius (4 th century CE).....	170
4.1.4: The need for secrecy in Roman letter writing.....	171
4.2: The Caesar cipher (1 st century BCE)	173
4.3: Roman sources on the Spartan <i>scytale</i>	185
4.3.1: Cornelius Nepos (1 st century BCE).....	186
4.3.2: Aulus Gellius (2 nd century CE)	187
4.3.3: Ausonius (4 th century CE).....	189
4.4: Reasons for absence of the <i>scytale</i> in sources on Roman warfare.....	192
Chapter 5: The development of the principle of the transposition cipher system of the <i>scytale</i> in ciphers from the Renaissance to the Second World War	197
5.1: Alberti's cipher disk (1466-1467 CE).....	199
5.2: Bellaso's system (ca. 1553 CE)	204
5.3: Cipher machines (18 th -20 th century CE).....	205
5.4: The Enigma machine (Early to mid-20 th century)	208
5.5: 20 th century transposition and columnar transposition ciphers.....	210
5.6: 20 th century cylindrical and strip ciphers	215
Chapter 6: Summary and Conclusion	223
Bibliography	229
List of translations and commentaries	251
Appendix 1: Greco-Roman sources on cryptography and steganography	255
1: Aeneas Tacticus (<i>How to Survive under Siege</i> , ca. 360 BCE).....	255
2: Aeschylus (<i>Agamemnon</i> , 458 BCE)	261
3: Ammianus Marcellinus (<i>Roman History</i> , 4 th century CE).....	263
4: Aristophanes (late 5 th /early 4 th century BCE)	264
5: Athenaeus of Naucratis (<i>The Learned Banqueters</i> , early 3 rd century CE).....	265
6: Aulus Gellius (<i>Attic Nights</i> , ca. 177 CE)	266

7: Ausonius (<i>Epistles</i> , 4 th century CE)	269
8: Cassius Dio (<i>Roman History</i> , 3 rd century CE)	270
9: Cicero (<i>Letters to Atticus</i> , 68-44 BCE)	270
10: Cornelius Nepos (<i>The Book on the Great Generals of Foreign Nations</i> . Pausanias, 1 st century BCE)	271
11: Diodorus Siculus (<i>Library of History</i> , 1 st century BCE)	271
12: Frontinus (<i>Stratagems</i> , late 1 st century CE)	272
13: Herodian (<i>History of the Empire from the Death of Marcus</i> , late 2 nd /early 3 rd century CE)	273
14: Herodotus (<i>Histories</i> , ca. 440 BCE)	273
15: Homer (<i>Iliad</i> , 8 th /7 th century BCE)	276
16: Julius Africanus (<i>Kestoi</i> , late 2 nd /early 3 rd century CE)	277
17: Justin (<i>Epitome of the Philippic History of Pompeius Trogus</i> , 2 nd century CE)	279
18: Ovid (43 BCE-17/18 CE)	280
19: Philo of Byzantium (<i>Compendium of Mechanics</i> (Μεγανίκε συνταχίς)), 3 rd century BCE) ..	288
20: Pliny the Elder (<i>Natural History</i> , 77-79 CE)	288
21: Plutarch (late 1 st /early 2 nd century CE)	288
22: Polyaeus (<i>Stratagems of War</i> , second half 2nd century CE)	293
23: Polybius (<i>The Histories</i> , 2 nd century BCE)	294
24: Porphyry of Tyre (<i>Life of Pythagoras</i> , 3 rd century CE)	298
25: Suetonius (<i>Life of the Caesars: Lives of the Caesars</i> 1 and 2. <i>The Deified Julius</i> (1) and <i>The Deified Augustus</i> (2), 121 BCE)	298
26: Xenophon (<i>Hellenica</i> , late 5 th /early 4 th century BCE)	299
Appendix 2: Medieval, Renaissance, and modern sources on cryptography and steganography referring back to Greco-Roman sources	301
1: Leon Battista Alberti (<i>De Componendis Cifris</i> , 1466-1467)	301
2: Gerolamo Cardano (<i>De Subtilitate</i> , 1550)	304
3: Isidore of Seville, <i>The Etymologies</i> (5th/6th century CE)	305
4: Photius (<i>Lexicon</i> , 9 th century CE)	305
5: Procopius of Caesarea (<i>Secret History</i> , 6 th century CE)	306
6: Edgar Allan Poe (<i>A Few Words on Secret Writing</i> , 1841)	306
7: <i>Sylloge Tacticorum</i> (10 th -century Byzantine military manual)	307
8: Charles François Toussaint and René Prosper Tassin (<i>Nouveau traité de diplomatique</i> , 1750)	308

List of tables and illustrative material

Figure 1: Possible reconstruction of Aeneas Tacticus' water clock as described by Polybius (Polybius, <i>The Histories</i> , 10.43).	42
Figure 2: Five tablets with the letters of the ancient Greek alphabet used for fire signalling, as discussed by Polybius (<i>The Histories</i> , 10.45.6-12).....	43
Figure 3: Polybius square: a 5x5 square in which a modern 26-letter alphabet is placed.	45
Figure 4: ADFGX cipher: table filled with letters of a 26-letter modern alphabet in a random order agreed upon between sender and recipient.	47
Figure 5: ADFGX cipher table with rows and columns marked with the letters 'A', 'D', 'F', 'G', and 'X'.	47
Figure 6: <i>Scytale</i> with strip of writing material wrapped about it.	129
Figure 7: Text: 'Enemy attacks at Dawn Tomorrow', written on <i>scytale</i>	129
Figure 8: Strip of writing material with text unwrapped from <i>scytale</i>	130
Figure 9: Text 'Enemy Attacks at Dawn Tomorrow' written across complete strip of writing material.	131
Figure 10: Complete strip of writing material cut into pieces to show partial and complete letters.....	132
Figure 11: Two possible reconstructions of Aeneas Tacticus' wooden disk used instead of an astragalus. Left: reconstruction Diels; right: reconstruction Welskopf.	157
Figure 12: Encrypting text with a Caesar cipher with a right shift of three.....	182
Figure 13: Decrypting text with a Caesar Cipher with a right shift of three.	182
Figure 14: Caesar Cipher with a right shift of three applied to ancient Greek alphabet.....	183
Figure 15: Possible reconstruction of Alberti's cipher disk based on his discussion of the cipher disk in his work 'De componendis Cifris'.	201
Figure 16: An example of the Jefferson wheel cipher.	207
Figure 17: M-94 cipher Cylinder used by the United States Army from 1922/1923-1942...208	
Figure 18: Rotors on enigma machine. Enigma machine used by the German military intelligence services in the Second World War.	209
Figure 19: Example of modern substitution cipher. Step 1: plaintext message written in gid, text written from left to right and top to bottom.	211
Figure 20: Example of modern substitution cipher. Step 2: encryption text, text from columns written from left to right in rows.....	212

Figure 21: Example of modern substitution cipher. Step 3: encrypted text divided into groups of four letters.....	213
Figure 22: Example of modern substitution cipher. Ciphertext cut into strips.....	214
Figure 23: Model of strip cipher M-138-A, used by the American Intelligence Service from 1916-1960s, especially during the Second World War.	218

Introduction

It may well be that ciphers in classical antiquity were more advanced than the literature would lead us to expect [...].¹

The 21st century will see transposition regain its true importance.²

The aim of the current study is to reassess the extant evidence concerning the cryptographic Spartan device known as the *scytale* and to challenge the view promoted by modern historians of cryptography that see the *scytale* essentially as a simple ‘stick’ that would have served little practical use as a vehicle for secret communication in the ancient world – starting with my title ‘*Myths and histories of the Spartan scytale*’, as a response to Kelly’s article ‘*The myth of the scytale*’ (1998) in which Kelly argues against the practical use of the *scytale* in antiquity. Yet, on the contrary, in this study I will seek to demonstrate that the cryptographic principles employed in the *scytale* show an encryption and coding system that is no less complex than some 21st century transposition ciphers – and that the system was as complex and secure as other known ancient ciphers (including the substitution code used in the so-called Caesar cipher discussed in chapter 4). Indeed, I will draw salient comparisons with a selection of modern transposition ciphers (and their historical predecessors) in order to illustrate the relative sophistication of the Spartan *scytale* as a practical device for secret communication. This, I will argue, helps to establish the conceptual basis that the *scytale* would, theoretically, have offered its ancient users a secure method for such secret communication – particularly over long distances. I will complement this side of my argument with a detailed review and comprehensive new analysis of the surviving classical sources that similarly reveal the useful

¹ Leighton 1969, 153.

² Bauer 2000, 100.

role played by the *scytale* as an actual cryptographic tool in ancient Sparta (chapter 2). The main research question of this thesis is, therefore: *What can a comprehensive review and reassessment of the extant sources describing the cryptographic Spartan device known as the scytale do to challenge the view promoted by modern historians of cryptography that denies the scytale its deserved status as a vehicle for secret communication in the ancient world?* This first part of the thesis starts with a general introduction to the themes and aims of the study (*Introduction*). It is followed by a section on working definitions (*Working Definitions: Steganography and Cryptography*), and a section briefly summarising the contents of the study as a whole (*Overview*) to give a clear overview of the relevant contexts in which the Spartan *scytale* will be analysed and discussed here. Then the introduction will move on to a literature review in which I evaluate the reasons that many modern historians of cryptography put forward to show that the Spartan *scytale* was – according to them – not a real cryptographic device (*Review of literature*). As will be shown throughout the work, there exists a trend among modern historians of cryptography and secret communication to accept the biased accounts of ancient non-Spartan (particularly Athenian) sources from the 5th and 4th centuries BCE on the *scytale*, in which disparaging connections are made between the ‘non-Greek’ Spartans and their penchant for secrecy – but also their supposed illiteracy (see chapters 1 and 2). Finally, this introductory chapter concludes with a section on the applied research methodology at work in this thesis and the necessary limitations of the current study (*Research methodology*).

Cryptography and steganography form part of contemporary studies of mathematics and computer science – but also play significant roles in studies of military history, both ancient and modern. Scholars working in these fields have written numerous works in which ancient methods of secret communication – or cryptography and steganography – are referred to in passing as the early (which, in these studies, typically signifies ‘primitive’) precursors to modern cryptographic methods. However, none of these modern works focus in depth and

detail upon the ancient history of ancient cryptography and steganography, nor does any such study offer a comprehensive account of all the extant ancient sources in which secret communication is mentioned. Although David Kahn's extensive 1967 work *The Codebreakers* is an excellent source, this work still does not give a complete overview of all original Greco-Roman sources. What is more, there is a dominant trend amongst the current scholarship to underestimate the complexity and practical utility of the earliest forms of cryptography and steganography. One of the likely reasons for this, as I will argue, is because of the unfamiliarity of some historians of cryptography with the politically coloured biases towards the Spartans that we often encounter in classical Athenian sources, which can lead to the misinterpretation of original Greek and later Roman sources which draw upon them. A common assumption among historians of cryptography is, for example, that the Spartan *scytale* could not have had any practical value in official communication security because it was fundamentally a device that represented nothing more than a 'toy cipher'.³ As this thesis will argue, a better understanding of the full range of surviving ancient Greek and Roman sources where we find accounts and descriptions of secret communication – both cryptographic and steganographic – along with the recognition and better understanding of parallels between ancient and modern cryptography, will help us to re-evaluate the sophistication and security of the Spartan *scytale*. A re-evaluation of the relative complexity of some other familiar Greek and Roman methods for secret communication, will also allow us to better appreciate the strategic role that cryptographic devices such as the Spartan *scytale* could – and, this thesis maintains, would – have played in military contexts in the ancient world.

In the classical world, it seems, the first 'Greeks' to adopt the use of secret communication are the Spartans – already seen by Herodotus, and later by other Greeks (especially Athenians) as a people exhibiting strangely 'other' and 'non-Greek' practices – including a tyrannical

³ Gardner 1983, 56; Smart 2018, 3.

regime and the concomitant use of secret communication, more typical of ‘non-Greek’ oriental societies (Herodotus, *Histories*, 6.58-60; see chapters 1 and 2).⁴ Indeed, as we will see, it may well have been the case that the Spartans originally adopted and copied the use of secret communication from the Persians, as Herodotus implies in his *Histories* (chapter 1). It is particularly upon the Spartan innovations in cryptography – and, more especially, their use of the *scytale* – that this thesis will accordingly focus. The particular aim of the current study is to demonstrate that the Spartan *scytale* – the oldest known transposition cipher used for secret communication (chapter 2) – employed cryptographic principles no less complex than those employed by some Renaissance and later communication security devices – including some used up to the 20th century. This will be achieved by examining a full range of original Greek and Latin sources to offer a comprehensive survey and analysis of extant evidence for the use of the *scytale* among the Spartans. I will use my review of this evidence to argue against those historians of cryptography (such as Anderson, Kelly, and West) who maintain that the Spartan *scytale* was never actually used for secret communication.⁵ Analysing the operations and encryption principles of ancient ciphers in the light of more sophisticated modern transposition or permutation ciphers offers a useful point of departure for analysing and understanding the comparatively complex cryptographic principles which the *scytale* exploited. As Leighton already stated in 1969:

It may well be that ciphers in classical antiquity were more advanced than the literature would lead us to expect and that they influenced Renaissance cryptography.⁶

⁴ The earliest known evidence for the use of cryptography and steganography in antiquity comes from Mesopotamia and Egypt. See Porphyry of Tyre, *Life of Pythagoras*, 11-12; Caubet 2008, 421; Kasten 2001, 2; Nemet-Nejat 1998; Pieprzyk, Hardjono, and Seberry 2013, 6; Waldstein & Wisse 1995; Wisse 1979; 1980; 1981; 1982; 1983; 1989; 1990. See also Zapechnikov, Tolstoy et al. 2015, 146; see also § 1.1.

⁵ Anderson 1970, 68; Dimovski & Gligoroski 2003, 1; Ritter 1991, 3; Kelly 1985, 162; Kelly 1998, 245; West 1988, 42.

⁶ Leighton 1969, 153.

Yet, as this thesis will go on to demonstrate, it might be better to maintain that there are ‘shared principles’ between the *scytale* and later – including modern – transposition or permutation ciphers than arguing that *scytalae* have influenced either Renaissance or modern ciphers since there is no substantive evidence for this direct influence.

Working definitions: steganography and cryptography

Steganography describes the practice of concealing a message within another message, an image, or an object, without giving any outward sign that a secret message is hidden in it – in other words, steganography is ‘the practice of undetectably altering a work to embed a secret message’.⁷ The hidden message that is hereby created is called a steganogram.⁸ A steganogram or steganographic message need not be written in code or further encrypted in any way because its physical concealment provides (or is intended to provide) the necessary protection required to ensure the secure delivery of the message between sender and recipient.⁹ A steganogram is simply, therefore, any hidden or concealed message. Ancient sources in steganography often pre-date the ancient sources on cryptography – offering us some of our earliest examples of secret communication. As I will go on to show, certain societies and periods also seem to exhibit a preference for steganographic over cryptographic methods. A cryptogram is rather more complex than a steganogram. Cryptography is the practice of securing communication

⁷ Cox, Miller et al. 2008, 2. See also Johnson, Duric et al. 2001, 1; Kahn 1996a, 1; Schaathun 2012, 15; Singh 1999, 5; Whitiak 2003, 1. The term, which first appears in the title of Johannes Trithemius’ 1499 book *Steganographia*, comes from the ancient Greek words *στεγανός* (*steganos*), meaning ‘covered’ or ‘concealed’, and *γράφειν* (*graphein*), meaning ‘to write’.

⁸ Kartalopoulos 2009, 12.

⁹ Where an extra degree of security is desired, the steganogram or hidden message may also be encrypted or enciphered in which case it becomes a coded steganogram.

not by concealing but by enciphering a text.¹⁰ An original message called a plaintext is converted into a disguised (encrypted) message called a ciphertext.¹¹ This message, which is now encrypted, is called a cryptogram.¹² Cryptography, therefore, works with inputting and outputting either cipher or code. There are two fundamental types of ciphers found in the ancient world: transposition and substitution ciphers. In a transposition cipher the normal sequence of letters of a plaintext is rearranged. Hereby, alphabetic letters are not typically substituted by any other letters, numbers or symbols.¹³ In substitution ciphers, however, the letters of a plaintext message are substituted with other letters, characters, or symbols that are not necessarily found in the original text and the sequence of ciphertext letters that is used for such encryption and decryption is known as a ciphertext alphabet.¹⁴ The ‘Caesar’ cipher that will be discussed in chapter 4 can be regarded as a simple substitution technique for encryption whereby each letter of a plaintext is replaced by a letter that can be found a fixed number of positions down the ciphertext alphabet¹⁵ – for example a right shift of three in the case of Caesar’s supposed use of the cipher. The Spartan *scytale*, on the other hand, is an example of a transposition cipher.

¹⁰ Bauer 2013, xix; Hodges 1985, 146; Reba & Shier 2015, 479-480; Reinke 1962, 113; Seyfarth 1970, 181; Smith 1955, 16. The term ‘cryptography’ comes from the ancient Greek words *κρυπτός* (*kryptos*), meaning ‘hidden from’ or ‘secret’, and *γράφειν* (*graphein*) meaning ‘to write’. Like the term ‘steganography’, the term ‘cryptography’ is a neologism and was not used in antiquity, (pace Sheldon 2008, 19), first appearing in scholarship in Toussaint and Tassin’s 1750 work *Nouveau traité de diplomatie*, and in fiction in Edgar Allan Poe’s 1843 short story ‘The Gold Bug’.

¹¹ Mollin 2005, 1; Reba & Shier 2015, 480.

¹² Mollin 2005, 1.

¹³ Bauer 2007, 382; Reinke 1962, 113; Singh 1999, 5.

¹⁴ Bauer 2007, 382; Reinke 1962, 113; Singh 1999, 5.

¹⁵ Mollin 2005, 11; Stinson 1995, 4.

Overview

The thesis starts with a *Review of literature* in which the main arguments are discussed that are set out by historians of cryptography to support their hypothesis that the Spartan *scytale* could never have been used as a cryptographic device – the main argument being that (according to these scholars) *scytalae* were simple sticks that could never have had any useful practical value in cryptography. However, as will be argued, these scholars focus far too narrowly on the principal meaning of the word *scytale* being ‘stick’. This hypothesis, I suggest, might be based on biased non-Spartan views of the Spartans being illiterate, uneducated, foolish and secretive – as first put forward by Herodotus in his *Histories*, where he made connections between Sparta, oriental states, and secrecy (shown by four examples of secret communication discussed by the historian, and opposed to a free Greece, especially Athens, in which open public speech was ideologically valued and where secret communication was related to despotic and oriental values (chapter 1). By reassessing the extant ancient sources on the *scytale* as evidence it will be shown that *scytalae* could (and very likely would) have been used for a variety of purposes, ranging from record keeping to the writing and sending of secret messages (chapter 2). Even though all our surviving Greek and Roman sources are non-Spartan (or even anti-Spartan), it will be shown that ancient authors accepted that the Spartans used *scytalae* in the context of communication – especially over long distances – but that concrete evidence for its use as a device for encrypted *secret* communication remains inaccessible. The thesis will then turn to the work of the 4th-century BCE military author Aeneas Tacticus, since historians of cryptography presume that he would have discussed the *scytale* as a Spartan cryptograph if he had been familiar with the device because the author dedicated a chapter of his work *How to Survive Under Siege* to secret communication. Yet, as will be shown in chapter 3, Aeneas Tacticus had various reasons for not discussing the *scytale* – the main reason being that the

author seems to have had a greater interest in hidden messages (steganography) than in encrypted messages (cryptography), while the *scytale* messaging technique is a cryptographic method. In chapter 4 Roman cryptography and steganography will be discussed, with a focus on Roman responses to and appreciation of the *scytale*. The chapter will show that, although the Romans were familiar with the *scytale* as a cryptographic device, they, like Aeneas Tacticus, had various reasons not to use the *scytale* in their confidential communication. The main reason why the Romans did not use the device has to do with the differences between the ways in which the Greeks and Romans sent letters. As will be shown in chapter 4, in ancient Greece a messenger appears to have typically carried a message stick (*scytale*) as a badge of identification, authentication, and authority, and to have delivered his message orally, but in the Roman world the sending of sealed letters meant that messaging became more of a private affair between individuals. Hereby, letters were not delivered orally by a messenger with a message stick or *scytale*. The use of the *scytale*, for either normal or secret communication must, therefore, have appeared wholly alien and unpractical to the Romans. Instead of using the *scytale*, the Romans used the far less sophisticated Caesar cipher in their own secret communication (§ 4.2), a substitution cipher that shows some connection to the transposition system of the *scytale*. In chapter 5, I turn to the development of the principle of the transposition cipher system in later transposition ciphers (used from the Renaissance to the Second World War and beyond) to show the usefulness and functionality of the principle of the *scytale* as a transposition cipher. Hereby it will be shown that although modern cryptographic systems have now supplanted classical ciphers like the Spartan *scytale*, the basic concepts associated with the transposition cipher that most likely started with the Spartan use of the *scytale* are still widely used today.

Review of literature

The thesis follows aims to make a significant and original contribution to the existing scholarship on the topic of ancient cryptography by filling a gap in the current literature, and thereby casting new light upon some of the (incorrect) assumptions and (mis)readings of the ancient sources prevalent in the field, in addition to offering new knowledge of the Spartan *scytale* as a cryptographic device. Important general studies on the history of cryptography include Bauer's *Secret History: The Story of Cryptology* (2013) and *Unsolved! The History and Mystery of the World's Greatest Ciphers from Ancient Egypt to Online Secret Societies* (2017); D'Agapeyeff's *Codes and Ciphers – A History of Cryptography* (1939); Dooley's *A Brief History of Cryptology and Cryptographic Algorithms* (2013); Kahn's *The Codebreakers* (1967, 1974, and 1996a); Meyer's *The History of Cryptography* (2017); Singh's *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography* (1999); and Sheldon's *Espionage in the Ancient World: An Annotated Bibliography of Books and Articles in Western Languages* (2008). All of these works offer overviews of general cryptographic and steganographic history. Examples from antiquity up to the Middle Ages are briefly mentioned as an embryonic or primitive phase in the evolution of secret communication technologies, and are followed in each case by a more extensive discussion of secret communication from the early Renaissance until the modern day. In each case, the main focus of the studies is typically the use of cryptography in the First and Second World Wars – often presented as a technical apogee. This leads to the undervaluation and underappreciation of the relative sophistication of cryptographic devices described in ancient Greek and Roman sources (if these sources are discussed or referred to at all).¹⁶ Whitiak, for example, claims that original sources show us

¹⁶ Cox, Miller et al. 2008; D'Agapeyeff 1939; Kahn 1967; 1996a; 1996b; Mollin 2005; Sheldon 2008, 54-148; Singh 1999; Whitiak 2003, 1.

that Greek historians were familiar with a range of steganographic methods for secret communication.¹⁷ However, as we will see, ancient historians such as Herodotus actually only referred to reports of stories and events in which secret messages played a role. There is no evidence that Greek historians were personally or directly familiar with such ‘unGreek’ stratagems – and they even potentially invented these stories themselves (see e.g. Herodotus’ contributions discussed in § 1.2).

In cognate studies of relevance to the research set out in this thesis, Gardthausen’s most thorough survey of writing in ancient Greece – *Griechische Paleographie* (1911-1913) – has a short section on basic principles of cryptography and steganography (pp. 300-306; followed by a longer section on coding in arithmetic (pp. 307-319)), but Gardthausen does not engage directly with any of the extant sources on cryptography and steganography from antiquity. The work that comes closest to a complete overview of sources on classical cryptography is Sheldon’s *Espionage in the Ancient World: An Annotated Bibliography of Books and Articles in Western Languages* (2008). Although this study offers an excellent summary and catalogue of modern sources dealing with the history of cryptography, as the title implies, this book gives no substantive overview of *ancient* sources on the theme. Commentaries on and translations of ancient sources typically discuss passages on secret communication very briefly – if they are discussed at all (see the footnote for a list of all commentaries and translations in which the relevant passages can be found).¹⁸

¹⁷ Whitiak 2003, 1.

¹⁸ On the Spartan *scytale*: Brownson 1918, 221- 223, translation of Xenophon, *Hellenica*, 3.3.8; Brownson 1921, 47-49, translation of Xenophon, *Hellenica*, 5.2.34; Brownson 1921, 49-51, translation of Xenophon, *Hellenica*, 5.2.37; Douglas Olson 2009, 161, translation of Athenaeus of Naucratis, *The Learned Banqueters*, 451c-d; Henderson 2000, 191, translation of Aristophanes, *Birds*, 1280-1285; Henderson 2000, 403-405, translation of Aristophanes, *Lysistrata*, 985-991; Oldfather 1950, 425, translation of Diodorus Siculus, *Library of History*, 13.106.8-9; Perrin 1916, 113; translation of Plutarch, *Life of Alcibiades*, 38; Perrin 1916, 275-277; 285-289,

translation of Plutarch, *Life of Lysander*, 16-17.1; 19.4; 19.5-7; 20; Perrin 1917, 27; 41, translation of Plutarch, *Life of Agesilaus*, 10.5; 15.4-6; Perrin 1926, 130; Plutarch, *Life of Artaxerxes*, 6.2-5; Shackleton Bailey 1999, 155, translation of Cicero, *Letters to Atticus*, 10.10 (Letter 201); Shepherd 1793, 280; translation of Polyaeus, *Stratagems of War*, 7.19; Smith 1928, 219-221, translation of Thucydides, *History of the Peloponnesian War*, 1.131.1; Watson 1886, 326-327, translation of Cornelius Nepos, *Life of Pausanias*, 3.3-5; on the Caesar cipher and Caesar's secret letter to Quintus Cicero: Cary & Foster 1914, 419, translation of Cassius Dio, *Roman History*, 40.9.3; Rolfe 1914, 109, translation of Suetonius, *Lives of the Caesars* 1. *The Deified Julius*, 56.6; Rolfe 1914, 279, translation of Suetonius, *Lives of the Caesars* 2. *The Deified Augustus*, 88; Rolfe 1946, 235-237, translation of Aulus Gellius, *Attic Nights*, 17.9.2-4; 17.9.6-16; on Aeneas Tacticus' *How to Survive Under Siege*, Hunter & Handford 1927; Illinois Greek Club 1928; Whitehead 1990; on Julius Africanus' *Kestoi* (based on Aeneas Tacticus' *How to Survive Under Siege*, Illinois Greek Club 1928; on secret communication in Ovid's works: Goold 1977, 13; 45; translation of Ovid, *Heroides*, 1.31-36; 4.3-5; Goold 1977, 329-333; 395; 403; 497, translation of Ovid, *Amores*, 1.4.15-28; 1.4.55-58; 2.5.15-20; 2.7.5-6, 2.15.15-18; 3.11a.23-24; Mozley 1929, 15; 19; 41; 45-47; 53-55; 75; 83; 87; 93-95; 107-109; 153-155; 163, translation of Ovid, *Ars Amatoria*, 1.33-34; 1.91; 1.395-398; 1.455-458; 1.569-580; 1.597-600; 2.131-140; 2.243-246; 2.313-314; 2.394-396; 2.409-410; 2.427-428; 2.593-596; 2.639-640; 3.483-498; 3.619-630; on spying: Dewing 1935, 351-353, translation of Procopius, *Secret History*, 30.12-15; on a message hidden in a hare: Godley 1920, 161-163, translation of Herodotus, *Histories*, 1.123.4-1.124; Rolfe 1946, 237-239, translation of Aulus Gellius, *Attic Nights*, 17.9.18-27; Shepherd 1793, 22, translation of Polyaeus, *Stratagems of War*, 1.24; on a message tattooed on a slave's head: Godley 1922, 37-39, translation of Herodotus, *Histories*, 5.35.2-4; on Demaratus' wax tablet sent to the Spartans: Godley 1922, 557, translation of Herodotus, *Histories*, 7.239; Shepherd 1793, 80, translation of Polyaeus, *Stratagems of War*, 2.20; Watson 1853, Justin, *Epitome of the Philippic History of Pompeius Trogus*, 2.10.12-17; on a message written under the wax of a wax-tablet, probably sent by the Carthaginian general Hasdrubal: Rolfe 1946, 237, translation of Aulus Gellius, *Attic Nights*, 17.9.16-17; Watson 1853, translation of Justin, *Epitome of the Philippic History of Pompeius Trogus*, 21.6; on a cipher message hidden in the scabbard of a sword: Rolfe 1950, 445-447, translation of Ammianus Marcellinus, *History*, 18.6.17-19; on secret correspondence between Timoxenus and Artabazus: Godley 1925, 131, translation of Herodotus, *Histories*, 8.128.2-129.1; on Bellerophon's tablet: Murray & Wyatt 1999, 287 (Murray & Wyatt (I)), translation of Homer, *Iliad*, 6.168-169; on beacon signals: Murray & Wyatt 1999, 301-303 (Murray & Wyatt (II)), translation of Homer, *Iliad*, 18.203-214; Paton, Walbank et al. 2011, 233-237, translation of Polybius, *Histories*, 10.43-44; Sommerstein 2008, 35-39, translation of Aeschylus, *Agamemnon*, 281-316; on invisible ink: *Veterum Mathematicorum Opera*, 102, discussion of Philo of Byzantium, *Compendium of Mechanics*, D.80 (102.40-44; author's translation); Jones & Andrews 1980, 311, translation of Pliny, *Natural History*, 26.39 (62); on fire signalling used among the Carthaginians: Shepherd 1793, 246, translation of Polyaeus, *Stratagems of War*, 6.16.2; on Greek and Roman stratagems: Bennett & McElwain 1925, 247-249, translation of Frontinus, *Stratagems*, 13; on 'ancient codes' discussed by Ausonius in late antiquity (referring back to among other things the Spartan *scytale*): Evelyn-White 1921, 111-113, translation of Ausonius, *Epistles*, 28.10-31.

From the 18th century onward, historians have questioned the idea of the *scytale* being used as a cryptographic device by the Spartans. One of the earliest challenges to the view of the *scytale* as a cryptographic device we see in Toustain and Tassin's 1750 work *Nouveau traité de diplomatique, par deux religieux bénédictins de la Congrégation de s. Maur* [R.P. Tassin, C.F. Toustain et J.B. Baussonnet] – in which the two scholars describe the *scytale* not as a cryptographic device but as a steganographic device instead:

le *scytale* Laconique n'appartenoit pas plutôt la cryptographie, qu'à quelque espèce d'écriture commune [...]. [le *scytale*] étoit par conséquent un secret assez grossier de stéganographie [...] (Toustain and Tassin, *Nouveau traité de diplomatique*, 605)

the Laconian *scytale* did not fit [into any type of] cryptography. It was more a kind of common (in this case hidden) writing [...]. [The *scytale*] was, therefore, a rather crude example of steganography.

In steganography a complete message is hidden in or under another message or object, while in cryptography the letters of the message itself are encrypted or encoded in some fashion. Toustain and Tassin appear to assume that the widespread use of the *scytale* as a 'dispatch stick' (described in numerous ancient sources, and discussed further in chapter 2) allowed for hidden messages to be sent – either within the *scytale* rod or beneath the *scytale* message (the term *scytale* referring, as Plutarch explains, to both carrier and text in this context; Plutarch, *Life of Lysander*, 19.5-7; see § 2.3.10 and 2.4):

Sur une bande ou lanière fort étroite du cuir ou de parchemin, placée autour d'un cylindre ou d'un bâton, dont un correspondant avoit de semblable; les Lacédémoniens écroivoient les dépêches, concernant leur affaires d'Etat. Ces lanières confiées à des couriers ne formoient sens yeux des enemies, qui pouvoient les intercepter, parceque, pour les lire, il falloit avoir un cylindre de la même forme, qui celui, dont de s'étoit servi en les écrivant [...] (Toustain and Tassin, *Nouveau traité de diplomatique*, 605)

On a narrow band or strap of leather or parchment, placed around a cylinder or staff (a *scytale*), of which a correspondent (the receiving party) had a similar one, the Lacedaemonians would write messages concerning their affairs of state. These straps that were entrusted to couriers, were meaningless to the eyes of enemies if they would intercept them because, in order to read them, the enemy would have needed a cylinder of the same form as the one that had been used in writing them.[...].

Yet the *scytale* appears to have offered the ancient Spartans opportunities for both steganographic (hidden) and cryptographic (encoded) secret messaging. As this thesis will set out to demonstrate, in ancient Greece, messenger sticks (*scytalae*) were used for authentication purposes.¹⁹ A messenger could have wrapped a secret letter around a *scytale* and in that way could have hidden the message in plain sight – a classic steganographic method. The cryptographic element comes into play when the strip of writing material was unwrapped from the *scytale* and all the letters in the message changed position (and some letters would not even have remained intact if text was written over the edges of the strip (see § 2.3.10; 2.4; 4.3.2; Plutarch, *Life of Lysander*, 19.7; Aulus Gellius, *Attic Nights*, 17.9.12-13). What is more, although some ancient writers do discuss the *scytale* in the wider context of secret messaging (chapter 2), there is no evidence to suggest that the *scytale* was used primarily or solely for steganographic (that is, hidden) messages as Toustain and Tassin presume.

Responding to Toustain and Tassin's comments on the *scytale* as a steganographic rather than cryptographic device, a group of scholars who similarly challenge the idea of the *scytale* being used in antiquity as a Spartan cryptograph emerges in the last third of the 20th century, starting with Anderson (1970), and followed by (among others) Kelly (1985; 1998), Sheldon (1987), and West (1988). These scholars variously present five core arguments to substantiate their theory that *scytalae* were never used as devices for secret communication. The first and most important comes from Kelly and West, who both stress that the principal meaning of the word *σκυτάλη* (*scytale*) in ancient Greek is simply 'stick' or 'staff' and that such terminology is, in their view, incompatible with the *scytale* serving as a cryptographic device.²⁰ According to Kelly:

¹⁹ Anderson 1970, 68; West 1988, 43-45.

²⁰ Kelly 1985, 162; Kelly 1998, 245; West 1988, 42

though the etymology of the word *skytale* is indeterminate, its principle meaning in ancient Greek is ‘stick’ or ‘staff’.²¹

Kelly continues:

it is ironic that writers should ever have thought that the Spartans ever sent secret or codes messages. Throughout the long centuries of their history the Spartans were viewed by other Greeks as a conservative, tradition-bound people deeply interested in military matters, but not [...] in learning and culture.²²

But the fact that other Greeks saw the Spartans as conservative does not necessarily mean that the Spartans would never have used secret communication. On the contrary, as will be shown in chapter 2, Greeks after Herodotus saw the Spartans as a hostile ‘other’ people exhibiting ‘non-Greek’ practices – including the use of secret communication – much like (so the Greeks imagined) the oriental states which had historically threatened and repeatedly tried to invade Greece. After Kelly, West points out that:

a cryptographic interpretation of [the] *σκυτάλη* has come to look increasingly implausible with a more widespread appreciation of the fact that in [Archilochus’] days a written message was in itself a relative novelty; [...] it is clear that Archilochus lived in a society still essentially oral.²³

Although it is correct to suggest that the 7th-century BCE Greek poet Archilochus of Paros most likely still lived in an essentially oral society, as West argues, this again does not necessarily show that the Spartans could never have used the *scytale* for secret communication in the 5th and 4th centuries BCE (§ 2.2.1). Sheldon argues – without references or further explanation – that:

While [the *skytale*] may be [the first transpositional cryptograph], it cannot be dated to the classical period and is almost certainly not Spartan. There is even serious doubt that it was a method of cryptography.²⁴

²¹ Kelly 1998, 245.

²² Kelly 1998, 245.

²³ West 1988, 42.

²⁴ Sheldon 1986, 44.

On the contrary, it will be shown in chapter 2 of this thesis that most sources that discuss the *scytale* as a Spartan cryptograph can be dated to the 5th and 4th centuries BCE – the classical period – and that it is highly plausible that the *scytale* was used as a Spartan cryptographic device at this time.

The idea of the Greek word for *scytale* simply referring to a ‘stick’ and the understanding that its function, therefore, must be equally simplistic and primitive is also widespread in the secondary scholarship on this topic. The notion that its description in the ancient Greek as a ‘stick’ is incompatible with the *scytale* serving as a cryptographic device is reiterated by Strasser, who claims that Roman authors had promoted the erroneous assumption that ‘*such a ‘stick’ or ‘rod’ was used by the warlike Spartans*’.²⁵ We also find this view expressed more recently by Coles and Landrum, who stress the basic simplicity of the *scytale* – which they describe as:

simply a rod around which a piece of leather was wrapped.²⁶

Indeed, the predominant view of the *scytale* as merely a ‘toy cipher’ in modern histories of cryptography may owe something to popular studies of secret codes, including those aimed at children. D’Agapeyeff in his 1939 work *Codes and Ciphers – A History of Cryptography* – one of the first popular modern books on the history of cryptography – states that, to modern eyes, the *scytale*:

does not appear a very secret method of writing, as it can easily be deciphered by juggling together the edges of the roll; but doubtless at the time of Alcibiades and Lysander, when the invention was new, knowledge of reading was sufficiently rare to ensure the secrecy of the [...] method.²⁷

²⁵ Strasser 2007, 278.

²⁶ Coles & Landrum 2009, 7.

²⁷ D’Agapeyeff 1939, 15.

Significantly, D'Agapeyeff does not see the *scytale* as a complex cipher.²⁸ However, deciphering a *scytale* message was not as simple as D'Agapeyeff seems to presume. Alcibiades and Lysander – who received messages by *scytale* (§ 2.3.10) – would have received a strip with partial and broken letters (Aulus Gellius, *Attic Nights*, 17.9.12-13), and would not have been able to understand the intended messages properly without using a *scytale* of the exact same size and diameter themselves (§ 2.3.10-2.4). Following up on D'Agapeyeff, Gardner's 1983 study *Codes, Ciphers and Secret Writing* similarly suggests that a *scytale* device entailed nothing more than a message wrapped around a cylinder made of wood. In keeping with the intended readership of his work, perhaps, he even suggests the use of pencils or cardboard tubes as toy *scytalae* that children can use to send each other secret messages for fun – clearly representing the *scytale* as a 'toy' and as a rudimentary device that would not have been used in the context of any kind of serious communication security.²⁹ Sheldon in turn, in her 1986 article 'Tradecraft in Ancient Greece', also stresses the simplicity of ancient Greek cryptographic devices and messages – like the Spartan *scytale*, arguing that they:

would hardly deceive a modern military censor, but could well have fooled a simple-minded gatekeeper or a barbarian [...] in an age when reading and writing were uncommon.³⁰

Walker – writing in 2008 – follows a similar line and argues that in many ancient societies the use of encryption of the kind that the *scytale* could offer would have been unnecessary since the majority of people would have been illiterate anyway.³¹ Mollin (2005) adds that in our modern world the primary goal of cryptography is to secure confidential information – while this was simply not the case in antiquity. Instead, he argues, cryptography in antiquity was only

²⁸ D'Agapeyeff 1939, 15; 135.

²⁹ Gardner 1983, 56. Although Gardner mentions the *scytale* as being the earliest known code device used by the Spartans, he discusses it as nothing more than a 'toy' cipher.

³⁰ Sheldon 1986, 46-47.

³¹ Walker 2008, 150.

used to increase the level of mysticism in religious practices.³² While this theory is persuasive in the case of cryptographic coding described in the contexts of ancient Egypt and Mesopotamia (see § 1.1) – I will demonstrate that it is not the case for the Spartan *scytale*.

The idea of the *scytale* system as being far from sophisticated and its use for official correspondence being impractical and unnecessary can, more recently, also be found in Smart's 2018 study on modern cryptography, *CyBOK Cryptography Knowledge Area Issue*. Here Smart illustrates this enduring notion of the *scytale* as an example of simple 'toy' cryptography, by explicitly excluding these and other ancient cryptographic devices from his history, arguing that these historical ciphers are nothing more than 'toy examples' that have no place in serious modern studies of the evolving history of cryptography.³³ This prevalent and enduring idea of the *scytale* as merely a 'toy cipher', I argue, is misleading and appears to prompt too many historians of cryptography to assume that the *scytale* would have been far too simplistic to have been useful as a means of secret communication in real world military and tactical operations.

Although Kelly and West are broadly correct in stating that one of the principal meanings of the word *scytale* in classical Greek is 'stick' or 'staff', the Greek word actually has a wide range of meanings – from 'stick' or 'staff' to 'finger-bone' and 'serpent' and, as we will see, is also used in ancient sources to refer to Spartan identity tags, cash receipts, and – in Aristophanes – as a euphemism for a phallus.³⁴ Kelly, West, Strasser, et al., focus upon a narrow range of the available definitions. What is more, in themselves, the definitions of the *scytale* that these critics do accept ('stick' or 'staff') do not necessarily mean that *scytalae* could never have been used as devices for secret communication. On the contrary, the method for using the *scytale* as a device for encrypted messaging as described by Plutarch and Aulus

³² Mollin 2005, 5.

³³ Smart 2018, 3.

³⁴ See for these and all other meanings of the word '*scytale*': Liddell & Scott Greek-English Lexicon, entry *σκυτάλη*; Montanari, *The Brill Dictionary of Ancient Greek*, entry *σκυτάλις*.

Gellius (discussed in greater depth and detail in chapter 2; Plutarch, *Life of Lysander*, 19.7; Aulus Gellius, *Attic Nights*, 17.9.12-13) is so detailed and obviously useful, that it seems more than likely that *scytalae* were actively used for this purpose in contexts where secrecy of communication was important. This is not to say that *scytalae* were always or only used for the purpose of secret, encrypted communication. The extant evidence certainly does not support this theory. *Scytalae* were clearly used for many different purposes, including the sending of various types of messages. But when necessary, the ancient sources suggest that the *scytale* also offered its users an ingenious means of encryption. Based on a comprehensive survey of ancient sources making direct references to *scytalae*, this thesis will seek to demonstrate that the conclusions drawn by these critics are flawed, and will show that their arguments denying the cryptographic potential of the Spartan *scytale* can be challenged on the basis of this extant evidence.

Anderson, in his 1970 study of *Military Theory and Practice in the Age of Xenophon*, also argued that *scytalae* were used not as devices for secret communication, but instead as official messenger's equipment, as a sort of authentication device – the second argument put forward by historians of cryptography who do not see the *scytale* as a cryptographic device.³⁵ Although there is plenty of support for this type of usage as authentication in the extant evidence (chapter 2), this thesis will take issue with the idea that this was the sole purpose of the *scytale* and its only use in antiquity. Again, there is no evidence in the extant sources to suggest that the *scytale* was used primarily or solely for authentication purposes. Hiding an encrypted message in plain sight and conveying it through hostile territories using the vehicle of an official piece of equipment or authentication device is entirely plausible and there is nothing in Anderson's theory to preclude the use of the *scytale* for secret communication as part of its 'officially' recognised purpose. Indeed, such an officially sanctioned use would

³⁵ Anderson 1970, 68.

actually support and enhance the opportunities for secret messaging – enabling the *scytale* messenger and message to access protected areas.

Anderson's theory was later adapted by West who added to this argument that *scytalae* could also have been used by messengers as mnemonic aids: in West's theory slight incisions would have been made into the *scytalae*, which all had a different meaning, to help a messenger to remember the message that he was supposed to deliver.³⁶ In support of her hypothesis, West points out that notched sticks used

as mnemonic aids for conveying messages are attested from Australia, North America, West Africa, China, Mongolia, and South-East Asia; they were also used in ancient Scandinavia. The stick would be incised in the presence of the messenger, to whom the meaning of each notch was verbally emphasised.³⁷

Although no evidence shows that this particular mnemonic technique was actually adopted anywhere in ancient Greece, and none of the extant sources discuss the *scytale* in this context, West points out that when the word *scytale* was first attested in the Greek world by Archilochus of Paros in the 7th century BCE, this world was still essentially oral and a written message was a novelty (chapter 2, especially § 2.3.1).³⁸ Although this is a valid – indeed, important – observation, reminding us that literacy and written communications in the ancient world are complex issues, we should not take a single reference to the *scytale* in a fragmentary archaic Greek source and extend the speculative definition of that reference to discussions of *scytalae* in ancient sources from later centuries.³⁹ We should acknowledge that ancient forms of cryptography will have gone through various stages of evolution and although it is quite possible – even plausible – that *scytalae* were once used both for authentication purposes and

³⁶ West 1988, 43-45.

³⁷ West 1988, 45. See also Fischer 2004, 14; Glassner 2003, 1.

³⁸ West 1988, 42.

³⁹ A detailed engagement with ancient literacy and letter writing lies beyond the scope of this thesis, but see e.g. Adams 2003; Boring 1979; Cartledge 1978; Goody and Watt 1968; Harris 1989; Harvey 1966; Millender 2001; Street 1984; Woodard & Scott 2014.

as mnemonic aids, this does not mean they were only ever used for such purposes and again that they were never used as devices for secret communication. One of the central problems with the various theories proposed by Toustain and Tassin, Anderson, West, et al., then, is that they attempt to limit the use of the *scytale* to a specific activity or function. Sheldon, for example, argues that a *scytale* could either have been used for authentication – as Anderson suggests – or as a tool for secret communication, but not both, and she does not admit its use as a mnemonic aid.⁴⁰ Such arguments also tend to assume that the official purpose of the *scytale* was fixed and immutable, and that it could not be ‘hacked’ or put to use serving purposes other than those befitting its officially sanctioned role. These arguments also assume that such official uses were constant over time – that the use of the *scytale* in the 7th century BCE, for example, would have continued in more or less the same way into the 5th century BCE and beyond. This thesis will take issue with the idea that there was only one sole purpose of the *scytale* and only one primary use in antiquity, and demonstrate that the use of the *scytale* develops over time to include its use as a sophisticated means of cryptographic communication. It will show that a stick or staff can and could have been used for a variety of different purposes, including authentication, mnemonic aid, and also as a device for secret communication. Next to the two objections to the use of the *scytale* as a cryptograph raised by modern historians of cryptography – the fact that it was simply a stick or that it could only have been used as messenger authentication and/or as mnemonic aid – a third core objection to the use of the *scytale* as a cryptographic device concerns its absence from a major work on ancient secret communication. West points out that the 4th-century BCE Greek military strategist Aeneas Tacticus did not discuss the *scytale* in chapter 31 of his work *How to Survive Under Siege* which is dedicated to secret communication.⁴¹ This point was later adopted by Whitehead, and

⁴⁰ Sheldon 2008, 11-14.

⁴¹ West 1988, 42.

by Strasser in support of their corresponding view that the *scytale* was not used by the Spartans as a device for cryptographic communication: we might expect Aeneas Tacticus to have mentioned the *scytale* if it were a device with which he was familiar.⁴² However, there are a number of possible reasons to explain the fact that Aeneas Tacticus did not discuss the *scytale* as a Spartan cryptograph, as will be discussed in chapter 3 – the most important one being that Aeneas Tacticus seems to have had a much greater interest in hidden messages (steganography) than in encrypted messages (cryptography).

In correlation to this downplaying of the Spartan *scytale* as an effective cryptographic device useful in secret military communications, modern cryptographers instead typically posit the Roman Caesar cipher – a basic substitution cipher that will be discussed in chapter 4 – as being a (and sometimes *the*) crucial conceptual milestone in the development of ancient and modern cryptography.⁴³ Indeed, as opposed to the Spartan *scytale*, modern cryptographers have acknowledged the Caesar cipher as a working and useful system in ancient cryptography – albeit a simple one. Indeed, modern historians of cryptography often (erroneously) present Caesar’s professional use of the cipher as a historical fact – in marked contrast to their dismissive view of the Spartan *scytale* as little more than a toy.⁴⁴ Finally, there is also, perhaps, the magic of Caesar’s name to consider in explaining this discrepancy in treatment of Spartan versus Roman encryption techniques. As a famous Roman general, Caesar is better known (including by historians of cryptography) than the Spartans and their *scytalae* are. This potentially explains why historians of cryptography seem to take a greater and more serious interest in the Caesar cipher than in the *scytale*. However, this thesis argues instead that the

⁴² Strasser 2007, 278; Whitehead 1990, 183-184.

⁴³ Kahn 1967, 77; Mollin 2005, 11; Oriyano 2013, 56; Stewart, Chapple et al. 2012, 362; Stinson 1995, 4; Stinson 2002, 4.

⁴⁴ Churchhouse 2002, 13; Gardner 1983, 56; Mollin 2005, 5; Piper & Murphy 2002, 22; Sheldon 1986, 46-47; Walker 2008, 150.

Spartan *scytale* offers an example of ancient cryptography that is earlier and at least as sophisticated as the Caesar cipher. It argues that the principle of encryption which the ancient *scytale* employed can be seen as leading to, or perhaps inspiring, later transposition ciphers that would be constructed – and used in two World Wars. And, in turn, it argues that the common cryptographic principles upon which all transposition ciphers – from the Spartan *scytale* to twentieth and twenty-first century systems – operate, help us to see just how effective a device such as the *scytale* must have been when used for encrypted communications in antiquity.

Research methodology

The key research methodology employed in this thesis involves a comprehensive survey and analysis of the extant evidence for the use of ancient cryptographic techniques. To achieve this, a complete catalogue of the ancient classical sources in which secret communication devices, techniques, and messages are discussed is included as an appendix to this work (Appendix 1). A detailed examination of these sources was then conducted, and a typology established whereby different kinds of cryptographic and steganographic communications were evaluated and assessed in terms of their dependence upon encryption involving ciphers of varying degrees of complexity and/or concealment. Those secret communications involving encryption (rather than simple concealment) were then further evaluated to assess whether their operations depended upon a substitution or transposition cipher. This classification enabled the identification of a tradition of secret communication in the ancient world that centred upon the efficacy of transposition ciphers (such as the Spartan *scytale*) and variations thereon – and not, as received histories of cryptography have previously argued, solely upon the efficacy of substitution ciphers (such as the Caesar cipher). By establishing this principle and by comparing the techniques for cryptography using transposition keys in the ancient world and

in later periods (from the Renaissance to the Second World War), the reliability of the transposition cipher even in its more (perhaps, in its most) rudimentary form – the Spartan *scytale* – was able to be established. This, in turn, enabled an important re-evaluation to be attempted of the likely efficacy of the *scytale* as a means of secret communication in the ancient world.

Because of the character and scope of the study included in this thesis, there are necessarily certain limitations to this research and its approach: in particular, the work does not focus on *all* known extant forms of ancient cryptography and steganography from *all* ancient civilisations but instead focuses on those in the classical, Greco-Roman world, especially on the Spartan *scytale* – the earliest known transposition cipher. There is some – yet little – material evidence of cryptographic and steganographic practices from antiquity: e.g. abnormal hieroglyphics found on Egyptian tombs or encrypted texts found on clay tablets from Mesopotamia (§ 1.1). Another example of material evidence are inscribed curses, as is known from the invocation of St Sergios at a rock-cut church in Matiane (Görene) in Cappadocia. Here an inscription was found in red paint on a *tabula ansata* on the church wall that appears to have been written in a form of code based on a division of the Greek alphabet whereby letters appear to have been used to indicate numbers.⁴⁵ Then there is Greek papyrus from Egypt dating to the time of the emperor Hadrian. The writing on one side of the papyrus seems to be a spell in Greek, but written in a substitution cipher to prevent the text from being read by outsiders.⁴⁶ Finally, there is a Greek vase with a scene from the Iphigeneia in Tauris with a potential image of a *scytale*. Yet, very little is known about the vase. It was sold at a French auction in the 18th century and now probably lost.⁴⁷

⁴⁵ Donderer 1995, 97-122; *Supplementum Epigraphicum Graecum* 54, nr. 1524.

⁴⁶ Hunt 1929.

⁴⁷ Trendall 1952.

Because of the limited quantity of material evidence, especially from the classical period (the 5th and 4th centuries) on which the thesis focuses – the thesis limits itself to the discussion of literary examples. Yet, further research into the surviving material evidence would certainly help to add further nuance to the study – especially a study of the vase. An overview of all Greek and Roman sources on cryptography and steganography is provided in Appendix 1 – hereby providing the first complete list of original sources on these subjects. Appendix 2 gives an overview of all medieval and (early) modern sources from the 5th/6th century CE to the 19th century CE that refer back to the ancient sources provided in Appendix 1.

Prologue⁴⁸

By way of setting the scene for the analysis of ancient cryptographic and steganographic methods that follows, the thesis begins with a short prologue, in which the following research question is posed: *By establishing common links and principles of operation, and by comparing the techniques for encoded communications in the ancient world and in later periods (from the Renaissance to the Second World War), can we establish the theoretical reliability (or otherwise) of ancient methods and devices of secret communication – in this case Aeneas Tacticus' method for fire signalling?*

Communication security is of major importance to our modern world. Indeed, as Gerolymatos points out, the gathering of intelligence and spying on one's enemies is essential for any government in order to determine the political and military direction of the state especially in times of conflict when essential information on enemies can obviously facilitate the war effort.⁴⁹ Yet, since antiquity, individuals in all civilisations have been trying to encipher confidential correspondence – mainly in a military context, according to our available sources⁵⁰ – while others have been trying to decipher it. In fact, in the 6th century CE Procopius of Caesarea already described the practice of secretly communicating and spying as a very old one that went all the way back to the ancient Near Eastern kingdoms (Procopius of Caesarea, *Secret History*, 12-14). Sheldon accordingly argues that:

⁴⁸ This prologue is based on my previous publication: Diepenbroek, M. L. M. 'From Fire Signals to ADFGX: A case study in the adaptation of ancient methods of secret communication', published in *KLEOS - The Amsterdam Bulletin of Ancient Studies and Archaeology* (Issue 2; 2019, 63-76).

⁴⁹ Gerolymatos 1986, 13.

⁵⁰ Yet, evidence for the use of secret confidential information in other contexts in antiquity might be lost.

Ancient governments, like modern ones, realised that to keep their borders safe, to control their populations and to keep abreast of political developments abroad, they needed a means to collect the intelligence which enabled them to make informed decisions.⁵¹

And Van Tilborg claims that:

The protection of sensitive information against unauthorized access [...] has been of prime concern throughout the centuries.⁵²

Intelligence activities – including the use of cryptography and steganography for secret communication – therefore, have always been an integral part of statecraft.⁵³ Besides its use in a military context, other ancient uses of cryptography and steganography include its use in love letters (Ausonius, *Epistles*, 28.21-22; Ovid, *Ars Amatoria*, 3.627-630; Pliny the Elder, *Natural History*, 26.39 (62); see also chapter 4), its use to increase the level of mysticism in inscriptions, and its use in magical and religious texts (§ 1.1).⁵⁴ From accounts of Greek (and later Roman) history starting in the archaic period, for example, we know that both normal (that is, non-encrypted) and simple encoded or encrypted messages could be sent over long distances by means of fire signals – as discussed in a wide range of different sources: from philosophers including Aristotle (*On the Universe*, 398a), via tragedians like Aeschylus (*Agamemnon*, 7-9; 20-29; 278-350), and poets including Homer (*Iliad*, 4.275-276; 5.770-771; 18.203-214), Simonides (*Elegies*, 130; edition Sider) and Virgil (*Aeneid* 10.454; 11.526; *The Eclogues*, 8; 59); to orators like Cicero (*The Verrine Orations*, 2.5.35); and historians including Appian of Alexandria (*The Civil Wars*, 1.6.51; 12.66; *The Spanish Wars*, 6.15.90-92), Diodorus Siculus (*Library of History*, 18.57.5; 19.17.7), Flavius Josephus (*Books of the History of the Jewish*

⁵¹ Sheldon 2008, 8.

⁵² Van Tilborg 2006, xiii.

⁵³ Sheldon 2008, 8.

⁵⁴ Pieprzyk; Hardjono, and Seberry 2013, 6; Waldstein & Wisse 1995; Wisse 1979; 1980; 1981; 1982; 1983; 1989; 1990.

War against the Romans, 4.10.5), Herodotus (*Histories*, 6.115; 7.183; 9.3), Livy (*History of Rome*, 22.19.6), Polybius (*The Histories*, 1.19; 8.28-29; 10.42-47), Suetonius (*Life of the Caesars* 3. Tiberius, 65); Thucydides (*History of the Peloponnesian War*, 1.63; 2.94; 3.22; 3.80; 4.42. 4.111; 8.95; 8.102) and Xenophon (*Hellenica*, 1.1.1-4; 2.1.27; 5.1.27; 6.2.33-34). Sources discussing fire signalling as a method of long distance communication also appear in writings by scholars like Apollodorus (*Epitome*, 5.19) and Pliny (*Natural History*, 35.48 (14)), in geographers like Pausanias (*Description of Greece*, 2.25.2); and finally in military authors including Aeneas Tacticus (*How to Survive Under Siege*, 4.1; 4.5-6; 6.1-6-7; 7.1-7.4; 10.25-26), Caesar (*The Gallic War*, 2.33; 3.65-67; 7.3; *The Civil War*, 3.65), Julius Africanus (*Kestoi*, 77); Onasander (*The General*, 25.3); Maurice (*Strategikon*, 7.2.10), Polyaeus (*Stratagems of War*, 4.19.2; 6.16.2) and Vegetius (*The Military Institutions of the Romans*, 3.5.25).⁵⁵

In the earliest instances of fire signalling in ancient Greece, it was only possible to communicate using a prearranged coded message, which would have been highly inconvenient when the parties involved needed to communicate securely on urgent matters. The 4th-century BCE Greek military author Aeneas Tacticus accordingly invented a more sophisticated methodology for fire signalling, which could be used to send a series of messages, hereby communicating important (and, crucially, secret) dispatches during periods of war, including during periods of siege warfare (Aeneas Tacticus' particular field of interest and expertise). Since Aeneas Tacticus' method was evidently laborious and open to errors – as will be discussed later in this section – the Hellenistic Greek historian Polybius is supposed subsequently to have developed an improved method based on the same principles, either forming the basis for or based upon what modern cryptographers know now as the 'Polybius square' (Polybius, *The Histories*, 10.45.6-12) – a device that would be used by the German

⁵⁵ Hyde 1915. See also Aschoff 1984; Dvornik 1974, 31-33; Sheldon 1987, 135; Sheldon 2005, 127; Woolliscroft 2001, 159-171.

military intelligence services about two thousand years later as the basis for their ADFGX and ADFGVX ciphers, two important German cipher systems used late in the First World War.⁵⁶ This connection between Aeneas Tacticus' fire signalling and the German ciphers does not indicate a direct line of reception and technological development from an ancient mode of secret communication to a modern one; rather, it aptly signals one of the central research questions that this thesis sets out to investigate – as posed at the beginning of this prologue – whether we can establish the reliability (or otherwise) of ancient methods and devices of coded communication by establishing a common link and principle of operation between those ancient devices (for which we only have limited evidence as to their effectiveness) and later devices (for which we have better evidence and proofs of their effectiveness and reliability).

Very early on in Greek history, extant sources reveal that mountain tops were clearly used both as watch-towers and as signalling stations from which (secret and non secret) messages could be sent over long distances by lighting strategic fires. There are numerous extant references to this strategy for long distance communication from the ancient world, not only in works of history but of literature too as the list provided at the beginning of this section shows. Thus, to take just one salient example from this extensive list, Aeschylus – in his *Agamemnon* – described how Clytaemnestra received word from Agamemnon returning from Troy by means of beacons signals that were fast and efficiently sent from one station and one hilltop to the next:

τίς τόδ' ἐξίκοιτ' ἄν ἀγγέλων τάχος;

Ἥφαιστος Ἰδης λαμπρὸν ἐκπέμπων σέλας.

φρυκτὸς δὲ φρυκτὸν δεῦρ' ἀπ' ἀγγάρου πυρὸς

ἔπεμπεν (Aeschylus, *Agamemnon*, 281-283; for the complete passage see Appendix 1, page 261-263).

⁵⁶ Kahn 1996b, 76-77; 83; Mollin 2005, 9-10; Mollin 2006, 89.

what messenger could reach here with such speed? Hephaestus, sending a bright blaze on its way from Mount Ida; and then from that courier-fire beacon sent on beacon all the way here.

As it was only possible to send one prearranged message using this archaic system of fire signalling, communicating parties needing to communicate on urgent matters faced significant limitations – limitations that Polybius acknowledged in a passage on fire signalling among the ancient Greeks (10.43-46):

τὸν μὲν οὖν πρὸ τούτου χρόνον ἀπλῆς γινομένης τῆς πυρσεΐας κατὰ τὸ πλεῖστον αὐτὴν ἀνωφελῇ συνέβαινε γίνεσθαι τοῖς χρωμένοις. διὰ γὰρ συνθημάτων ὀρισμένων ἔδει τὴν χρεΐαν συντελεῖν: τῶν δὲ πραγμάτων ἀορίστων ὑπαρχόντων τὰ πλεῖστα διέφυγε τὴν τῶν πυρσῶν χρεΐαν, οἷον ἐπ’ αὐτῶν τῶν νῦν εἰρημένων. (Polybius, *The Histories*, 10.43-5-6; for the complete passage see Appendix 1, page 295).

Now in former times, as fire signals were simple beacons, they were for the most part of little use to those who used them. For the service had to be performed by signals previously determined upon, and as facts are indefinite, most of them defied communication by fire signals.

The 4th-century BCE Greek general and military author Aeneas Tacticus ('the Tactician') accordingly invented a method for fire signalling in which water clocks and torches were used, whereby a series of messages could be sent back and forth between distant mountain tops. Aeneas Tacticus' system is discussed in a now lost work on military preparations but its basic design has been handed down to us via Polybius (10.44). According to Polybius, Aeneas Tacticus discussed that communicating parties had to follow the following procedure:

γνοίη δ' ἂν τις ἐκ τούτων. φησὶ γὰρ δεῖν τοὺς μέλλοντας ἀλλήλοις διὰ τῶν πυρσῶν δηλοῦν τὸ κατεπεῖγον ἀγγεῖα κατασκευάσαι κεραμεῖα, κατὰ τε τὸ πλάτος καὶ κατὰ τὸ βάθος ἰσομεγέθη πρὸς ἀκρίβειαν: εἶναι δὲ μάλιστα τὸ μὲν βάθος τριῶν πηχῶν, τὸ δὲ πλάτος πήχεος. εἴτα παρασκευάσαι φελλοὺς βραχὺ κατὰ πλάτος ἐνδεεῖς τῶν στομάτων, ἐν δὲ τούτοις μέσοις ἐμπεπηγένηαι βακτηρίας διηρημένας εἰς ἴσα μέρη τριδᾶκτυλα, καθ' ἕκαστον δὲ μέρος εἶναι περιγραφὴν εὐσημον. ἐν ἐκάστῳ δὲ μέρει γεγράφθαι τὰ προφανέστατα καὶ καθολικώτατα τῶν ἐν τοῖς πολεμικοῖς συμβαινόντων, οἷον εὐθέως ἐν τῷ πρώτῳ. (Polybius, *The Histories*, 10.44.2-4; for the complete passage see Appendix 1, page 296-297).

He [Aeneas] says that those who are about to communicate urgent news to each other by fire-signal should procure two earthenware vessels of exactly the same width and depth, the depth being some three cubits and the width one. Then they should have corks made a little narrower than the mouths of the vessels and through the middle of each cork should pass a rod graduated in equal sections of three fingerbreadths, each clearly marked off from the next. In each section should be written the most evident and ordinary events that occur in war.

If all worked well, the receiving party could then read the intended message. What Polybius and (we infer from the attributions to Aeneas Tacticus here) what Aeneas Tacticus also described was a highly inventive mode of long distance communication. Indeed, it has been described as the earliest form of telegraphy used in the world and the most sophisticated system for secret communication discussed by Polybius (see Figure 1).⁵⁷ It is suggested by the 2nd-century CE author Polyaeus that the Carthaginians used a similar method successfully: Polyaeus implied that by sending (secret) fire signals the Carthaginians were always provided in the most rapid way with what they needed in their warfare (Polyaeus, *Stratagems of War*, 6.16.2; for the complete passage see Appendix 1, page 294).⁵⁸ Fairly recent experiments in archaeology – carried out by Woolliscroft in 2001 – have shown the Carthaginian system to be feasible (and potentially also Aeneas Tacticus' similar system, as reconstructed by Polybius).⁵⁹ Although at first, doubts were raised as to whether the ancient Greeks and Romans would have had the engineering skills to build and use such a system – and would have been able to make the system work quickly and reliably – Woolliscroft showed the potential and usefulness of these ancient fire signalling systems.

⁵⁷ D'Agapeyeff 1939, 16-17; Dvornik 1974, 42-43; Hunter & Handford 1927, 120; 122-123; Liddel 2018, 127-128; Oldfather 1928, 46-47; Rihll 2018, 281-287.

⁵⁸ See also Dvornik 1974, 56; Sheldon 1987, 28.

⁵⁹ Woolliscroft 2001; Sheldon 2005, 205.

However, there are two significant downsides to Aeneas Tacticus' method. First, it would have been extremely difficult to let the two water clocks run exactly parallel, as Woolliscroft argues:⁶⁰

It is in fact surprisingly difficult to make water run out of two vessels at exactly the same rate and even tiny inaccuracies become more serious the longer the clock is left running.⁶¹

Because of this it is hard to believe that Aeneas Tacticus' mechanism ever functioned well. What is more, with this method it remains the case that only pre-arranged messages could be transferred between the communicating parties – something that Polybius apparently acknowledged himself. He states that it would have been impossible to communicate by using Aeneas Tacticus' method, if anything unexpected occurred:

περὶ γὰρ ὧν ἀδύνατον γινῶναι πρὶν ἢ γενέσθαι, περὶ τούτων οὐδὲ συνθέσθαι πρὸ τοῦ δυνατόν. τὸ δὲ συνέχον ἐστὶ τοῦτο: πῶς γὰρ ἂν τις βουλευσάιτο περὶ τοῦ βοηθεῖν μὴ γινώσκων πόσοι πάρεισι τῶν πολεμίων ἢ ποῦ; (Polybius, *The Histories*, 10.45.1-5; for the complete passage see Appendix 1, page 297).

For it is impossible to agree beforehand about things of which one cannot be aware before they happen. And this is the vital matter; for how can anyone consider how to render assistance if he does not know how many of the enemy have arrived, or where?

⁶⁰ Hunter & Handford 1927, 120.

⁶¹ Woolliscroft 2001, 32, see already Hunter & Handford 1927, 120.

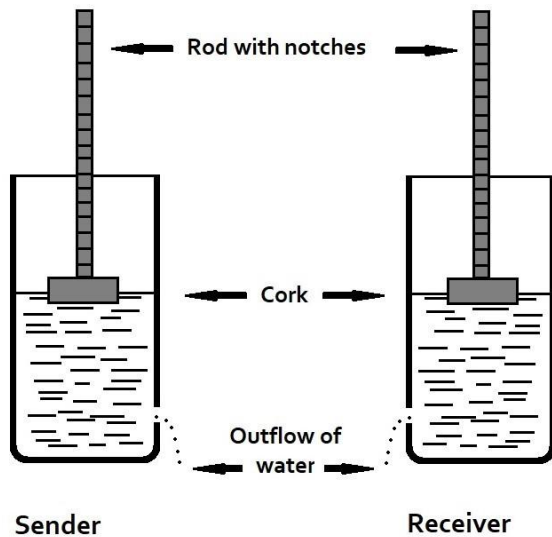


FIGURE 1: POSSIBLE RECONSTRUCTION OF AENEAS TACTICUS' WATER CLOCK AS DESCRIBED BY POLYBIUS (POLYBIUS, *THE HISTORIES*, 10.43).⁶²

Indeed, Polybius here showed that it would have been impossible to communicate by using Aeneas Tacticus' method if anything unexpected were to have occurred (*λοιπὸν ὁπότεν ἐκ τῶν καιρῶν ἀνυπονόητά τινα συμβαίνει, φανερόν ὥς οὐ δύναται δηλοῦσθαι κατὰ ταύτην τὴν ἐπίνοιαν [...] when circumstances produce some unexpected event, it is evident that it cannot be conveyed by this plan*; 10.45.3). Polybius, therefore, believed Aeneas Tacticus' method to have been a slight advance over the earliest and simplest beacon signals, yet the system was still quite rudimentary as he argues – since still only a series of prearranged messages could be sent. Therefore, Polybius decided to improve upon this method by developing it into a more sophisticated system of fire signalling: a system capable of dispatching with accuracy any kind of message (*Ὁ δὲ τελευταῖος <τρόπος>, <πάντη πάντως> μὲν ἐστὶν ὀρισμένος καὶ πᾶν τὸ κατεπεῖγον δυνάμενος ἀκριβῶς διασαφεῖν [...] The most recent method [...] is quite definite and*

⁶² Author's illustration based on Aschoff 1984, 47-48.

capable of dispatching with accuracy every kind of urgent message; Polybius, *The Histories*, 10.45.6). Thus, he described how:

τὸ τῶν στοιχείων πλῆθος ἐξῆς δεῖ λαμβάνοντας διελεῖν εἰς πέντε μέρη [...]. μετὰ δὲ ταῦτα πλατεῖα παρεσκευάσθαι πέντε τοὺς μέλλοντας ἀποδιδόναι τὴν πυρσεῖαν ἀλλήλοις ἑκατέρους καὶ γράψαι [...] καθαιρεθέντων δὲ τούτων λοιπὸν <ὁ> σημαίνων ἀρεῖ μὲν τοὺς πρώτους ἐκ τῶν εὐωνύμων, διασαφῶν τὸ πλατεῖον ποῖον δεήσει σκοπεῖν. [...] τοὺς δὲ δευτέρους ἐκ τῶν δεξιῶν κατὰ τὸν αὐτὸν λόγον, ποῖον δεήσει γράμμα τῶν ἐκ τοῦ πλατείου γράφειν αὖ τὸν ἀποδεχόμενον τὴν πυρσεῖαν (Polybius, *The Histories*, 10.45.6-12; for the complete passage see Appendix 1, page 297-298).

We take the alphabet and divide it into five parts [...]. Each of the two parties who are about to signal to each other must [take] five tablets and write one division of the alphabet on each tablet [...], the dispatcher of the message will now raise the first set of torches on the left side indicating which tablet is to be consulted [...]. Next he will raise the second set on the right on the same principle to indicate what letter of the tablet the receiver should write down.

1	2	3	4	5
α 1	ζ 1	λ 1	π 1	φ 1
β 2	η 2	μ 2	ρ 2	χ 2
γ 3	θ 3	ν 3	σ 3	ψ 3
δ 4	ι 4	ξ 4	τ 4	ω 4
ε 5	κ 5	ο 5	υ 5	

FIGURE 2: FIVE TABLETS WITH THE LETTERS OF THE ANCIENT GREEK ALPHABET USED FOR FIRE SIGNALLING, AS DISCUSSED BY POLYBIUS (*THE HISTORIES*, 10.45.6-12).⁶³

Like Aeneas Tacticus, Polybius still used torches, but replaced the water clocks with tablets on which the letters of the Greek alphabet were written (see Figure 2; Polybius, *The Histories*, 10.45.6-12. See for a parallel from Roman times: Julius Africanus, *Kestoi*, 77). One could then send messages letter by letter, whereby each fire signal represented one letter.

⁶³ Author's illustration based on Savard 1998-1999.

Although Polybius' method was still extremely laborious, it was clearly a significant improvement over Aeneas Tacticus' method, since in Polybius' system no water clocks were involved that had to run in parallel. What is more, when using Polybius' system every possible alphabetic message could be sent between communicating parties, instead of only a series of prearranged messages. This is made possible by the use of the alphabetic tablets that form the basis for what is known in modern cryptography as the 'Polybius square' – which some historians of cryptography (erroneously) believe to have been invented by Polybius himself.⁶⁴ A modern invention that is only based on Polybius' system, a basic Polybius square consists of five rows and five columns, which gives 25 cells. In these cells the 26 letters of a modern alphabet are written in their normal order from left to right, and top to bottom (see Figure 3). Hereby, following an idiosyncratically Latin rather than Greek tradition, the letters 'I' and 'J' are usually placed in the same block.⁶⁵ All rows and columns in the square have a number. In a basic square these are the numbers one to five for both rows and columns. Every letter in the square thus gets a coordinate. The letter 'A', for example, can be found in the first row on the first column, which gives the coordinate 1-1, written as '11'.⁶⁶ In this way, all the letters in the square have a coordinate between '11' (A) and '55' (Z). The coordinates can be compared to the place of the letters on Polybius' tablets (Polybius, *The Histories*, 10.45.6-12).

⁶⁴ Smith 1955, 16; Kahn, 1996, 76-77; 82-83; Mollin 2005, 9-10; Mollin 2006, 89.

⁶⁵ Kahn 1996b, 83; Lunde 2012, 78-79; Mollin 2006, 90.

⁶⁶ Mollin 2006, 90; Lunde 2012, 78-79; Kahn 1996b, 83.

	1	2	3	4	5
1	a	b	c	d	e
2	f	g	h	i/j	k
3	l	m	n	o	p
4	q	r	s	t	u
5	v	w	x	y	z

FIGURE 3: POLYBIUS SQUARE: A 5X5 SQUARE IN WHICH A MODERN 26-LETTER ALPHABET IS PLACED.⁶⁷

A modern message that is sent by use of a Polybius square, looks like a series of numbers. The message ‘*SEND MORE TROOPS BEFORE MIDNIGHT*’, for example, would appear as the following numerical sequence:

43 15 33 14 32 34 42 15 44 42 34 34 35 43 12 15 21 34 42 15 32 24 14 33 24 22 23 44

Since every coordinate contains two numbers – one for the row and one for the column – an encrypted text is created that is twice as long as the non-encrypted text.⁶⁸ To decipher the message, the recipient would take a Polybius square, look for the coordinates in the square, and check which letters correspond to these coordinates – using the square as the ‘key’ with which to decrypt the encoded text.

The Polybius square has reportedly been used for simple cryptographic communications in this way by the British army in the Boer War, and by both the British and German armies in the First and Second World Wars.⁶⁹ Yet, the basic cryptographic operating principles upon which the Polybius square and its encryptions works can also be seen to be

⁶⁷ Author’s illustration based on Salomon 2003, 29.

⁶⁸ Mollin 2005, 1; Reba & Shier 2015, 480.

⁶⁹ Kahn 1996, 83; Lunde 2012, 78-79; Mollin 2006, 90; Van Tilborg 2006, 32.

employed as the basis for other more sophisticated modern cryptographic methods. In the last year of the First World War, for example, the German military intelligence services used the Polybius square in their ADFGX and ADFGVX ciphers,⁷⁰ named after the only five, and later the only six, alphabetic letters that appeared in the ciphertext.⁷¹ Messages encrypted with the ciphers were transmitted by Morse code so these six letters were chosen to minimise transmission errors, since the letters sound very different from one another in Morse code. In March 1918 the first of the cipher systems was introduced: the ADFGX cipher. This cipher used a Polybius square of 5x5. This square was filled with 26 letters of the German alphabet in random order, and the ensuing distribution pattern – the encryption key – shared between sender and recipient (see Figure 4).⁷² This scrambling of letters is a key characteristic of the modern Polybius square (see Figures 4 and 5) – something that we cannot see in the ancient accounts of Polybius’ system in which the letters never seem to have changed position (Polybius, *The Histories*, 10.45.6-12).⁷³

⁷⁰ Van Tilborg 2006, 32.

⁷¹ Childs 1919, 13; Dooley 2016, 65; Klima & Sigmon 2012, 55; Mollin 2005, 1; Reba & Shier 2015, 480.

⁷² The German alphabet has 30 letters: 26 letters as in the English alphabet and 4 more signs (ä, ö, ü and ß). These signs were left out in the Polybius square.

⁷³ If Polybius had decided to change the order of letters on his tablets (regularly), the method would have become more secure. Yet, in this case communicating parties would have had to send each other the key information on the changed order of letters.

A	N	B	R	I
Q	E	U	H	P
K	L	O	W	D
S	C	V	X	Z
G	T	Y	F	M

*FIGURE 4: ADFGX CIPHER: TABLE FILLED WITH LETTERS OF A 26-LETTER MODERN ALPHABET IN A RANDOM ORDER AGREED UPON BETWEEN SENDER AND RECIPIENT.*⁷⁴

The rows and columns of the Polybius square used for the cipher were then labelled with the letters ‘A’, ‘D’, ‘F’, ‘G’, and ‘X’ to produce a coordinate for each of the plaintext letters: in this case, for example, the plaintext letter ‘Y’, was encrypted as ‘XF’ (see Figure 5).

	A	D	F	G	X
A	A	N	B	R	I
D	Q	E	U	H	P
F	K	L	O	W	D
G	S	C	V	X	Z
X	G	T	Y	F	M

*FIGURE 5: ADFGX CIPHER TABLE WITH ROWS AND COLUMNS MARKED WITH THE LETTERS ‘A’, ‘D’, ‘F’, ‘G’, AND ‘X’.*⁷⁵

In this way, a ciphertext was created that was twice as long as the plaintext, and that only contained the letters ‘A’, ‘D’, ‘F’, ‘G’, and ‘X’. The plaintext message ‘*Send weapons quickly*’, for example, would have been substituted into the following ciphertext:

⁷⁴ Author’s illustration.

⁷⁵ Author’s illustration.

GA DD AD FX FG DD AA DX FF AD GA DA DF AX GD FA FD XF

It is relevant to mention here that the aforementioned step is only the first stage of ADFGX encryption. This is followed by columnar transposition before sending the message (as will be discussed in § 5.5). The addition of this second element makes the system a combination of a transposition and a substitution cipher.⁷⁶ One of the characteristics of a Polybius square is that the ciphertext only consists of these five distinct characters. The ADFGX cipher has this distinctive Polybius square characteristic, potentially making it identifiable to enemy agents as a code based on Polybius square principles and, thus, giving those who intercepted it the opportunity to decode it easily. In June 1918, three months after the introduction of the first ADFGX cipher, the Germans added an extra row and column to the Polybius square that was used for the cipher to create a 6x6 grid to increase the level of sophistication of the method. Extending the grid meant that an extra letter was required to create the ciphertext. The letter V was chosen for this, since this letter sounds different from the five other letters in Morse code. The newly created cipher was accordingly (and perhaps unimaginatively) called the ADFGVX cipher.⁷⁷ It worked in the exact same way as its predecessor the ADFGX cipher. The ADFGX and ADFGVX ciphers were the most advanced cipher systems that the German military intelligence used during the First World War.⁷⁸ In fact, despite being based on the encryption principles of the Polybius square and sharing common features with an ancient Greek fire signalling device invented more than two thousand years earlier, they turned out (according to

⁷⁶ This is only the first stage of ADFGX encryption. It is followed by columnar transposition before sending the message. See for columnar transposition ciphers e.g.: Bauer 2013, 128-130; 136; 2017, 217-222; Bishop 2003, 19; Childs 1919, 13; Churchhouse 2003, 45-46; Collard 2004; Dooley 2016, 62-65; Kahn 1996, 535; 539; Stamp & Low 2007, see also § 5.5.

⁷⁷ Klima & Sigmon 2012, 55-57.

⁷⁸ Mollin 2000, 12.

military historians and modern cryptographers) to be amongst the toughest ciphers known in military secret communication until the end of the First World War.⁷⁹

At the beginning of this prologue the following research question was posed: *By establishing common links and principles of operation, and by comparing the techniques for encoded communications in the ancient world and in later periods (from the Renaissance to the Second World War), can we establish the theoretical reliability (or otherwise) of ancient methods and devices of secret communication – in this case Aeneas Tacticus' method for fire signalling?* The fact that we see the same basic technologies of secret communication exhibited in antiquity – in this case by Aeneas Tacticus – and again in the First World War – in the ADFGX and ADFGVX ciphers – helps us to appreciate more fully the practical efficiency and value of those basic technologies and techniques as they would have been used in antiquity. Indeed, the fact that ancient core principles of cryptography are still in use in some form in 20th (and even 21st; see chapter 5) century methods for secret communication demonstrates that these methods would and could have worked well in antiquity – an idea that this thesis now sets out to consider more fully in the controversial context of the ancient Spartan *scytale*.

⁷⁹ Churchhouse 2002, 45-46; Kahn 1996b, 334; 535-539; Mollin 2000, 12.

Chapter 1: Ancient steganography: Herodotus' contributions

Συμφέρονται δὲ [...] οὗτοι [...] τοῖσι Πέρσῃσι (Herodotus, *Histories*, 6.59)

The Lacedaemonians are like the Persians.

Συμφέρονται δὲ [...] Αἰγυπτίοισι Λακεδαιμόνιοι (Herodotus, *Histories*, 6.60)

Moreover, the Lacedaemonians are like the Egyptians [...].

In this chapter the first examples of (steganographic) secret communication known from the ancient world are introduced – and we examine how these examples potentially influenced later sources on (cryptographic) secret communication from the classical period – and, indeed, how they subsequently influenced later historians of cryptography, prompting them to downplay the sophistication and utility of the Spartan *scytale*. The chapter starts with a short section on the earliest evidence of cryptography in the ancient world, coming from Egypt and Mesopotamia to provide some context for ancient secret communication (§ 1.1). This is followed by a discussion of Homer's story of Bellerophon's tablet – often seen in modern cryptography as the first extant example of cryptography from the Greco-Roman world. Contrary to prevailing views in the contemporary scholarship, it will be argued that there is no clear evidence supporting the idea of a cryptographic message sent in this context. Instead, it will be argued that it is more plausible that in this story a straightforwardly private message was sent (§ 1.1.1). From Homer the thesis will move on to examine Herodotus, who (it is argued here) actually provided us with the earliest extant examples of secret (steganographic) communication in a Greco-Roman context (§ 1.2). The chapter focuses on the examples of secret communication as discussed by Herodotus and their application in emphatically 'foreign', 'other', and 'non-Greek' contexts. The research question that will be addressed in this chapter is, therefore: *What*

are the instances of secret communication in Herodotus' Histories and how are these coloured by Herodotus' view of the Spartans as non-Greek? This part of the thesis (§ 1.2) will start with an examination of Herodotus' views towards tyrannical regimes and oppression and the necessity – according to Herodotus – for the use of secret communications to help overthrow such regimes. Herodotus depicted the Spartans as familiar with ‘non-Greek’ oriental practices including the use of secret communication (§ 1.2.1). This will be followed by an analysis of the four key examples of steganography discussed in Herodotus' work (§ 1.2.2; 1.2.3; 1.2.4; 1.2.5). In the fourth example (§ 1.2.5) it will be shown that Herodotus made an explicit connection between the Spartans and the use of secret communication – the first reference of its kind to Spartan cryptography.

1.1: Ancient cryptography and steganography

Extant evidence for the ancient application of cryptography first appears in the second millennium BCE in Egypt and Mesopotamia.⁸⁰ In this context, ancient historians suggest that the replacing of standard writing signs for non-standard signs was most likely intended not to hide confidential information, but to impart some magical prestige and authority to a scribe's writing.⁸¹ No examples of cryptography and steganography are known from Egypt and Mesopotamia that appear to have had the primary purpose of sending confidential information

⁸⁰ Caubet 2008, 421; Kasten 2001, 2; Nemet-Nejat 1998; Pieprzyk, Hardjono, and Seberry 2013, 6; Waldstein & Wisse 1995; Wisse 1979; 1980; 1981; 1982; 1983; 1989; 1990. See also Porphyry of Tyre, *Life of Pythagoras*, 11-12. Zapechnikov, Tolstoy et al. – modern cryptographers – refer to cryptography being well-known from archaeological data since 2000 BCE without referring to any sources (Zapechnikov, Tolstoy et al. 2015, 146). They may be referring to the Egyptian and Mesopotamian uses of cryptography in this case.

⁸¹ Mollin 2005, 4-5; Pieprzyk, Hardjono, and Seberry 2013, 6; Waldstein & Wisse 1995; Wisse 1979; 1980; 1981; 1982; 1983; 1989; 1990.

from one person to another whereby the coding or encryption was designed such that a third party would not understand the message. Yet, it has been suggested that a cuneiform tablet from Seleucia on the Tigris (dating to 1500 BCE) containing an encrypted recipe for glass-making – is a clear attempt to protect confidential information.⁸² However, we should not wholly overlook the possibility that an ancient recipe for glass-making might have been valued by its ancient Mesopotamian makers as *magical* no less than *technical* or commercial and that its encryption may not necessarily have been designed to disguise confidential information but to appropriately acknowledge and record the supernatural, mystical, aspects of ancient glass-making.

Our earliest evidence shows that instead of the Mesopotamians or Egyptians, it was the Greeks, particularly the Spartans, followed by the Romans – who first seem to have used encrypted communications for securing confidential information. However, evidence for the use of cryptography and steganography used for the purpose of securing confidential information in other ancient civilisations may be lost.⁸³ Historians of cryptography are, therefore, arguably over-confident in claiming that the earliest civilisations certainly did not encrypt messages to secure confidential information (as, for example, Mollin suggests) or that it was unquestionably the Egyptians who first invented cryptography for the purpose of securing confidential information (as Kasten argues).⁸⁴

⁸² Caubet 2008, 421; Mollin 2005, 5.

⁸³ In fact, it has been suggested that all ancient civilisations have been familiar with the use of cryptographic and steganographic methods and devices to conceal their confidential correspondence. The only exception may have been ancient China because of the complexity of the Chinese ideogram alphabet (Pieprzyk; Hardjono and Seberry 2013, 6). Yet, Al-Kadi presumes that even in ancient China cryptography was used (Al-Kadi 1992, 103).

⁸⁴ Kasten 2001, 2; Mollin 2005, 5.

1.1.1: Bellerophon's tablet

It has been suggested by some historians of cryptography – for example by Mollin – that the first extant example of secret communication designed for strategic rather than magical effect from Greek and Roman sources can be found in Homer's *Iliad* (6.166-170; 178. See also Pliny, *Natural History*, 13.27; Plautus, *Bacchides*, 810–11; as well as surviving fragments of Euripides, *Bellerophon*; *Stheneboea*; Sophocles, *Iobates*).⁸⁵ According to Homer's *Iliad*, in an embedded story narrated by the grandson of the mythical hero Bellerophon, a secret message was once used to arrange a murder. In the first and apparently sole reference to letter writing in the *Iliad*, we hear how Bellerophon – being a guest friend at the court of king Proetus of Tiryns – is accused by the king's wife of attempting to rape her. Proetus, not wanting to kill a guest protected by the strict rules of *xenia*, could not punish Bellerophon himself. So he instead invented a pretext and sent Bellerophon to his father-in-law Iobates, king of Lycia, sending with him a tablet with 'baneful' or 'evil signs' (*σήματα λυγρὰ*; *semata lygra*); 6.168; see also *σῆμα κακόν*; *sema kakon*; 6.178) requesting Iobates to kill him. Thus,

ὧς φάτο, τὸν δὲ ἄνακτα χόλος λάβεν οἷον ἄκουσε:

κτεῖναι μὲν ῥ' ἄλέεινε, σεβάσσατο γὰρ τό γε θυμῷ,

πέμπε δέ μιν Λυκίην δέ, πόρεν δ' ὃ γε σήματα λυγρὰ

γράφας ἐν πίνακι πτυκτῷ θυμοφθόρα πολλά,

δειῖξαι δ' ἠνώγειν ᾧ πενθερῷ ὄφρ' ἀπόλοιτο. (Homer, *Iliad*, 6.166-170; for the complete passage see Appendix 1 page 276).

[Proetus] shunned killing him [Bellerophon], for his heart shrank from that; but he sent him to Lycia, and gave him fatal tokens, scratching in a folded tablet signs many and deadly, and ordered him to show these to his father-in-law [Iobates], so that he might perish.

⁸⁵ Mollin 2000, 4.

And a little further on Homer continues:

δὴ σῆμα κακὸν παρεδέξατο γαμβροῦ (Homer, *Iliad*, 6.178; for the complete passage see Appendix 1, page 276).

he [Iobates] had received from him [Bellerophon] the evil token from his son-in-law [Proetus].

Murray and Wyatt translate *σήματα λυγρά* (*semata lygra*) as ‘deadly signs’ – probably referring to the fact that Bellerophon was carrying his own death sentence – and *σῆμα κακὸν* (*sema kakon*) as ‘an evil token’ in line 6.178.⁸⁶ Already in antiquity there was discussion about what Homer precisely meant by his references to ‘baneful signs’ and ‘an evil token’ in this context. The earliest preserved comments on the passage are those of the 3rd century BCE grammarian Zenodotus of Ephesus and of the late 3rd/early 2nd-century BCE grammarian Aristarchus of Samothrace. According to Aristarchus, the words ‘baneful signs’ (*σήματα λυγρά*; *semata lygra*) did not mean alphabetic ‘letters’ as previous scholia critics – including Zenodotus – had assumed (*τῆς λέξεως γράμματα*; Aristarchus, *Scholia to the Iliad*, lines 6.168-169a; Edition Erbse). Aristarchus proposed instead that king Proetus drew or inscribed pictorial images on a tablet which his father-in-law Iobates would understand and act upon, but which Bellerophon (a stranger and non-family member) would not be able to comprehend (Aristarchus, *Scholia to the Iliad*, lines 6.166-170; *Venetus A*; Edition Erbse). Again, on line 6.178 Aristarchus similarly insists that Homer must have meant signs instead of letters. Aristarchus apparently believed that Proetus must have engraved signs, images or symbols instead of having written alphabetic letters (*σημεῖα λέγει, οὐ γράμματα [...] he [Homer] says signs, not letters*).⁸⁷ As Schmidt points out, Aristarchus may well have been inspired to suggest the idea of signs being used in this context (instead of alphabetic letters)

⁸⁶ Murray & Wyatt 1999, 287.

⁸⁷ Derived from Schmidt 1920, 58.

after seeing ancient Egyptian hieroglyphics.⁸⁸ Yet, although Aristarchus may well have believed that the mythical Greek Proetus wrote in a sort of proto-Greek, quasi-Egyptian, pictogram-based script, resembling ancient hieroglyphics, it remains unclear whether Aristarchus understood Proetus to have used these pictogram ‘signs’ as a way of encoding his message to Iobates – or whether this was assumed to be the usual means of written communication between members of this (mythical) ancient Greek family.⁸⁹ It remains unclear for many modern scholars what exactly was supposed to have been written on Bellerophon’s tablet and whether or not some kind of code was employed in this communication. Powell, for example, speaks of ‘inscribed signs’ that were very simple marks known to be made on folded tablets from Mesopotamia and Anatolia, and he argues that Homer’s words *σήματα λυγρά* could certainly not have referred to any known script.⁹⁰ Bellamy instead presumes that the signs were straightforwardly alphabetic signs instructing Iobates to act,⁹¹ while Bowra sees the text on Bellerophon’s tablet as:

something mysterious and rare, an echo from a far Mycenaean past, not fully understood [and] a dark element in a remote legend.⁹²

Chadwick sees the text on the tablet as ‘exotic’, ‘magical’, and a ‘reference to a dim past’, and Van Oldenburg Ermke speaks of ‘deadly and ominous signs’.⁹³ The example is not as clear-cut as some historians of cryptography assume. There is nothing in Homer’s text to exclude the possibility that the tablet in question contained a written message using conventional symbols or letters. In fact, various scholars since the 19th century suggested that

⁸⁸ Schmidt 1920, 58.

⁸⁹ On the origins of the Greek alphabet see e.g. Garfield 2013; Keightley 1856; Keightley 1859; Maas 2012; Mure 1854; Powell 1997; Richardson 1984 (I); Richardson 1984 (II); Schmidt 1920; Schwab 2011; Steiner 1994.

⁹⁰ Powell 1997, 27-28.

⁹¹ Bellamy 1989, 289-307, especially 290-294.

⁹² Bowra 1972, 12.

⁹³ Chadwick 1976, 182; Van Oldenburg Ermke 1959, 103. See also Kirk 1962, 165, 184; Willock 1978, 245.

the words *ἐν πίνακι πτυκτῷ* (*en pinaki ptykto*; 6.169) in Homer's text should be translated as 'sealed tablet'⁹⁴ – since seals and sealed tablets were common in correspondence in the Near East since the 4th millennium BCE. The words being translated as 'folded' or 'folding tablet' indicates a diptych like the one found in the Bronze Age shipwreck at Uluburun and in use also in Roman times.⁹⁵ This idea of a folded tablet further supports the argument that the message was not written in any form of code.⁹⁶ The fact that the letter was folded would have granted Proetus the necessary protection and security he needed to ensure that his letter to Iobates remained unread by its intermediary, Bellerophon. Thus, the references to 'baneful' or 'evil signs' in Homer (*σήματα λυγρά*; 6.168; and *σῆμα κακὸν*; 6.178) could simply refer to the fact that Bellerophon was carrying his own death warrant within the message he unwittingly carried between Proetus and Iobates. Indeed, we can already see this idea in antiquity: Apollodorus, for example, – writing in the 1st or 2nd century CE – claimed that Proetus sent Bellerophon to Iobates with a simple letter providing clear written instructions that he was to kill Bellerophon:

Προῖτος [...] ἔδωκεν ἐπιστολὰς αὐτῷ πρὸς Ἰοβάτην κομίσαι, ἐν αἷς ἐνεγέγραπτο Βελλεροφόντην ἀποκτεῖναι (Apollodorus, *The Library*, 2.31)

Proetus [...] gave him [Bellerophon] a letter to take to Iobates, in which it was written that he [Iobates] was to kill Bellerophon.

However, the example of Bellerophon's letter as a potential candidate for the first literary reference to a (fictional) coded letter is complicated further when we consider that the story of

⁹⁴ See e.g. Garfield 2013, 44; Keightley 1856, 126; Keightley 1859, 126; Maas 2012, 216; Mure 1854, 485; Powell 1997, 27; Richardson 1984 (I), 72-74; Richardson 1984 (II), 72-74; Schwab 2011, 202; Steiner 1994, 16.

⁹⁵ See e.g. Garfield 2013, 44; Keightley 1856, 126; Keightley 1859, 126; Maas 2012, 216; Mure 1854, 485; Richardson 1984 (I), 72-74; Richardson 1984 (II), 72-74; Schmidt 1920, 65-66; Schwab 2011, 202; Steiner 1994, 16; for ancient diptychs see e.g. Bowman 1975, 237-252; Pulak 1998, 188-224.

⁹⁶ Spar & Jursa 2014, lxxxix.

this secret communication is located in a period of ancient history in which Greek literacy is only just emerging. Alphabetic literacy had arrived in Greece in the 8th century BCE, around the time that Homer composed his work.⁹⁷ In fact, Bellerophon's tablet is the only indication in the *Iliad* in which Homer indicates any explicit knowledge of the art of writing.⁹⁸ This leads Bellamy to conclude that the *σήματα* (*semata*) inscribed on Bellerophon's letter offer evidence of Greek alphabetic writing systems already being in use in the 8th century BCE in archaic Greece.⁹⁹ Although this may be this case, in general in ancient Greece, the habit of writing and the specific practice of letter-writing as a mode of communication appears to have remained restricted down to the end of the 5th century BCE (since the majority of written sources can be dated to this period)¹⁰⁰ – after which basic literacy and exchange of letters seems to have become fairly widespread in the Greek world, although the topic of ancient literacy remains a highly contested topic.¹⁰¹ It is debateable whether the custom of communicating via written missive or letter (encrypted or otherwise) was a concept with which Homer and his archaic Greece audience would have been familiar. Ceccarelli is slightly more cautious than Bellamy, therefore, when suggesting that Homer referred to some kind of alphabetic writing given the

⁹⁷ Swiggers, 1996; Trapp 2003, 6.

⁹⁸ Ceccarelli 2013, 56, 59; Chadwick 1976, 182; Rosenmeyer 2001, 39. One more passage in the *Iliad* might be a reference to writing (Homer, *Iliad*, 7.175–89). In this passage the heroes during the Trojan war mark tokens (*κλήρον ἐσημήναντο καστός*) and put them in a helmet. A herald (*κῆρυξ*) then goes around showing the lot that came out, until Ajax recognizes it (*γνῶ δὲ κλήρον σῆμα ἰδὼν*) and rejoices. As Ceccarelli points out, the marks on the tokens were simply signs, recognisable by the person who made them, but devoid of any meaning for the others. They functioned as symbolic signs, as a language, but cannot be confused with writing (Ceccarelli 2013, 59–60). See also Heubeck 1979, 127–128; and Steiner 1994, 10–16, who stresses the importance of differentiating between messages based on linguistic communication and *semata* (signs), as well as Bowie (2013).

⁹⁹ Bellamy 1989 (I), 289–307, especially 290–294. See also Bellamy 1989 (II); Havelock 1982, 10; Steiner 1994, 4.

¹⁰⁰ Novokhatko 2015, 11.

¹⁰¹ Ceccarelli 2013, 185; Trapp 2003, 6. For the role of writing in Herodotus' time, see O'Toole 1991–1992, 148–160. For literary and letter writing in ancient Greece, see Adams 2003; Boring 1979; Cartledge 1978; Goody and Watt 1968; Harris 1989; Harvey 1966; Millender 2001; Powell 1997; Street 1984.

unequivocal reference to these two kings communicating through the medium of a folded tablet but that we can extrapolate little more from this story.¹⁰² Indeed, Steiner and Rosenmeyer focus judiciously upon the importance of the tablet as a token of guest friendship instead of the murderous message that was sent between Proetus and Iobates, and differentiate between the singular and plural forms of the word *σήμα* (*sema*) in this context.¹⁰³ According to these two scholars, the tablet (or letter) itself was a *σήμα* (*sema*) or ‘token’ (singular) of guest friendship – known from both literary (Euripides, *Medea*, 613; Pollux, *Onomasticon* 9.71)¹⁰⁴ and archaeological records (e.g. terracotta plaques carrying painted names potentially designed for guest friends as identification or leaden plates carrying inscriptions referring to an agreement made between individuals).¹⁰⁵ The symbols inscribed on the tablet or letter were therefore the *σηματα* or ‘linguistic signs’ conveying Proteus’ message to his father-in-law.¹⁰⁶ This is something we can potentially also see in Murray and Wyatt’s translation of the words *σήμα κακόν* as ‘evil token’ in their rendering of line 6.178 of the *Iliad*: ‘evil’ since the tablet contained an instruction to murder Bellerophon, and a ‘token’ since the tablet or letter was a token sent from Proetus to Iobates.¹⁰⁷ Since we do not and can not know anything concrete in this case about the character of the text or symbols – these ‘linguistic signs’ – inscribed on the token or tablet, it cannot be said with any confidence that the case of Bellerophon’s letter as described in Homer’s *Iliad* is an example of ancient code-writing or cryptography. It can only be said with certainty that Homer’s narrative offers us an account of a private message sent from Proetus to Iobates in a sealed tablet or letter – most likely in a non-Greek language because of the oriental

¹⁰² Ceccarelli 2013, 60. See also Burkert 1983, 51-56.

¹⁰³ Rosenmeyer 2001, 40-42; Steiner 1994, 15.

¹⁰⁴ Müri 1976, 5.

¹⁰⁵ Gauthier 1972, 68 (note 18); Herman 1987, 62 (Figure 8a-d and note); Ladner 1979, 223-225; Steiner 1994, 31.

¹⁰⁶ Rosenmeyer 2001, 40-42; Steiner 1994, 15.

¹⁰⁷ Murray & Wyatt 1999, 287.

context of the passage and background of Proetus and Iobates – serving ostensibly as a token of guest friendship but also communicating a more sinister (‘baneful’ or ‘evil’) message – Bellerophon’s death sentence.

1.2: Secret communication in Herodotus’ *Histories*

The earliest Greco-Roman source which provides us with unambiguous examples of secret communication is not Homer’s *Iliad*, then, but Herodotus’ *Histories*. We can find at least 61 instances of trickery and deceit in Herodotus’ work.¹⁰⁸ To be more precise: all but three instances of written communication in Herodotus’ work – fourteen letters (1.123; 1.125; 1.187; 3.40; 3.42; 3.122; 3.128 (2x); 5.14; 5.35; 6.4; 7.239; 8.22; 8.128) and two other written messages (5.28 (a message written on a slave’s head); and 8.22 (an inscription)) – are related to trickery and deceit, and four of these sixteen instances of communication are clear examples of secret communication or hidden confidential messaging: that is, steganography (1.123; 5.28; 7.239; 8.128).¹⁰⁹ What is more, each of these steganographic messages have key features in common: all instances are examples of long distance communication sent when roads were guarded; there is no intra-Greek (Greek to Greek) exchange of messages, or the messages were sent in extra-Greek settings (sent to locations geographically outside of Greece); and all four instances reveal an aversion to oriental despotism and the perceived

¹⁰⁸ Herodotus, *Histories*, 1.21.1-22.3; 1.59.3-6; 1.60.3-5; 1.80.2; 1.96.2-98.2; 1.123; 1.125; 1.187; 1.191; 1.207.6-7; 2.100.2-4; 2.121A.1; 2.121D; 2.121E; 2.133; 2.162.1; 2.172; 3.1.3-5; 3.4; 3.16.6; 3.61; 3.69.3-6; 3.85-86.2; 3.122; 3.123.2; 3.128 (2x); 3.130.1-2; 3.153-158.2; 4.134.3; 4.139.2; 4.146.4; 4.154.3-4; 4.201; 5.12-13; 5.20; 5.24-25.1; 5.35; 5.49-50; 5.63.1; 6.4; 7.239; 8.5; 8.22; 8.24-25.2; 8.27.3; 8.28; 8.75-76; 8.87; 8.109; 8.128-129.1; 8.137; 9.33.4-5; 9.34; 9.94; 9.98.2-4; 9.110.2-112; 9.116.2-3; 9.120.2-4.

¹⁰⁹ The three letters that did not involve trickery and deceit are two letters sent between Amasis and Polycrates (Herodotus, *Histories*, 3.40-42), and a letter from Darius to Megabyzus instructing the latter to attack Paeonia (Herodotus, *Histories*, 5.14.1).

strangeness of non-Greeks. In three instances secret letters were involved: a message from the Mede Harpagus to the future king Cyrus of Persia in a letter hidden in a hare (Herodotus, *Histories*, 1.123.4-1.124), a message from the Spartan king Demaratus to the Spartans on Xerxes' invasion of Greece written under the wax of a wax tablet (7.239), and correspondence between Timoxenus, *strategos* of the Scionians, and the Persian commander Artabazus through letters written and sent hidden by the feathers on arrows that were shot into an agreed place (8.128). The fourth instance is a message from Histiaeus of Miletus to his son-in-law Aristagoras – tattooed on a slave's head – inciting Aristagoras to revolt against king Darius (5.35.2-4). These four examples of steganography will be discussed below but I will start by giving some context on Herodotus's views towards tyranny and how the instances of secret communication fit into this context (§ 1.2.1). This will be followed by an analysis of the two non-Greek examples of steganography (§ 1.2.2; 1.2.3), followed by the example in which a Greek corresponded with a non-Greek (§ 1.2.4), before turning finally to Demaratus' message to the Spartans (§ 1.2.5). Hereby it will be shown that one can see a pattern in these four secret messages in Herodotus' accounts, namely, that each of the examples of steganography in the *Histories* clearly shows Herodotus' negative views towards the despotic non-Greek regimes and oriental kingdoms who used secret communication in contrast to an open and democratic Greece – especially Athens – that was no longer under Persian rule, and where people communicated openly with each other (see § 1.2.6). In fact, as Ceccarelli points out, at the time at which Greek democracy first appeared, oral communication was seen as the most democratic form of communication – as opposed to the secretive written records that the Greeks assumed were used by tyrannical oriental regimes.¹¹⁰

¹¹⁰ Ceccarelli 2013, 195.

1.2.1: Herodotus' views towards non-Greek secret communication

As will be discussed in the following sections, all four steganographic letters discussed by Herodotus are examples of long distance communication sent when roads were guarded. This may simply show that secret forms of communication were (and still are) necessary under despotic and tyrannical regimes. However, Herodotus had more personal reasons to despise oriental suppressing regimes. Although his birthplace Halicarnassus was a Greek city which lay on the extreme eastern edge of the Greek world, by Herodotus' time – the early 5th century BCE – it was subject to Persian control.¹¹¹ As a defender of a free Greece and vocal advocate of its freedom from tyrannical Persian rule, Herodotus seems to have taken part in political struggles against the Persian king or 'tyrant' Lygdamis. These struggles ended in the death of Herodotus' cousin (or uncle) Panyassis and in Herodotus' own exile.¹¹² Because of this personal experience of and strong aversion to despotic regimes, Lateiner suggests that Herodotus especially supported cases in which an otherwise defenceless individual attempted to outwit or out-manoeuvre a powerful tyrannical autocrat – as is the case in three out of four instances of the examples of steganography that can be found in his work (Herodotus, *Histories*, 1.123.4-1.124; 5.35.2-4; 7.239).¹¹³ All eastern rulers mentioned in the *Histories* are depicted as despotic invaders (Croesus (Book 1), Cyrus (Book 1), Cambyses (Book 2-3), Darius (Book 3-4), Xerxes (Book 7-9)),¹¹⁴ and Herodotus' narrative is full of stories about characters who used various forms of trickery and deceit either to gain power as despotic leaders (negatively portrayed) or to deceive these leaders (e.g.: Herodotus, *Histories*, 1.8-12;

¹¹¹ Gould 2012, 674.

¹¹² Gould 2012, 674; Waters 1972, 138.

¹¹³ Lateiner 1990, 231; Gould 2012, 674; Waters 1972, 138.

¹¹⁴ The story of Deioces the Mede (1.96-101) is an example of the evils of autocratic rule, something that Dewald calls the 'despotic template' (Dewald 2003, 28-33). In this version of the template, a *tyrannis* (the rule of a tyrant) is a bureaucratic autocracy, and it is marked by an institutional harshness and distance between ruler and ruled (Dewald 2003, 28-33; Ferrill 1978, 385-398).

1.47-49; 1.60; 1.63; 3.72; 3.85-88; 3.154-60; 8.24-25). We can also find various examples of political treachery (Herodotus, *Histories*, 1.205.2; 4.78.2; 5.37.1; 3.65.6; 9.85) and of military deceit that Herodotus appears to have admired for its effectiveness or intellectual ingenuity (Herodotus, *Histories*, 1.21; 1.91.1; 1.212.2; 2.100.2; 3.72 and 3.85-88 on Darius using lies, trickery and deceit to become the king (negatively portrayed); 3.150-160 (on how the Persian nobleman Zopyrus played a decisive role in Darius' siege of Babylon by mutilating himself and convincing the Babylonians that he was deserting from Darius' camp and requesting shelter in the city – while he then opened the city's gates to the Persians); 4.146.3; 4.160.4; 4.201-202; 6.77.-79; 8.27.3-4; 9.90.3).¹¹⁵ Such acts of deception necessarily had to be hidden from what Greek sources (including Herodotus) call the 'King's Eyes and Ears' – apparently a sort of ancient 'secret service', most likely in the form of a group of high ranking officials through whom (in the view of the Greeks) the Persian king received all sorts of information on agitation throughout his kingdom (Aeschylus, *The Persians*, 979; Herodotus, *Histories*, 1.114.2; Xenophon, *Cyropaedia*, 8.2.10-12; 8.6.17-18).¹¹⁶ That fact that the Greeks potentially saw the 'King's Eyes and Ears' as some sort of secret police or intelligence agency becomes most clear from a passage in Xenophon's *Cyropaedia* where the author told us that Cyrus had men spying for him:

τοὺς βασιλέως καλουμένους ὀφθαλμοὺς καὶ τὰ βασιλέως ὦτα οὐκ ἄλλως ἐκτίσαστο ἢ τῷ δωρεῖσθαι τε καὶ τιμᾶν· τοὺς γὰρ ἀπαγγέιλαντας ὅσα καιρὸς αὐτῷ εἶη πεπύσθαι μεγάλως εὐεργετῶν πολλοὺς ἐποίησεν ἀνθρώπους καὶ ὠτακουστεῖν καὶ διοπεύειν τί ἂν ἀγγείλαντες ὠφελήσειαν βασιλέα (Xenophon, *Cyropaedia*, 8.2.10)

[He] acquired the so-called “king's eyes” and “king's ears” in no other way than by bestowing presents and honours; for by rewarding liberally those who reported to him whatever it was to his interest to hear, he

¹¹⁵ See also Dewald 1993, 55-70; Hollmann 2005, 316-323. Hollmann provides us with a list of 69 instances of trickery and deceit in Herodotus.

¹¹⁶ Bowie 2007, 160.

prompted many men to make it their business to use their eyes and ears to spy out what they could report to the king to his advantage.

We cannot know what Herodotus thought of the 'King's Eyes' since he discussed it in a fairly neutral way, by simply saying that Cyrus appointed one person as the 'King's Eye', and various other men as this person's assistants (τὸν δὲ κου τινὰ αὐτῶν ὀφθαλμὸν βασιλέος εἶναι, τῷ δὲ τινὶ τὰς ἀγγελίας φέρειν ἐδίδον γέρας, ὡς ἐκάστῳ ἔργον προστάσσων; Herodotus, *Histories*, 1.114.2). Yet, the passage shows that Herodotus saw a connection between oriental states and kings spying on their people.

Indeed, this idea of spying and eavesdropping on one's subordinates in oriental states can also be found in Herodotus' discussion of how Deioces the Mede had spies and eavesdroppers throughout his lands (κατήκοοι ἦσαν ἀνὰ πᾶσαν τὴν χώραν τῆς ἡρχε [...] and he [Deioces] had spies and eavesdroppers everywhere in his dominions; Herodotus, *Histories*, 1.100.2). Through its association with these closed societies and tyrannical (that is, non democratic) 'non-Greek' states, ancient sources attribute to Sparta a similar sort of secret service or *krypteia* (Justin, *Epitome of the Philippic History of Pompeius Trogus*, 3.3; Plato, *Laws*, 1.633b-c; 6.763b; a *Scholia on Plato's Laws* 1.633b-c; 6.763b, Edition De Forest Allen, Burnet, et al.; Plutarch, *Life of Cleomenes*, 28.4; *Life of Lycurgus*, 28.1-7; Pseudo-Heraclitus of Pontus (*Fragmenta Historicorum Graecorum*, 2 = Aristotle, Fragment 538).¹¹⁷ Significantly, as Bowie and Briant point out, descriptions of the 'King's Eyes and Ears' can only be found in Greek sources – but not in Persian sources.¹¹⁸ The same is the case for our sources on the Spartan *krypteia* and the *scytale*: all sources are non-Spartan – and accordingly unreliable and liable to (anti-Spartan, pro-Athenian) bias. In fact, Herodotus repeatedly insists that the Spartans are more like the Persians and the Egyptians than they are like the other Greeks (Herodotus,

¹¹⁷ Cartledge 2003, 70; Ross 2012.

¹¹⁸ Bowie 2007, 160; Briant 2002, 343-344; Sheldon 2008, 79.

Histories. 6.58-60). Their constitution even fell into his category of non-Greek oriental regimes as the historian told us in book 6:

νόμος δὲ τοῖσι Λακεδαιμονίοισι κατὰ τῶν βασιλέων τοὺς θανάτους ἐστὶ ὡντὸς καὶ τοῖσι βαρβάροισι τοῖσι ἐν τῇ Ἀσίῃ· τῶν γὰρ ὧν βαρβάρων οἱ πλεῖνες τῷ αὐτῷ νόμῳ χρέωνται κατὰ τοὺς θανάτους τῶν βασιλέων (Herodotus, *Histories*, 6.58)

The Lacedaemonians have the same custom at the deaths of their kings as have the foreign people of Asia; for the most of the foreigners use the same custom at their kings' deaths.

Συμφέρονται δὲ ἄλλο οὗτοι τόδε τοῖσι Πέρσησι· ἐπεὰν ἀποθανόντος τοῦ βασιλέος ἄλλος ἐνίστηται βασιλεύς, οὗτος ὁ ἐσιὼν ἐλευθεροῖ ὅστις τι Σπαρτητέων τῷ βασιλείῃ ἢ τῷ δημοσίῳ ὄφειλε· ἐν δ' αὖ Πέρσησι ὁ κατιστάμενος βασιλεὺς τὸν προοφειλόμενον φόρον μετιεῖ τῇσι πόλεσι πάσῃσι (Herodotus, *Histories*, 6.59)

Here is another matter wherein the Lacedaemonians are like to the Persians:—When one king is dead and another takes his office, this successor releases from debt what Spartan so ever owed anything to the king or the commonwealth; so too among the Persians the king at the beginning of his reign forgives all cities their arrears of tribute.

Συμφέρονται [...] τάδε Αἰγυπτίοισι Λακεδαιμόνιοι· (Herodotus, *Histories*, 6.60)

Moreover, the Lacedaemonians are like the Egyptians [...].

The fact that Herodotus explicitly describes the Spartans as using non-Greek practices clearly aligns Sparta with those oriental states in which – according to the Greeks – kings were supposed to spy and eavesdrop on their subordinates, hereby suggesting that the Persian and perhaps also Spartan society (e.g. with the *krypteia*) were particularly interested in using and intercepting secret communications (see e.g.: Aeschylus, *The Persians*, 979; *The Suppliants*; Aristotle, *On the Universe*, 398a; Herodotus, *Histories*, 1.114.2; 8.8.1-2; Justin, *Epitome of the Philippic History of Pompeius Trogus*, 3.3; Plato, *Laws*, 1.633b-c; 6.763b; a *Scholia on Plato's Laws* 1.633b-c; 6.763b, Edition De Forest Allen, Burnet, et al.; Plutarch, *Life of Cleomenes*, 28.4; *Life of Lycurgus*, 28.1-7; Pseudo-Heraclitus of Pontus (*Fragmenta Historicorum*

Graecorum, 2 = Aristotle, Fragment 538; Xenophon, *Cyropaedia*, 8.2.10-12; 8.6.17-18). Because of Herodotus' dislike of despotic regimes – having been brought up as a Greek under Persian rule – it seems logical, therefore, that the four instances of secret communication that will be discussed in the following sections of this chapter all reveal an aversion to oriental despotism and the perceived strangeness of non-Greeks – including Spartans – using secret communication and spies. For Herodotus and other Greeks after him, non-Greek states stood in clear contrast to a free Greece – where people communicated openly with each other, the epitome of which would have been Athenian democracy after Athens had disposed of its own tyrants. Non-Greek (including Spartan) tyranny and practices including the use of secret or secretive communication remained a marker of oriental states and their 'foreign' ways¹¹⁹ – while freedom (especially freedom of speech and communication) became a marker for Greece and the Greek ways.¹²⁰

1.2.2: Harpagus to Cyrus: the message in the hare

The first instance of secret communication that Herodotus offers is an account of steganography that occurs in Book 1.¹²¹ According to Herodotus, political intrigue and feuding among the Persians once prompted the Median general Harpagus, to plot against his king Astyages, seeking revenge for the murder of Harpagus' son by the king. Harpagus, therefore, plotted to assist the Persian prince Cyrus against Astyages in a *coup d'état*. Having garnered support from some Median nobles, Harpagus sent word to Cyrus through a message hidden in

¹¹⁹ Dewald 2003, 32-58.

¹²⁰ Georges 1994; Hall 1989, 191-195; Konstan 1987; Lateiner 1989, 152-155; Pelling 2002, 126; Sinclair 1967, 39; Thomas 2002, 116.

¹²¹ Although modern historians of cryptography often present the stories as clear facts (e.g. on Demaratus' letter to the Spartans see Bauer 2013, 7-8; Bartlett 2002, 8-12; Singh 1999, 5), it cannot be said with certainty how much of the stories is fact and how much is fiction. See for this designation of the Spartans being depicted as having 'non Greek' practices e.g. Cartledge 2009; 2013; Osborne 2011.

the body of a hare, since he desired to make his intent known to Cyrus. Yet, the plot obviously had to remain a secret, and, as Herodotus told us, all roads were guarded. Harpagus, therefore, decided to hide a message in a hare that was then presented to Cyrus as a gift (1.123-1.124):¹²²

οὕτω δὴ τῷ Κύρῳ διαιτωμένῳ ἐν Πέρσῃσι βουλόμενος Ἄρπαγος δηλῶσαι τὴν ἐωυτοῦ γνώμην ἄλλως μὲν οὐδαμῶς εἶχε ἅτε τῶν ὁδῶν φυλασσομενέων, ὃ δὲ ἐπιτεχνᾶται τοιόνδε· λαγὸν μηχανησάμενος, καὶ ἀνασχίσας τούτου τὴν γαστέρα καὶ οὐδὲν ἀποτίλας, ὥς δὲ εἶχε οὕτω ἐσέθηκε βυβλίον, γράψας τὰ οἱ ἐδόκεε (Herodotus, *Histories*, 1.123; for the complete passage see Appendix 1, page 273-274).

Harpagus desired to make known his intent to Cyrus, then dwelling among the Persians; but the roads were guarded, and he had no plan for sending a message but this—he artfully slit the belly of a hare, and then leaving it as it was without further harm he put into it a paper on which he wrote what he thought fit.

After receiving the gift, cutting the hare open and reading the message, Cyrus acted upon Harpagus' advice to rally the Persians against the Medes, and with the help of Harpagus, Cyrus was victorious (1.127). Herodotus finished his story by stating that in this way king Astyages was deposed from his sovereignty after ruling cruelly for 35 years (*Ἀστυάγης μὲν νυν βασιλεύσας ἐπ' ἔτεα πέντε καὶ τριήκοντα οὕτω τῆς βασιλείης κατεπαύσθη*; 1.130) The example clearly shows that Herodotus had negative views towards oriental despotic regimes and that he believed that there was a close connection between these regimes and the use of secret communication. The story of the steganographic message in the hare is a direct reference to overcoming tyrannical rule since Harpagus urged Cyrus to revolt against Astyages. As will be shown in the other three examples of steganography found in Herodotus work, this relationship between oriental despotic regimes and the use of secret communication keeps repeating itself – culminating in our last example – Demaratus' letter to the Spartans (§ 1.2.5; *Histories*, 7.239) – which shows how a

¹²² On Harpagus' motives for sending the message and his role in the story as described by Herodotus, see Gray 1995, 185-211, see also: Polyaeus, *Stratagems of War*, 3.13.3.

Spartan in an oriental context first used secret communication (at least, in the history told according to Herodotus).

1.2.3: Histiaeus to Aristagoras: the tattooed slave

The second Herodotean story in which steganography played a crucial role can be found in book 5 of the *Histories*.¹²³ According to Herodotus, Aristagoras, tyrant of Miletus, once launched a joint expedition with the Persian *satrap* Artaphernes to conquer Naxos, to bolster his political position (5.28-32). The mission was a debacle and Herodotus reports that, sensing his imminent removal as a tyrant, Aristagoras chose to invite the whole of Ionia into rebellion against the Persian king Darius the Great (5.33-35.1; for the complete passage see Appendix 1, page 274-275). According to Herodotus, to foment this revolt – the Ionian Revolt¹²⁴ – Histiaeus, tyrant of Miletus and father-in-law to Aristagoras, who was at the time residing in the Persian city of Susa – shaved the head of his most trusted slave and tattooed a secret message on it urging Aristagoras to revolt against king Darius. As in the previous example, secret communication was the only safe way of sending the message since again a revolt was discussed that had to be kept secret and all roads were guarded – as Herodotus tells us (*οὐδαμῶς εἶχε ἀσφαλέως σημῆναι ὥστε φυλασσομενέων τῶν ὁδῶν*; 5.35.3). Histiaeus then waited for the slave's hair to grow back, and subsequently sent the man to Aristagoras in Miletus, instructing him to let Aristagoras shave his head again for the message to become visible (5.35.2-4).¹²⁵

¹²³ Modern cryptographers again, often present this story as an historical account based in fact (Bauer 2013, 8; Singh 1999, 6).

¹²⁴ On causes of the Ionian Revolt as discussed in Herodotus' work, see Evans 1976; Forrest 1979, 315-317; 320-322; Manville 1977, 80-91; Waters 1985. See also Blamire 1959; Lang 1968.

¹²⁵ Chapman incorrectly suggests that Herodotus' work is the only account of the Ionian Revolt available to us (Chapman 1972, 546). In addition to Herodotus' work we have e.g. Aeschylus' *The Persians*, and Thucydides, *History of the Peloponnesian War*, 1.22. On Histiaeus' role in Herodotus account of the Ionian Revolt see Blamire 1959; Chapman 1972, 546-568; Evans 1976; Lang 1968.

Ceccarelli presumes that, according to Herodotus, Histiaeus tattooed the word ‘*revolt*’ on the slave’s head.¹²⁶ However, in his account Herodotus did not disclose what Histiaeus’ message actually said. Still, the information was enough to prompt Aristagoras to convene a council and prepare for rebellion against Persia (5.36; see also Aeneas Tacticus, *How to Survive Under Siege*, 31.28-29; Aulus Gellius, *Attic Nights*, 17.9.18-27; Polyaeus, *Stratagems of War*, 1.24). As in the previous example of Harpagus to Cyrus, we see another rebellion in an oriental state being discussed in secret by officials of the highest ranks. Again, the purpose of the rebellion is to depose of an oriental tyrant – in this case the Persian king Darius. Yet, in this case the instigator of the rebellion did not come from an oriental state himself, as in the previous examples. Instead the instigator was Histiaeus – the Greek tyrant of Miletus in Asia Minor – communicating with his son-in-law Aristagoras who was at the Persian court of Darius. The example fits in well with Herodotus’ negative view towards tyranny and the importance of deposing oriental tyrants since this example shows how in the Near East slaves could be mutilated in order to send messages – at least according to Herodotus.¹²⁷ It also shows that Greeks in Asia Minor – who were already living in an oriental context – could have had a chance to learn about the use of secret communication in oriental states. It will be shown later in this thesis that this example is slightly different in context from Demaratus’ letter to the Spartans. While the message from Histiaeus to Aristagoras was sent between two Greeks who were living in Ionia under Persian rule, Demaratus – having come from Sparta, instead of Ionia – sent his letter to the Spartans while in exile at the Persian court.

¹²⁶ Ceccarelli 2013, 114.

¹²⁷ Ceccarelli 2013, 127.

1.2.4: Correspondence between Timoxenus and Artabazus: letters on arrows

The third instance of a secret letter occurs in Book 8 of Herodotus' work. This story is set at the siege of Potidaea in 479 BCE,¹²⁸ after the battle of Salamis. Timoxenus, *strategos* of the Scionians, betrayed his city by trading messages with the Persian commander Artabazus through letters hidden under the feathers on arrows – *περώσαντες* (*pterosantes*); literally 'covered' or 'furnished with feathers' (8.128.1) – that were shot into an agreed place. The messages were wrapped around the shaft of the arrow that was subsequently covered in feathers to make the message invisible – just as the message on the slave's head was covered by his hair (5.35.2-4; see also Aeneas Tacticus, *How to Survive Under Siege*, 31.25-27):¹²⁹

ὅπως βυβλίον γράψει ἢ Τιμόξεινος ἐθέλων παρὰ Ἀρτάβαζον πέμψαι ἢ Ἀρτάβαζος παρὰ Τιμόξεινον, τοξεύματος παρὰ τὰς γλυφίδας περιελίξαντες καὶ περώσαντες τὸ βυβλίον ἐτόξευον ἐς συγκείμενον χωρίον (Herodotus, *Histories*, 8.128.2; for the complete passage see Appendix 1, page 275-276).

Whenever Timoxenus wrote a letter for sending to Artabazus, or Artabazus to Timoxenus, they would wrap it round the shaft of an arrow at the notches and put feathers to the letter, and shoot it to a place whereon they had agreed.

Timoxenus' treachery was apparently discovered only when Artabazus missed his aim. Instead of his steganographic arrow falling in the spot agreed upon, Artabazus accidentally shot a Potidaean. People who came to aid the wounded man found the letter on the arrow and Timoxenus' betrayal became known (8.128-129.1).¹³⁰ This is a good example of Herodotus' negative view towards non-Greek practices – since here a Greek (Timoxenus) betrayed his fellow Greeks by aiding the Persians in using secret communication. Unlike truthful Greeks,

¹²⁸ For the date, see e.g. Burliga 2008, 92-93. See also Thucydides, *History of the Peloponnesian War*.

¹²⁹ Godley 1925, 131; How & Wells 1928, 700.

¹³⁰ This example shows that secret communication always runs the risk of discovery.

Herodotus seems to imply in the passage, Timoxenus acted like a Persian (a non-Greek) – as the Spartans did too, as will be discussed in the next example (7.239; see also 6.58-60).

1.2.5: Demaratus' letter to the Spartans: a message hidden under the wax of a wax tablet

The final secret letter to be discussed here – found in Book 7 of the *Histories* – shows that according to Herodotus, the Spartans in the 5th century BCE already used secret communication as oriental states did. According to Herodotus, when the Spartan king Demaratus was in exile at Xerxes' court in Persia, he wanted to send word to the Spartans to inform them about Xerxes' invasion of Greece. Since Demaratus was afraid that the message would fall into the wrong hands, he wrote the message under the wax of a wax tablet. The seemingly blank tablet reached Sparta, and the Spartans were initially confused about what to do with an ostensibly blank tablet until Gorgo – the wife of King Leonidas – suggested that they look for a hidden message (οἱ Λακεδαιμόνιοι, πρίν γε δὴ σφι, ὡς ἐγὼ πυνθάνομαι, Κλεομένεος μὲν θυγάτηρ Λεωνίδεω δὲ γυνὴ Γοργῷ ὑπέθετο ἐπιφρασθεῖσα αὐτή, τὸν κηρὸν κνᾶν κελεύουσα, καὶ εὐρήσειν σφέας γράμματα ἐν τῷ ξύλῳ [...]) When the tablet came to Lacedaemon, the Lacedaemonians could not guess its meaning, till at last (as I [Herodotus] have been told) Gorgo, Cleomenes' daughter and Leonidas' wife, discovered the trick of herself and advised them to scrape the wax away, when they would find writing on the wood; 7.239; see also Aulus Gellius, *Attic Nights*, 17.9.16-17; Polyaeus, *Stratagems of War*, 2.20; Justin, *Epitome of the Philippic History of Pompeius Trogus*, 2.10.12-17; Julius Africanus, *Kestoi*, 53. See for a similar example of a secret message written under the wax of a wax tablet by Hamilcar the Rhodian in the time of Alexander the Great: Aulus Gellius, *Attic Nights*, 17.9.16-17; Justin, *Epitome of the Philippic History of*

Pompeius Trogus, 21.6; for the complete passage see Appendix 1, page 275).¹³¹ Here we see for the first time Spartans communicating with each other secretly – yet in a partially oriental context, since Demaratus sent the message while he was in exile at the court of Xerxes of Persia. This implies that the Spartans probably learned to use secret communication from the Persians, e.g. when living amongst them, at least according to Herodotus. In the next chapter it will be shown that other Greeks after Herodotus, in the 5th and 4th centuries BCE started to connect Sparta more often to secrecy and secret communication after reading the *Histories*. This work introduces a contradiction that we see playing out in several post-Herodotean sources as well: that is, on the one hand, the Spartans are stereotyped as uncivilised, stupid, and semi-literate, while on the other hand they are associated with cunning secrecy and deception – including the use of secret *written* communications. To return to Demaratus' example, Herodotus does not tell us why it was Gorgo who discovered the message or how she discovered it,¹³² but according to Herodotus, because of Demaratus' letter, the Spartans were warned in time, informed the other Greeks, and together they defeated the Persians at the Battle of Salamis (Herodotus, *Histories*, 7.239; 8). This is significant since Demaratus had to rely on the ingenuity of the Spartans to discover the secret message. The apparent success of the message being delivered and understood seems to be the major point of discussion for modern historians of cryptography. Sheldon, for example, sees Demaratus' message as 'one of the most

¹³¹ According to Justin it was not the king's wife, but his sister who discovered Demaratus' message (Justin, *Epitome of the Philippic History of Pompeius Trogus*, 2.10.12-172.10.13). As Millender points out, Herodotus' account of the Spartans' reception of this message credits the Lacedaemonian authorities with the ability to read and implies Gorgo's familiarity with wooden writing tablets (Millender 2001, 142). See also Dvornik 1974, 57; Sheldon 1987, 28; Sheldon 2005, 42.

¹³² The passage in which Gorgo discovered Demaratus' secret message is the oldest known passage in which a woman took the initiative in deciphering a secret message. Later – in Roman love elegy – we find many examples in which the woman took initiative in sending secret messages (see Propertius, Tibullus, Ovid; especially Ovid, *Ars Amatoria*).

important messages in all of Greek history'.¹³³ And according to Singh, Xerxes had lost the vital element of surprise and, when the Persian fleet approached the Bay of Salamis near Athens, the Greeks were prepared.¹³⁴ As in the case of the Spartan *scytale* (see *Review of literature* and chapter 2) this shows how modern historians of cryptography often tend to present Herodotus' stories as clear historical facts, attributing the direct influence of the secret messages that Herodotus discusses to the success of subsequent historical events. The case, I argue, is more complex.

1.2.6: Analysing instances of secret communication in Herodotus' work

We can see a pattern in the secret messages that occur in Herodotus' 'history'. As Fabule points out:

the pattern reflects the following scenario: under the thumb of some potentate, a leader (foreign tyrant, a general, or client-king) sends a cunningly disguised secret message, that related information detrimental to his overlord.¹³⁵

The four instances of steganography in Herodotus' work are unique since they have three features in common that cannot be found in this combination elsewhere in the work in connection with other messages or in other instances of trickery and deceit.¹³⁶ First, all four instances are examples of long distance communication sent when roads were guarded. The aforementioned steganographic methods used for sending the messages were purposefully chosen instead of cryptographic methods and designed to raise as little suspicion as possible

¹³³ Sheldon 1986, 39.

¹³⁴ Singh 1999, 5.

¹³⁵ Fabule 2011, 36. For a concise list of exiled or alienated Greeks who, for their own purposes, solicited Persian assistance against their fellow-citizen, see Boedeker 1987, 191-192.

¹³⁶ Ceccarelli 2013, 113. For a list of all instances of trickery in Herodotus' *Histories* see Hollmann 2005, 316-323.

among third parties. Secondly, there is no intra-Greek exchange of messages. Messages were either sent between a Greek and a non-Greek (Timoxenus and Artabazus), between non-Greeks (Harpagus and Cyrus; Histiaeus and Aristagoras), or in a non-Greek setting (Demaratus as exile in Persia). Thirdly, all four instances deal with an aversion to oriental despotism. In the case of Timoxenus and Artabazus, Herodotus showed this aversion by overtly disapproving of Timoxenus' betrayal, while the other three cases even deal with overthrowing an oriental despot (Harpagus and Cyrus; Histiaeus and Aristagoras; Demaratus to the Spartans). It is also significant in the context of this thesis that written messages appear to have been more common in the Near East than in Greece in Herodotus' days.¹³⁷ In fact, until the first reading culture appears in Athens in the 4th century BCE (based on the fact that a large number of sources date to this period; see § 2.1) – and perhaps even after that – in ancient Greece letters and long distance communications were often related to an oriental and tyrannical context and believed to be fraught with dangers (see e.g.: Apollodorus, *Epitome*, 3.7; 5.19; Hellanicus Fragment 178a, in: *Fragmente der Griechischen Historiker* 4; Pausanias, *Descriptions of Greece*, 10.31.2; Plato, *Apology*, 41b; Herodotus, *Histories*, e.g. 1.99-100).¹³⁸ Homer's story of Bellerophon's tablet, as we saw above, potentially appeals to this oriental context of letters and letter writing in terms of the readiness of ancient scholia critics to interpret Proetus' writing as a kind of Egyptian hieroglyphic text (§ 1.1.1; Homer, *Iliad*, 6.166-170; 178).¹³⁹ Rosenmeyer further points out that the letter sent in Bellerophon's story encapsulates two major themes related to letter writing that can often be found in Greek literature: a deceitful letter and an association between letters and deceitful women – hereby again signposting towards the

¹³⁷ Ceccarelli 2013, 185. See for letters and letter writing in the ancient Near East e.g.: Bellamy 1989, 291-292; Luschán & Andrae 1943, 108-109; Mallowan 1966; Mylonas Shear 1998, 187-189.

¹³⁸ Ceccarelli 2013, 24.

¹³⁹ Bellamy 1989, 289; Ceccarelli 2013 60; Rosenmeyer 2001, 39.

decidedly negative view towards letter writing in the archaic period.¹⁴⁰ By the end of the 5th century BCE literacy was most likely more widespread in the Greek world than before this date and the exchange of letters took place regularly, it seems – based on the large number of inscriptions that have survived from this period.¹⁴¹ Yet, in Herodotus’ *Histories* letters are still relatively exceptional: only fourteen instances are found – none of which concern direct intra-Greek communication in a Greek context (as Demaratus’ letter to the Spartans was an indirect communication set in an oriental context).¹⁴² Significantly, in the time of Herodotus it appears that letters were seen as secretive weapons of an oriental tyrant opposing the ‘open’ communications of the free Greek polis (such as embassies’ decrees, and assembly speeches).¹⁴³ Yet, the four instances of steganographic communication in Herodotus show that, in these stories at least, the oriental weapon of letter writing was now imagined as being used *against* these oriental tyrants. What is more, one of these stories also shows that the oriental weapon of letter writing was now imagined as being used by the Spartans.

At the beginning of this chapter the following research question was posed: *What are the instances of secret communication in Herodotus’ Histories and how are these coloured by Herodotus’ view of the Spartans as ‘non-Greek’?* As has been shown in the chapter above, Herodotus’ four examples of secret communication in his *Histories* are clearly associated with non-Greeks and their use characterised as un-Greek behaviour. Hereby, we also discovered that Herodotus’ account of Demaratus’ letter to the Spartans plays a crucial role in the prevailing

¹⁴⁰ Rosenmeyer 2001, 42–44.

¹⁴¹ Yet, absence of evidence is not evidence of absence. Therefore, we must be careful when making such claims about literacy in ancient Greece (Ceccarelli 2013, 185). However, despite multiple investigations there is still no agreement on the degree of literacy achieved by all the Greeks in the late archaic and classical periods. See e.g.: Boring 1979; Cartledge 1978; Clanchy 1979; Goody 1986; Goody & Watt 1968; Harris 1989; Havelock 1963; 1982; Harvey 1966; Immerwahr 1990; Steiner 1994, 4; Street 1984; Swiggers 1996; Thomas 1989; Turner 1952.

¹⁴² Ceccarelli 2013, 113.

¹⁴³ Ceccarelli 2013, 279.

Greek view of the Spartans as a people familiar with the use of secret communication – as oriental states did. The fact that according to Herodotus, Demaratus sent his message while being at the Persian court even implies that the Spartans may have learned about the use of secret communication from the barbaric and uncivilised Persians – something most clearly depicted in passage 1.71.2 where the Persians are seen as a barbaric people living in a harsh land:

ἐπ' ἄνδρας τοιούτους στρατεύεσθαι παρασκευάζει, οἱ σκυτίνας μὲν ἀναξυρίδας σκυτίνην δὲ τὴν ἄλλην ἐσθῆτα φορέουσι, σιτέονται δὲ οὐκ ὅσα ἐθέλουσι ἀλλ' ὅσα ἔχουσι, χώρην ἔχοντες τρηχέαν (Herodotus, *Histories*, 1.71.2)

[The Persians are] men who wear breeches of leather and their other garments of the same, and whose fare is not what they desire but what they have; for their land is stony. Further they use no wine, but are water-drinkers, nor have they figs to eat, nor aught else that is good.

Herodotus here portrays the Persians as primitive as opposed to the more civilised Greeks from his own days. The Spartans – being more like the Persians than like other Greeks (Herodotus, *Histories*, 6.58-60) – are then twice depicted as truly Persian and ‘non-Greek’ in passages 1.152-153. In passage 1.152 Herodotus tells us that the Spartans refused to aid the Ionians – their fellow Greeks – in the Greek struggle against the Persian occupation (Herodotus, *Histories*, 1.152), while in the next passage Cyrus (according to Herodotus) argued that one should never be afraid of a people (in this case the Spartans) who perjured themselves and deceived each other:

Οὐκ ἔδεισά κω ἄνδρας τοιούτους, τοῖσι ἐστὶ χώρος ἐν μέσῃ τῇ πόλει ἀποδεδεγμένος ἐς τὸν συλλεγόμενοι ἀλλήλους ὀμνύντες ἐξαπατῶσιν (Herodotus, *Histories*, 1.153.1)

I never yet feared men [i.e. the Spartans] who have a place set apart in the midst of their city where they perjure themselves and deceive each other.

This clearly shows the Herodotean biases surrounding Persia and Sparta as being particularly ‘non-Greek’, which in this case means ‘primitive’, ‘uncivilised’ and untrustworthy. Moreover,

like the Persians, the Spartans supposedly used non-Greek methods of secret communication (Herodotus, *Histories*, 1.123; 5.28; 7.239; 8.128). Indeed, Herodotus' bias against the Spartans is evident in this context too – and introduces a contradiction that we see playing out in several post-Herodotean sources as well with the Spartans on the one hand being cunning, but on the other hand being illiterate and foolish – as we will see in the next chapter. Indeed, according to Herodotus, the Spartans did not even know what to do with the seemingly empty wax tablet that Demaratus sent them until Gorgo suggested scraping off the wax (Herodotus, *Histories*, 7.239) – one of many examples in which Herodotus apparently presented a paradoxical picture of the Spartans in his *Histories*. Herodotus' biased views formed the basis for various other Greek (especially Athenian) sources from the 5th and 4th centuries BCE on, where we find similar links between illiterate Spartans and secret communications. Here, in these later 5th and 4th century BCE sources, we also find discussed the cryptographic *scytale* – and it is to these sources that we turn in the next chapter.

Chapter 2: The *scytale*

This chapter analyses how classical Greek sources after Herodotus – mainly dating back to the 5th and 4th centuries BCE – discussed the *scytale* as a Spartan ‘non-Greek’ cryptographic device, hereby connecting the Spartans with the non-Greek practice of secret communication, and aligning them with the secretiveness and deception traditionally associated with oriental states in Greek sources. The research question that will be posed in this chapter is, therefore: *How did non-Spartan sources present the Spartan scytale, and what evidence is there in these sources to suggest that the scytale was (or was not) used as a device for secret communication in the 5th and 4th centuries BCE?*

This chapter will start with a short discussion of the depiction of Spartan society (§ 2.1) and literacy in Spartan society (§ 2.2) – both according to non-Spartan sources – to provide some context. This section will show how surviving Greek sources written after Herodotus present a similarly contradictory picture of Spartan society – as uncivilised and semi-literate, yet as adept in the use of secret *written* communications. Since there are no surviving Spartan sources on the theme, this gives us a biased non-Spartan point of view and warns us to approach the Greek sources with a degree of caution. In fact, there is only one potential Spartan reference to a *scytale*. According to Polyaeus – writing in the 2nd century CE – the 7th-century BCE Spartan poet Tyrtaeus referred to the Spartan practice of identifying soldiers by means of *scytalae* (Polyaeus, *Stratagems of War*, 1.17). However, the nine centuries that separate these two writers (and the loss of the work by Tyrtaeus to which Polyaeus refers) means that we have no way to verify the validity of this source.

This analysis will be followed by a survey and analysis of all extant ancient sources on the *scytale* – starting with Archilochus of Paros in the 7th century BCE, and finishing with Plutarch in the late 1st/early 2nd century CE (§ 2.3) – to uncover what these sources can tell us

about the design, concept, and operation of the *scytale*. Indeed, it will be shown that the Greek word for *scytale* carries a wide range of different meanings (several of which do relate to or signify messaging of some kind) and that context plays an important part in considering whether or not a Greek source invites an interpretation that supports our understanding of the *scytale* as a device for *secret* communication. This chapter will conclude with a detailed discussion and analysis of the technical and conceptual workings of the *scytale* (§ 2.4) as discussed in the two descriptions on its use from Plutarch (*Life of Lysander*, 19.5-7) and Aulus Gellius (*Attic Nights*, 17.6-16) in order to reassess the potential for the *scytale* to have been used as a cryptographic device in practice. Hereby, it will be shown how the *scytale* would have worked well as a cryptographic transposition device and provided a useful encryption device for long distance secret communications – especially in military contexts and/or when one of the interlocutors was based in enemy terrain.

2.1: Spartan society according to non-Spartan sources

As we saw in the previous chapter, Herodotus depicted the Spartans as using ‘non-Greek’ practices in their use of secret communications (Herodotus, *Histories*, 6.58-60; 7.239). Indeed, Herodotus described the Spartans as a people eager to conquer other nations and to forestall the dangers of the growth of other competitor Greek states, especially Athens (Herodotus, *Histories*, 1.46; 1.67-68; 1.70; 1.77; 1.82-83; 1.88; 3.57; 5.46-65; 5.74-75; 5.91.1-2; see also Thucydides, *History of the Peloponnesian War*, 2.8.4; 1.140.1). Thus, as Herodotus described in his account of Demaratus’ letter to the Spartans, one of the potential dangers (although probably not a very big danger in Herodotus’ view since Herodotus depicts the Spartans as foolish; Herodotus, *Histories*, 1.152-153) of the Spartan expertise in secret communication was that it could be used against other Greeks – including Athenians. Unsurprisingly, therefore,

Greek and especially Athenian sources after Herodotus (mainly from the 5th and 4th centuries BCE) tend to follow his lead in depicting the Spartans and their ‘non-Greek’ practices of secret communication negatively, and to distance themselves from the use of such strange and secretive stratagems and devices. Aristophanes for example – in his comedy *Birds* – depicted the Spartans as barbarians in a passage in which he opposed this barbarism to Athenian civilisation. Before Athens became civilised, the poet stated, Athenians would even have behaved like these barbaric Spartans – a thing they luckily, so it seems, did not do anymore in his days:

πρὶν μὲν γὰρ οἰκίσαι σε τήνδε τὴν πόλιν,

ἐλακωνομάνουν ἅπαντες ἄνθρωποι τότε,

ἐκόμων ἐπείνων ἐρρύπων ἐσωκράτουν

σκυτάλι' ἐφόρουν, νυνὶ δ' ὑποστρέψαντες αὖ

ὄρνιθομανοῦσι, πάντα δ' ὑπὸ τῆς ἡδονῆς

ποιοῦσιν ἅπερ ὄρνιθες ἐκμιμούμενοι. (Aristophanes, *Birds*, 1280-1285; for the complete passage see Appendix 1, page 264).

Before you built this city all men were crazy about the Spartans:

they wore their hair long, went hungry,

never bathed, acted like Socrates,

brandished batons [*scytalae*].

But now they've about-faced and gone bird-crazy,

and they're having a wonderful time imitating birds in everything they do.

It is not only in comic plays that we see this negative view of the Spartans from which other Greeks – especially Athenians – apparently wanted to distance themselves. Aristophanes' idea can be compared to Thucydides' suggestion of the Spartan ‘barbaric’ custom of dressing in a very simplistic ‘Spartan’ way as opposed to Athenian ‘more civilised’ customs (Thucydides, *History of the Peloponnesian War*, 1.6). More differences between Athens and Sparta can be

found in book 1 of Thucydides' work – a book that focuses on the causes of the Peloponnesian War. Opposed to Athens with its elaborately decorated temples and public edifices, the Athenian historian argues, Sparta was built in a very simplistic (read 'non-Athenian') way, while Lacedaemon (Sparta) was composed of rural villages as opposed to the cities found in Attica (1.10). Thucydides argues that Athens' military power – just before the Peloponnesian War – alarmed the war-like Spartans, who became afraid of losing their own empire to the Athenians and made the outbreak of the war inevitable (1.23; 1.79; 1.88; on the 'warlike' Spartans as opposed to educated/civilised other Greeks, see also: 1.68-1.71 (a speech by the Corinthians); 1.75-1.78 (a speech by the Athenians)). Plutarch added that war seemed so important to all of Spartan society, that even Spartan mothers urged their sons to come back from war either *with* their shields (that is, victorious), or *on* them (that is, dead), but never *without* – since the latter would mean a soldier had retreated or even deserted (Plutarch, *Moralia*, 241-242). With these warlike customs came the idea (among non-Spartans) of the Spartans being uneducated. According to Plato, the sophist Hippias of Elis complained about the Spartans not being able to count, let alone be able to understand and appreciate his lectures (in this case an astronomy lecture), in a discussion with Socrates:

Socrates: [...] χαίρουσιν ἀκούοντες Cποῖα; ἢ δῆλον δὴ ὅτι ἐκεῖνα ἃ σὺ κάλλιστα ἐπίστασαι, τὰ περὶ τὰ ἄστρα τε καὶ τὰ οὐράνια πάθη;

Hippias: Οὐδ' ὅπωςτιοῦν ταῦτά γε οὐδ' ἀνέχονται. [...] οὐδ' ἀριθμεῖν ἐκείνων γε, ὥς ἔπος εἶπεῖν, πολλοὶ ἐπίστανται (Plato, *Greater Hippias*, 285c).

Socrates: [...] what sort of discourses are those for which they applaud you and which they enjoy hearing? Or are they evidently those which you understand most admirably, those about the stars and the phenomena of the heavens?

Hippias: Not in the least; they won't even endure those [...] [and] one might say that many of them do not even know how to count.

With these statements comes the underlying idea of ‘civilised citizens’ in Athens as opposed to ‘simple’ and ‘uneducated’ folk in Sparta. Together with these negative stereotypical views of the ‘illiterate’ Spartans comes a further connection that seems to have been made between Sparta and secrecy. Thucydides, for example, discusses the secrecy of the Spartan government (*τὸ μὲν γὰρ Λακεδαιμονίων πλῆθος διὰ τῆς πολιτείας τὸ κρυπτόν ἡγνοεῖτο [...]* *For on account of the secrecy of their polity the number of the Lacedaemonians was unknown; History of the Peloponnesian War*, 5.68.2; see also 7.424). The Spartans do not count or keep written records of their citizens, therefore, Thucydides apparently reasons, the Spartans are both illiterate and secretive. They supposedly monitor their citizens and keep the state under close surveillance in other (non-Greek) ways, however. Various other non-Spartan sources, for example, discussed the ‘eyes and ears’ of the Spartan kings – or *krypteia*: Justin (*Epitome of the Philippic History of Pompeius Trogus*, 3.3), Plato (*Laws*, 1.633b-c; 6.763b), a *Scholia on Plato’s Laws*, Edition De Forest Allen, Burnet, et al.; Plutarch (*Life of Cleomenes*, 28.4; *Life of Lycurgus*, 28.1-7), and Pseudo-Heraclitus of Pontus (*Fragmenta Historicorum Graecorum*, 2 = Aristotle, Fragment 538).¹⁴⁴ This stereotypical view of the Spartans leads some modern historians to describe Sparta as the most secretive of all Greek states.¹⁴⁵ Yet, before we turn to a more detailed examination and analysis of the ancient sources, it is important to reiterate that all known sources on the *scytale* are non-Spartan, and even anti-Spartan. This raises an important caveat to be taken into consideration when analysing the extant evidence for the use of hidden, encrypted and coded communications in the ancient Greek world. That is, the ancient Greek and especially Athenian sources tend to be biased in their discussions of the ‘non-Greek’ practice of using cryptography and steganography. In fact, it must be remembered that the majority of ancient Greek sources that describe Spartan

¹⁴⁴ Cartledge 2003, 70; 2013-II; Powell 2017, 25; Ross 2012.

¹⁴⁵ Boring 1979, 94; Huxley 1983, 2.

secret communication practices – including the *scytale* – date from the 5th and 4th centuries BCE (including Aristophanes and Thucydides) – the period during and after the Peloponnesian War, and the Athenian defeat (when anti-Spartan sentiment would have been high).¹⁴⁶

In this chapter, then, I will consider how ‘non-Spartan’ Greeks variously described the Spartan *scytale* and its uses in order to assess the reliability of these sources, to reassess the viability of the *scytale* as an ancient mode of secret communication, and thereby to challenge modern theories, such as those forwarded by Kelly et al., which argue that the *scytale* was never actually used as a cryptographic tool in the ancient world.¹⁴⁷ As will be shown in this chapter, these sources offer fragments of a bigger picture that emerges only when we look directly at a wide range of available sources which discuss the *scytale*, allowing us to take a broader view of the varied meanings of the word *scytale*. As will be shown, the sources give us an idea of how *scytalae* could have been used for a variety of purposes, ranging from the identification of fallen soldiers on the battle field (*ὥστε μέλλοντες παρατάττεσθαι τὰ ὀνόματα σφῶν αὐτῶν ἐγράψαντο εἰς σκυταλίδας καὶ ἐξῆψαν ἐκ τῆς χειρός, ἵνα τελευτῶντες μὴ ἀγνοῶνται ὑπὸ τῶν οἰκείων [...] when about to enter the conflict, they [the Spartans] wrote their names on little sticks which they fastened to their arms, in order that, if they died, they would not be unidentified by their kinsmen*; Diodorus Siculus, *Library of History*, 8.27; *Excerpta Constantiniana* 4; see § 2.3.9) – to the sending of secret messages (see § 2.3; 2.4; Plutarch, *Life of Lysander*, 19.5-7; Aulus Gellius, *Attic Nights*, 17.9.6-16)

¹⁴⁶ Significantly, this idea of the Spartans being seen as a people using ‘non Greek’ practices can even be found in Kasten’s 2001 cryptographic report ‘One Fish, Two Fish, Red Fish, Blowfish: A History of Cryptography and its Application in Society’ in which the Greeks and Spartans are mentioned separately: Kasten 2001, 1-2.

¹⁴⁷ See Kelly 1985, 162; Kelly 1998, 245; West 1988, 42; Strasser 2007, 278. Kelly, who dismisses the idea that the *scytale* was ever put to proper practical purpose as a method of secret communication in antiquity, acknowledges that if the Spartans ever had used the *scytale* for secret communication, they would most likely have done so between the outbreak of the Peloponnesian War in 431 BCE and the Battle of Leuctra in 371 BCE.

Although the sources we have are all non-Spartan, we will see that they show that other Greeks – especially Athenians – acknowledged that the Spartans wrote and sent short written messages and that they sometimes communicated in a secretive way. As well as hiding steganographic messages under the wax of wax tablets, under the hair of a slave, or within the body of a hare (as Spartans and Persians did, or so Herodotus alleged in his *Histories*), later Greek sources from the 5th and 4th centuries BCE discuss the Spartans as using another device for sending long distance (and potentially secret) messages – the *scytale*. However, although such descriptions are aligned with the longstanding ancient Greek stereotype of the Spartans as a secretive society, they also need to be understood in connection to another predominant Greek caricature of Spartan society – which saw the Spartans as illiterate.

2.2: Literacy in Spartan society

Taking a very broad definition of literacy as the ‘ability of an individual to make any use of writing as a tool for the satisfaction of normal social, business, or political requirements, however great or small’, we can investigate whether the question of literacy in Spartan society helps to cast any light on these issues.¹⁴⁸ Significantly, Harvey and Tigerstedt, in their 1960s studies of the ancient Greek world argue that 5th and 4th century BCE Greek sources are unanimous (if also, as we have seen, highly biased) in declaring that the Spartans could not read or write.¹⁴⁹ Boring, although being slightly more cautious, seems to have adopted this view in his 1979 work *Literacy in Ancient Sparta* when stating that some Spartans might have been able to only write their name – while only very few Spartans could potentially

¹⁴⁸ Boring 1979, 1. See also Harris 1989, 3.

¹⁴⁹ Harvey 1966, 624; Tigerstedt 1965, 49; 111.

have been able to write much more.¹⁵⁰ These views are clearly based on Athenian passages that describe the Spartans as illiterate. Aristotle, for example, described the Spartans as raising their children without concern for literacy or the higher values and educational attributes valued and promoted by an Athenian ‘civilised’ upbringing (Aristotle, Fragments 611; Plutarch, *Life of Lycurgus*, 16.10; *Moralia*, 237a). What is more, the unknown author of the late 5th/early 4th-century BCE work *Dissoi Logoi* (or: *Pairs of Arguments*) claimed that as opposed to other Greek children, for the Spartans:

τὼς παῖδας μὴ μανθάνειν μουσικὰ καὶ γράμματα καλόν, Ἴωσι δ’ αἰσχρὸν μὴ ἐπίστασθαι ταῦτα πάντα καλόν, Ἴωσι δ’ αἰσχρὸν μὴ ἐπίστασθαι ταῦτα πάντα. (*Dissoi Logoi*, 2.10; see also Sphaerus the Borysthenite, *Fragmente der Griechischen Historiker*, 585; Plutarch, *Lycurgus*, 14; *Parallel Lives: Agis and Clemones*, 32.3; Xenophon, *Constitution of the Lacedaemonians*, 1-4)

it is seemly that their [i.e. the Spartans’] children not learn music and letters but for the Ionians it is unseemly not to know all these things.

However, as archaeological and epigraphic evidence shows, the Spartans were not completely illiterate. Cartledge, for example, in his 1978 article ‘Literacy in the Spartan Oligarchy’, discusses two inscribed bronze artefacts that were excavated at the Menelaion sanctuary near Sparta in 1975, which were inscribed in letter forms that are distinguishably ‘Lakonian’.¹⁵¹ One was a sacrificial meat-hook with the inscription ‘to Helen’ dating back to the (late) 6th century BCE; the other was an *aryballos* (a small spherical or globular flask with a narrow neck) dating back to the middle of the 7th century BCE. From the inscription on the *aryballos* it is clear that the item was dedicated to ‘Helen, wife of Menelaos’. Moreover, Cartledge points out the neatness of the inscription of the *aryballos*. This neatness suggests a long writing tradition in Sparta.¹⁵² In addition, there are a number of other inscriptions known

¹⁵⁰ Boring 1979, 1.

¹⁵¹ Cartledge 1978, 26; Catling & Cavanagh 1976, 145-157.

¹⁵² Cartledge 1978, 26.

to have come from Sparta, on e.g. grave stelae, public buildings and tableware (e.g. on a Spartan stele recording the names of those who fell at Thermopylae in 480 see Pausanias, *Description of Greece*, 3.14.1; Herodotus, *Histories*, 7.224.1; on the inscribed monument which the Lacedaemonians erected to mark the site of the regent Pausanias' reburial see Thucydides, *History of the Peloponnesian War*, 1.134.4, and Pausanias, *Description of Greece*, 3.14.1).¹⁵³ In fact, from surviving inscriptions it becomes clear that the Spartans produced a number of public documents on a variety of subjects, and possibly even stored them in a rudimentary archival system (as suggested by Boring and Millender).¹⁵⁴ We see, for example, an inscription that lists the winners of games at the *Leonidea* – a Spartan festival in honour of the legendary king Leonidas (*Inscriptiones Graecae*, V.1: *Lakonia and Messenia*, 1.20, cf. 1,18-19; see also: Plutarch, *Life of Agesilaus*, 19.10; Plutarch, *Moralia*, 1116f; Tacitus, *Annals*, 4.43); two inscriptions containing lists of contributions to the Spartan war fund during the Peloponnesian war (*Inscriptiones Graecae*, V.1: *Lakonia and Messenia*, 1.219); and two 5th century BCE contracts inscribed on a bronze tablet (*Inscriptiones Graecae*, V.1: *Lakonia and Messenia*, 2.159). What is more, the Spartans appear to have been in possession of written collections of Delphic oracles by at least the end of the 6th century BCE.¹⁵⁵ Ancient evidence recording Sparta's alliances in the Greek world and beyond also testifies to the practical literacy of Spartans. One such – a treaty between Sparta and the Erxadieis (a branch of the Aetolians) known as the 'Spartan-Aetolian treaty' (*Supplementum Epigraphicum Graecum*, 26.246) – dates back to around 420 BCE.¹⁵⁶ At least two inscribed

¹⁵³ *Inscriptiones Graecae*, V.1: *Lakonia and Messenia*; *Laconia Survey Inscriptions Catalogue*, *Laconia Survey Project*; Cartledge 2003 (I & II); Christidis, Arapopoulou & Chrite 2007; Hodkinson & Powell 2009; Hondius & Woodward 1919-1921, 88-143; Kennell 2010; Powell 2017; Tod 1933, 108-111.

¹⁵⁴ Boring 1979, 19-36; Millender 2001, 127.

¹⁵⁵ Parke & Wormell 1956 (see esp. nos. 1.82-98 for evidence concerning links between Delphi and Sparta, especially in connection with the dual kingship in Sparta).

¹⁵⁶ Bengtson 1975; Boring 1979; Millender 2001, 130-131; Peek 1974; Wolicki 2018, 21-30.

copies of such treatises have partially survived.¹⁵⁷ In fact, it is highly likely that there were once many more (now lost) Spartan inscriptions related to a variety of private and public events. Many Spartan documents would have been written on perishable materials such as wood, leather, or papyrus that have not survived. Millender, therefore, argues on the basis of the available evidence that we should not assume that the Spartans wrote very little, but that we should instead consider the existence of a great number of ‘now lost inscriptions’ from Sparta.¹⁵⁸ In fact, it has been argued that literacy skills – however basic – were even necessary for a full Spartan citizen, because of the Lacedaemonians’ frequent conduct of warfare and diplomacy.¹⁵⁹ The evidence discussed above therefore proves that the Spartans were certainly not completely illiterate, even if the true extent of literacy in Sparta as, indeed, in the ancient Greek world as a whole, is much debated.¹⁶⁰

Most of the relevant sources on the Spartan *scytale* discussed in this thesis come from non-Spartan (Athenian) sources from the 5th and 4th centuries, a period in which anti-Spartan sentiment must have been high amongst the Athenians because of the Peloponnesian War. This Athenian influence upon the picture of supposed Spartan illiteracy matters, because Athens prided itself in its own sophisticated literacy. The first book culture in the world – with various Athenian sources offering multiple references to book sellers and reading – developed in Athens in the second half of the 5th century BCE (Aristomenes Fragment 9; Eupolis, Fragment 327; Nicophon, Fragment 10; Theopompus, Fragment 79, all in Kassel and Austin *Poetae Comici Graeci*; Aristophanes, *Frogs*, 52f; Euripides, Fragment 369 in

¹⁵⁷ *Inscriptiones Graecae*, V.1: *Lakonia and Messenia*, 3; Bengtson 1975; Boring 1979; Millender 2001, 130-131; Peek 1974; Wolicki 2018, 21-30.

¹⁵⁸ Millender 2001, 138.

¹⁵⁹ Millender 2001, 159.

¹⁶⁰ See e.g.: Bodel 2001, 61; Cartledge 1978; 2001; 2013-II; Harvey 1966, 585-635; Hodkinson & Powell 2009; 2010; Millender 2001; Mintz 2018; Schrader 2011, 501; Too 2001, 69.

Tragicorum Graecorum Fragmenta; Plato, *Apology*, 26d-e).¹⁶¹ Large numbers of inscriptions from this period and later sources suggest that written documents also seem to have been widely used in Athens – and potentially in other cities as well – from the 5th and 4th century BCE onwards in public, private, monumental, commemorative and administrative contexts.¹⁶² Yet, again we have to be cautious when putting a date to literacy in Greece since this idea of the more widespread literacy in Greece from the 5th/4th century BCE is simply based on the large number of surviving texts from this period. Ceccarelli argues that from the Hellenistic period reading and writing were an important and central part of daily life in the ancient world throughout all levels of society.¹⁶³ However, despite multiple investigations, there is still no unanimous scholarly agreement on the degree of literacy achieved by all the Greeks in the late archaic and classical periods.¹⁶⁴ The question of whether or not Spartan society in these periods was broadly literate remains vexed. Indeed, in contrast to Athens with its seemingly common use of written documents for political, business, social, education, and all kinds of other activities, the extant sources include Spartan *illiteracy* as part of the stereotypical idea of Sparta being different from other city-states (especially Attica) – and Athenians certainly supposed the Spartan society to possess a very low level of literacy in comparison with their own. Hereby, according to (Athenian) tradition, the Spartans had no historical records, literature, or written laws – as was expressly prohibited by an ordinance of the lawgiver Lycurgus who supposedly lived and set up the Spartan Constitution (the Great Rhetra) in the 9th century BCE (Cicero, *On the Republic*, 2.10; Plutarch, *Comparison of*

¹⁶¹ O’Sullivan 1995, 115.

¹⁶² Harvey 1966, 624; Liddel 2018, 124; Rösler 2009, 436-437.

¹⁶³ Ceccarelli 2013, 2.

¹⁶⁴ See for studies on the spread and extent of literacy in ancient Greece e.g.: Boring 1979; Cartledge 1978; Ceccarelli 2013; Clanchy 1979; Goody 1986; Goody & Watt 1968; Harris 1989; Havelock 1963; 1982; Harvey 1966; Immerwahr 1990; Johnson & Parker 2009; Pébarthe 2006; Sickinger 1994; 2018; Steiner 1994, 4; Street 1984; Thomas 1989; Trapp 2003; Turner 1952.

Lycurgus and Numa, 4; *Life of Agesilaus*, 31; *Life of Lycurgus*, 7; 29; Thucydides, *History of the Peloponnesian War*, 1.18). According to Plutarch:

Νόμους δὲ γεγραμμένους ὁ Λυκοῦργος οὐκ ἔθηκεν, ἀλλὰ μία τῶν καλουμένων ῥητρῶν ἐστὶν αὕτη. τὰ μὲν γὰρ κυριώτατα καὶ μέγιστα πρὸς εὐδαιμονίαν πόλεως καὶ ἀρετὴν, ἐν τοῖς ἥθεσιν ὤετο καὶ ταῖς ἀγωγαῖς τῶν πολιτῶν ἐγκατεστοιχειωμένα, μένειν ἀκίνητα καὶ βέβαια, ἔχοντα τὴν προαίρεσιν δεσμὸν ἰσχυρότερον τῆς ἀνάγκης (Plutarch, *Life of Lycurgus*, 13.1)

None of his [Lycurgus's] laws were put into writing by Lycurgus [...] For he thought that if the most important and binding principles which conduce to the prosperity and virtue of a city were implanted in the habits and training of its citizens, they would remain unchanged and secure, having a stronger bond than compulsion.

Perpetuating these stereotypical, mythical ideas about Sparta having unwritten laws and the Spartans being mostly illiterate, Isocrates, in his *Panathenaicus* – written about 340 BCE – claimed that the Spartans were even more backward than barbarians. He argued that, while some barbarians had been pupils of more civilised cultures (such as Athens) and even occasionally their teachers, the Spartans had fallen so far behind civilised Greek culture and learning that they would not even know how to instruct themselves ‘in letters’ (meaning, in this context, in reading and writing) anymore (Isocrates, *Discourses* 12: *Panathenaicus*, 209). As Harris argues, the word that Isocrates (and other Greeks) used to describe the supposed illiteracy of the Spartans – *αγράφματος* (*agrammatos*), literally ‘illiterate’ – also seems to have meant ‘ignorant’, ‘uneducated’ or ‘uncultured’.¹⁶⁵ We also see this in Xenophon’s *Memorabilia* where the author seems to have meant a lack of culture when using the word *αγράφματος* to describe the Spartans (*agrammatos*; Xenophon, *Memorabilia*, 4.2.20). Aristotle even uses the word when speaking about animals – whereby the word meant ‘unable to utter articulate sounds’ which again seems to refer to the idea of an *agrammatos* (either human or animal)

¹⁶⁵ Harris 1989, 5-6.

being uncivilised (Aristotle, *The History of Animals*, 1.1.488a33).¹⁶⁶ And indeed, as Havelock points out, Greeks in the Classical period seem to have distinguished with relatively broad strokes between ‘literate/educated’ and ‘illiterate/uneducated’ people.¹⁶⁷ In fact, the Romans also seem to have adopted this view. In the Roman period the idea of ‘not knowing letters’ (*litteras nescire*) still seems to have referred more to a lack of culture than to actual illiteracy (see e.g.: Caecilius Statius, in: *Comicorum Romanorum Fragmenta* (ed. Ribbeck), 2.51 (line 60); Cato the Elder, *Origins*, Fragment 31; Cicero, *On the Orator*, 2.6.25; Seneca the Elder, *Suesoriae*, 7.13; Seneca the Younger, *On Benefits*, 5.13.3).¹⁶⁸ The idea of the Spartans being both illiterate and uneducated as an enduring Athenian stereotype is further supported by an account of Plutarch, who stated that it was Lycurgus who had originally decreed that, in order to develop themselves physically, the Spartans had to give up on their mental or intellectual development (Plutarch, *Life of Lycurgus*, 16). Finally, as Boring argues, it is not until the beginning of the 2nd century BCE that evidence for literacy in Sparta becomes more abundant and Athenian authors appear to accept that their Spartan neighbours might be more educated and cultured than previously understood or accepted.¹⁶⁹ This prevailing (Athenian) mythology concerning the relative lack of culture of the Spartans in the classical period (although grounded in the tradition that decreed the Spartans did not have written laws and upon the Spartan focus on physical rather than intellectual development) resulted in a predominant trend for other Greeks (especially Athenians) to see the Spartans not only as barbaric and illiterate, but also (perhaps even consequently) as secretive and different. With this mythical idea in mind, Campbell states that the Spartans were famous – or better still – notorious for their (physical) military deeds – while Melville and Melville argue that during the siege of Plataea

¹⁶⁶ Harris 1989, 6.

¹⁶⁷ Havelock 1982, 41.

¹⁶⁸ Harris 1989, 6.

¹⁶⁹ Boring 1979, 81.

the Spartans only used clumsily built and incomplete blockades since the Spartans were unable to build anything better.¹⁷⁰ Yet, as Rundle Clark points out, myth belongs to a way of thinking in which logical sense is irrelevant – myths do not necessarily represent real life.¹⁷¹ The same applies to stereotypes. The reality of Spartan literacy, therefore, is not necessarily represented by the prevailing myths and stereotypes. The Spartans in the 5th and 4th centuries BCE were obviously not completely illiterate, nor were they entirely ignorant or uneducated. Herodotus (as we saw in the previous chapter) describes the Spartans' sending and receiving of messages (Demaratus' letter; Herodotus, *Histories*, 7.239), and Plutarch argues that, although the Spartans did not learn to read and write for leisure (as the Athenians did), the Spartans did learn some literacy basics for *practical* reasons (*Γράμματα ἔνεκα τῆς χρείας ἐμάνθανον [...] They learned to read and write for purely practical reasons*; Plutarch, *Moralia: The Ancient Customs of the Spartans*, 4).¹⁷² Indeed, as Thomas argues, the purpose of learning to read and write has to be relevant to its users and to the contexts in which such literacy skills may be put to use, otherwise literacy cannot take root in a society, while Powell adds that writing in antiquity was never a scientific device, as we see it now. Instead, it was a tool only designed for practical ends by practical people.¹⁷³ Obviously, the practical reasons to learn to read and write are always different for everyone depending on the context of their situation and background. For the Spartans, for example, being able to read and write their names, as well as being able to read and write other simple messages in a variety of practical contexts (such as those relating to inscriptions) would probably have been sufficient – as illustrated by the simple votive inscriptions found at the 'Menelaion' and other Spartan archaeological sites. For a Spartan, then, having the literacy skills necessary to send and read a *scytale* message – would have been

¹⁷⁰ Campbell 2006, 37; Melville & Melville 2008, 157-158.

¹⁷¹ Rundle Clark 1959, 263.

¹⁷² Chadwick 1987, 11; Harris 1989, vii; O'Sullivan 1995, 115; Thomas 1995, 183.

¹⁷³ Powell 1997, 4; Thomas 2009, 13. See also Cartledge 1978.

just as useful as knowing how to sharpen a sword.¹⁷⁴ Thus, although some non-Spartan sources seem to perpetuate the belief that the Spartans were illiterate, barbaric, uncivilised, and uneducated (Plato, *Greater Hippias*, 284-285; especially 285c; Plutarch, *Life of Lycurgus*, 13.1) a range of other ancient sources signal a connection between Spartans and literacy in the context of messaging or keeping records – in which context these sources typically and significantly highlight the use of some kind of *scytale* (Aristophanes, *Birds*, 1280-1285; *Lysistrata*, 985-992; Athenaeus of Naucratis, *The Learned Banqueters*, 10.451d; Diodorus Siculus, *Library of History*, 8.27; 13.106.8-9; Nicophon, *The Birth of Aphrodite* (*The Fragments of Attic Comedy* 1 (Fragment 2)); Pindar, *Olympian Odes*, 6.90-92; Photius, *Lexicon*, entry: σκυτάλη (I and II); Plutarch, *Life of Agesilaus*, 10; 15; *Life of Alcibiades*, 38; *Life of Artaxerxes*, 6; *Life of Lysander*, 19; 20; Polyaeus, *Stratagems of War*, 1.17; Theophrastus, *Nomoi*, fragment from *Biblioteca Apostolica Vaticana*; *Vat. Gr. 2306*; Thucydides, *History of the Peloponnesian War*, 1.131.1; Xenophon, *Hellenica*, 3.3.8; 5.2.33-37; see § 2.4). According to these sources, *scytalae* could have been used in a variety of contexts and for a variety of purposes. These would have included giving a messenger formal authentication as we find in Pindar's odes:

ἔσσι γὰρ ἄγγελος ὀρθός, ἡνυκόμων σκυτάλα Μοισᾶν (Pindar, *Olympian Odes*, 6.90-92)

for you are a true messenger, a message stick [*scytale*] of the fair-haired Muses

The 'illiterate' Spartans were, it seems, perfectly able to read and to write and to use their skills in literacy (however basic) to communicate effectively in a variety of *practical* contexts. Indeed, we see this apparent contradiction between (Athenian) stereotype and (Spartan) reality already reflected in Herodotus' treatment of the Spartans. After the

¹⁷⁴ Boring 1989, 63. A society in which the majority of people cannot write more than their own name is known as a 'semi-literate' society (Havelock 1971, 14; Havelock 1982, 59; Turner 1973; Youtie 1971, 239-261). See on inscriptions from Sparta e.g.: Cartledge 2003 (I & II); Christidis, Arapopoulou & Chrite 2007; Hodkinson & Powell 2009; Hondius & Woodward 1919-1921, 88-143; Kennell 2010; Powell 2002; 2017; Tod 1933, 108-111.

Peloponnesian War and the Athenian defeat, when we might expect anti-Spartan sentiment to have been particularly high, and negative myths and stereotypes relating to Sparta to have flourished in Athens, we find Herodotus relating as history a story related to ‘barbaric’ Sparta – and to the overthrowing of oriental and ‘other’ despotic regimes (see § 1.2.6). As we saw in the preceding chapter, according to Herodotus, writing around 440 BCE, Demaratus sent a secret letter to the Spartans to warn them about the Persian invasion around 480 BCE (§ 1.2.5; Herodotus, *Histories*, 7.239) – hereby making a salient connection between Spartans and their characteristic secrecy. However, his account also (necessarily) assumes a connection between the Spartans and letter writing – that is, an acknowledgement of their literacy.

After Herodotus, other Greek sources – especially Athenian sources – in the 5th and 4th centuries BCE followed up on this Herodotean idea of the Spartans and their connections to secrecy and to secret writing (see e.g.: Plato, *Laws*, 1.633b-c; 6.763b; a *Scholia on Plato’s Laws*, 1.633b-c; 6.763b; Ed. De Forest Allen, Burnet, et al.).¹⁷⁵ According to such sources, non-Spartans seemed to have believed that the Spartans probably did not write all that often, but when they wrote letters or needed to communicate over any distance, they used a strange and secretive *scytale* device for writing and sending their messages (see § 2.3 and 2.4). And thus, we can dismiss the ‘myth’ of Spartan ‘illiteracy’ from our investigation into the question of whether the Spartan *scytale* would and could have been a useful device for secret communication in the ancient world. Those historians of cryptography who see the Spartans as illiterate ‘barbarians’ base their interpretation of Spartan society – and thereby the likelihood or otherwise that Spartan society might have used the *scytale* for secret communication – upon selective and biased ancient sources, as well as upon now outdated scholarship. We can therefore look again at the role of the *scytale* as a device for secret

¹⁷⁵ Cartledge 2003, 70; De Forest Allen, Burnet, et al. 1938; Ross 2012.

communication and investigate what the ancient Greek sources (mindful of their biases and limitations) have to tell us.

2.3: The *scytale* in non-Spartan sources

2.3.1: Archilochus of Paros (7th century BCE)

The first thing that strikes us when we take a comprehensive survey of the extant sources which discuss the Spartan *scytale* is the great variety of different devices and artefacts to which the label *scytale* seems to apply. The second significant discovery we make is the fact that, although most ancient Greek sources discuss the *scytale* in the context of messaging or communication of some kind, very few sources directly or unambiguously link the *scytale* to any type of *secret* communication.¹⁷⁶

In a passage from *The Learned Banqueters*, Athenaeus of Naucratis who wrote in the late 2nd/early 3rd century CE reported that Apollonius of Rhodes had referred to the *scytale* as a Spartan cryptograph in his *Treatise On Archilochus* on the 7th-century BCE poet Archilochus of Paros:

Σπαρτιᾶτιν σκυτάλην. ὅτι δὲ λευκῷ ἱμάντι περιειλοῦντες τὴν σκυτάλην οἱ Λάκωνες ἔγραφον ἃ ἠβούλοντο, εἶρηκεν ἱκανῶς Ἀπολλώνιος ὁ Ῥόδιος ἐν τῷ Περὶ Ἀρχιλόχου (Athenaeus of Naucratis, *The Learned Banqueters*, 10.451d; for the complete passage see Appendix 1, page 265-266)

[that the] Spartans wrapped their message-staffs in white thongs and wrote what they wanted on them, Apollonius of Rhodes discusses this at length in his *On Archilochus*.

¹⁷⁶ If some of the Spartans' contemporaries believed a *scytale* had only non-cryptographic uses, this would be to the Spartans' benefit. It would have been valuable disinformation.

Based on this passage some modern historians of cryptography see Archilochus as the first ancient writer to make reference to the *scytale* as a means of secret communication.¹⁷⁷ Yet, this claim cannot be made with any certainty for various reasons. Firstly, Archilochus' original work has not survived, nor has Apollonius of Rhodes' *Treatise on Archilochus* – the reputed second-hand (3rd century BCE) source for this attribution to Archilochus, which appears only at third-hand in a work by Athenaeus of Naucratis written in the late 2nd/early 3rd century CE. Ceccarelli argues that Athenaeus – and, therefore, Apollonius and potentially also Archilochus – here described an obscure and enigmatic mode of writing related to the Spartans.¹⁷⁸ Yet, this interpretation cannot be derived from Athenaeus' passage since nothing in the text indicates that *secret* messages were meant in this context. However, it is plausible that Archilochus might well have discussed the *scytale* as a cryptograph in Apollonius' source or any other source, because he appears to do the same in a fragment from Archilochus that has survived in the work of Herennius Philo. Here, Archilochus does appear to have had some cryptographic form of the *scytale* in mind (*On the Different Meanings of Words; Greek Iambic Poetry: From the Seventh to the Fifth Centuries BC*; Fragment 185). According to this source, he described the *scytale* as a sort of messenger-stick use for authentication – to give the speaker the right to speak – an idea also suggested by Bowie.¹⁷⁹

ἐρέω τιν' ὅμιν αἶνον, [...] ὄχθυμένη σκυτάλη (*On the Different Meanings of Words; Greek Iambic Poetry: From the Seventh to the Fifth Centuries BC*; Fragment 185)

A grieving message stick, I shall tell you people a fable

¹⁷⁷ Boring 1979, 40; Kelly 1998, 246; West 1988, 42.

¹⁷⁸ Ceccarelli 2013, 238-239.

¹⁷⁹ Bowie 2019, 284. See also Swift 2019.

As shown in the quotation, Gerber translates this as ‘a grieving message stick’ (ἀχνυμένη σκυτάλη).¹⁸⁰ Quite what a ‘grieving’ stick of any variety might look like is hard to imagine here but the word ‘grieving’ potentially refers to one of the *scytale*’s functions, namely to identify fallen soldiers on the battlefield – as will be discussed in more detail in § 2.3.9 on the Greek historian Ephorus (Diodorus Siculus, *Library of History*, 8.27; *Excerpta Constantiniana* 4; Polyaeus, *Stratagems of War*, 1.17). Yet, another possibility is that the word ἀχνυμένη in this context should not be translated as ‘grieving’ or ‘mourning’ but as ‘vexing’ or ‘annoying’ (see offered by the *LSJ*).¹⁸¹ This invites the interpretation that the messenger-stick in question is puzzling or perplexing in some way, perhaps because the message it contains is encrypted or encoded and therefore difficult to read for anyone without the means to decode its cipher. This is an intriguing possibility, but is far from clear-cut as a description of the *scytale* as an ancient cryptographic device. In this context the *scytale* could have been a messenger stick, a baton bearing incisions and functioning as an aide-mémoire for the messenger, or the vehicle for a Spartan non-secret message.¹⁸² What is more, many of Athenaeus’ sources were fictitious and anecdotal (as, significantly, Ceccarelli himself points out) – making it difficult to use Athenaeus as a reliable source here.¹⁸³ On the basis of the evidence that is available to us, we may logically say only that Apollonius referred to the *scytale* in the context of messaging and communication before Athenaeus did so; and that Archilochus probably – yet not provably – referred to the *scytale* in the same context earlier still in a now lost passage. The assumption that these early references to the *scytale* unambiguously indicate its use in *secret* messaging and communication would seem to be unjustified.

¹⁸⁰ Gerber 1999, 201.

¹⁸¹ Liddell & Scott Greek-English Lexicon, entry ἄχνυμαι..

¹⁸² Ceccarelli 2013, 32.

¹⁸³ Ceccarelli 2019, sv.v: Athenaios (166); Autokrates (297).

2.3.2: Pindar (5th century BCE)

Thus, although we cannot be certain on the basis of the extant evidence whether or not Archilochus of Paros refers to a *scytale* in the context of secret communication or merely as a device used in the context of messaging for the first time in the 7th century BCE, the Theban poet Pindar certainly refers to the *scytale* in a non-cryptographic messaging context in the 5th century BCE. It becomes clear from his sixth *Olympian Ode* that a *scytale* was used as a sort of messenger-stick – as heralds or bards would have – whereby the stick would give the bearer the chance and right to speak:

ἔσσι γὰρ ἄγγελος ὀρθός,

ἠυκόμων σκυτάλα Μοισᾶν,

γλυκὺς κρατὴρ ἀγαφθέγκτων ἀοιδᾶν (Pindar, *Olympian Odes*, 6.91-93; see also page 93)

for you are a true messenger,

a message stick of the fair-haired Muses,

a sweet mixing bowl of loudly ringing songs.

In Pindar's passage the *scytale* is clearly not used for sending secret messages. On the contrary, the context makes it clear that here a singer – holding the *scytale* or messenger stick – is thereby given the opportunity to praise an Olympian victor.¹⁸⁴ Although Race – in his translation of Pindar – translates the word *σχυτάλη* (*scytale*) as 'message stick', he then – in a note – refers to the Spartans' use of the *scytale* as a cryptographic device.¹⁸⁵ This dual reference (by Race) seems to suggest that Pindar's singer may have meant to communicate a secret message here – but this is not authorised by the text. While Boring seems to believe that Pindar indeed meant

¹⁸⁴ In a similar performance context, Archilochus – in Fragment 185 – also appears to describe the *scytale* as a messenger stick, although, here the speaker was about to tell a fable.

¹⁸⁵ Race 1997, 114-115.

a secret *scytale* message here, he argues that although Pindar said nothing about the *scytale* being used for secret communication in this passage, it shows his awareness of the existence of the common use of *scytalae* for the purpose of secret communication.¹⁸⁶ However, it seems clear that the *scytale* in Pindar's ode has no cryptographic associations and is simply the referent for a symbolic stick or staff.

2.3.3: Aristophanes (late 5th/ early 4th century BCE)

2.3.3.1: Birds

The comic poet Aristophanes, who was active in the late 5th to early 4th century BCE – provides our first Athenian source for the *scytale*. Aristophanes used the word twice in his plays. The word first appears in his *Birds*, where a herald tells the Athenian Peisetaerus that once upon a time, before Athens became civilised, all Athenians would behave like the barbaric Spartans (cf. Herodotus, *Histories*, 6.58-60 in which Herodotus described the Spartans as barbaric and ‘non Greek’; see also introduction to chapter 2). They would – for example – wear their hair long, never bath themselves, and brandish batons (*scytalae*) to threaten their enemies or simply to show their anger or excitement (Aristophanes, *Birds*, 1280-1285; for the complete passage see Appendix 1, page 264). Indeed, the 1st-century BCE grammarian Didymus points out in his ancient commentary on the *Birds* that a *scytale* was simply a stick carried about by Spartan commanders, which may have been used to strike an enemy or person of lower rank (*Didymi Chalcenteri Grammatici Alexandrini*, Fragment 1283-1284).¹⁸⁷ It is likely, then, that Aristophanes wanted his audience to think that the Spartans were carrying big phallic sticks for

¹⁸⁶ Boring 1979, 39.

¹⁸⁷ According to the *Scholia on Aristophanes' Birds* this is also mentioned by the 4th-century CE Roman author Symmachus – an author not discussed by Kelly or West (*Scholia on Aristophanes Birds*, 1283-1284; Edition: White 1914, 228).

no reason other than to look fashionably rugged and manly. Indeed, as Boring, Piccirilli and Sommerstein point out, Aristophanes probably referred here to a distinctive type of walking-stick with a twisted and knobbed end that is known from ancient Sparta – rather than referring to the Spartan cryptographic practice of sending *scytale* messages.¹⁸⁸ According to the scholarship on this topic, Spartans often used such walking-sticks, as did upper-class Athenians who aped Spartan ways – in comedy and in real life.¹⁸⁹ Thus, the passage is not a reference to *scytalae* being used for sending messages (secret or otherwise) per se. However, according to Sommerstein, the passage might show that the Athenians were familiar with *scytalae* in the context of their use for communicating ‘official Spartan dispatches’ – whether these were secret dispatches or not.¹⁹⁰ Although Jeffery does allow for the possibility that the Spartans used *scytalae* for the purposes of secret communication, there are some flaws in her argument. In her 1990 publication *The Local Scripts of Archaic Greece* she suggests that writing messages on leather rolls, and then winding them round a stick for transport (as might have been the case here) had once been common practice in archaic Greece, and that it is likely that in using the *scytale* for secret communication the Spartans were merely retaining this practice.¹⁹¹ However, the practice that Jeffery describes seems to be the opposite of how the Spartans actually used *scytalae* for sending secret messages. In Jeffery’s example, a message is first written on some writing material, like a strip of parchment, and only then wrapped around a *scytale* for easy transport – something that will also be discussed as a possibility in the analysis of the passages from Nicophon’s *Birth of Aphrodite* (*The Fragments of Attic Comedy* 1, Fragment 2), and

¹⁸⁸ Boring 1979, 41; Piccirilli 1981, 5; Sommerstein 1987, 283; 1990, 205; 2002; 236.

¹⁸⁹ Aristophanes, *Lysistrata*, 985-991; Boring 1979, 41; Sommerstein 1987, 283; 1990, 205; 2002; 236.

¹⁹⁰ Boring 1979, 41; Sommerstein 1990, 205. We also see this in Plutarch’s 2nd-century CE description of the *scytale* where Plutarch discussed that the stick as well as the (official) dispatch bore the same name: ‘*scytale*’ (*Life of Lysander*, 19.7).

¹⁹¹ Jeffery 1961, 57.

Thucydides' *History of the Peloponnesian War* (1.131.1). However, in using the *scytale* for sending secret messages, the ancient evidence suggests that the Spartans first wrote their message on the writing material that was *already* wrapped around the *scytale*, and then *unwrapped* it before it was sent away (possibly wound around yet another *scytale* rod for transportation). To decode the encrypted message, the recipient re-wrapped the material around a second (or third) *scytale* rod (which would have needed to be exactly the same diameter as the original to make easy decryption possible). Therefore, Jeffery might be correct in theorising that the Spartan *scytale* retains some element of an archaic Greek tradition involving the transportation of messages written on strips of leather and wrapped around a ceremonial staff of some kind – but there are crucial differences in the two practices. Indeed, it is noteworthy that Jeffery's theory aligns the Spartan *scytale* with an *archaic* (that is, an early, relatively primitive) practice for messaging in ancient Greek societies – perpetuating the Athenian stereotype of Sparta as a relatively primitive, backwards, and uncivilised society. It thereby potentially obscures the idea that the Spartan *scytale* might represent a development and evolution upon this earlier Greek tradition for messaging – downplaying the possibility that the *scytale* might also have been used for other, more sophisticated, types of (secret) communication.

Hornblower – who does believe that *scytalae* were used as cryptographic devices – points out that sticks in ancient Greece (*scytalae*), gave their bearer clear and visible power over other people, for example, to violate one's subordinates (as later in the Roman army an *optio*, acting as deputy of a *centurion*, carried a stick with which to keep the troops in order),¹⁹² but also to show symbolic power (as sceptres do for kings and queens).¹⁹³ The use of the *scytale* as a cryptographic device, he states, clearly illustrates that the Spartans had this feeling of

¹⁹² Rankov 2007, 41

¹⁹³ Hornblower 2009, 64-65.

physical and symbolic power that sticks would give their bearers and that they knew how to use it:

[the] *skytale* [was] used by high-ranking Spartans to send messages wrapped round a stick. The specifically Spartan use of a stick to send messages in this way nicely illustrates the evident Spartan feeling that a stick was good for saying things with.¹⁹⁴

Although Piccirilli did not discuss the *scytale* as a cryptographic device, he seems to agree with Hornblower on this point of physical and symbolic power when arguing that the *scytale* was the weapon par excellence of an archaic fighter and a symbol of strength (*l'arma per eccellenza del combattente arcaico e simbolo di forza*) – a point similarly made by Eliade.¹⁹⁵ Nevertheless, it is impossible to determine from this source whether or not the *scytale* in Aristophanes' *Birds* refers to a staff or baton, a walking stick, or a 'dispatch stick' – yet it seems unlikely, in either case, that any secret messaging is associated with its function in this context.

2.3.3.2: *Lysistrata*

A second passage in which Aristophanes used the word *scytale* (twice) can be found in the *Lysistrata* (985-992; for the complete passage see Appendix 1, page 264-265) – which, like *Birds*, is set in Athens. In this passage the Athenian magistrate Cinesias asks a Spartan messenger what he has hidden under his cloak. The messenger assures him that he is not hiding a weapon, but is instead carrying a 'Spartan walking stick' (*scytale*; 991). Cinesias – whom the herald is addressing – then assures him that he understands the problem, since he sometimes has a 'Spartan walking stick' too (992). The tone of the passage clearly suggests that the messenger is trying to hide a phallus, which he and Cinesias here euphemistically call a

¹⁹⁴ Hornblower 2009, 61.

¹⁹⁵ Eliade 1970, 20; Piccirilli 1981, 6. When used as a cryptographic device *scytalae* indeed gave power to both the sender and the recipient, not clear visible power that could have been used for violent purposes, but an invisible power since only the sender and recipient understood each other's messages.

‘Spartan walking stick’. As in the *Birds*, Aristophanes here mocks the unsophisticated (barbaric) Spartans. And again, this is not a reference to secret communication. Boring, therefore, seems in error when arguing that this passage offers evidence of the *scytale* being used for the purpose of secret communication.¹⁹⁶ Yet, although the herald in this case may be trying to hide an erect phallus, the reference to the *scytale* in this context might also be a reference to a walking stick (as in the previous passage) or to an official messenger stick (used as a sort of authentication device) as suggested by Anderson and West.¹⁹⁷ And again, although it is impossible to determine from this source whether or not the *scytale* in Aristophanes’ *Lysistrata* refers to a staff or baton, a walking stick, a ‘dispatch stick’, or a phallus, it seems unlikely that any secret messaging is associated with its function.

2.3.4: Nicophon (4th century BCE)

Nicophon – an Athenian playwright and near contemporary of Aristophanes – also referred to a *scytale* in his play *The Birth of Aphrodite*. Very few fragments from this comedy have survived, but one very short fragment in which the word *scytale* appears is collected in Edmonds’s *The Fragments of Attic Comedy* 1 (Fragment 2). In the fragment – which is only one sentence long – a figure urges another figure to let go of their *scytale* and parchment and wishes the other figure to go to hell (οὐκ ἐς κόρακας τὸ χεῖρ’ ἀποίσεις ἐκποδὼν ἀπὸ τοῦ σκυταλίου < > καὶ τῆς διφθέρας). Only a few commentaries and translations are available in which this passage is discussed. Edmonds – in his 1957 translation in *The Fragments of Attic Comedy* – translates the sentence as: *Let go the stick [scytale]-and-parchment and to hell with you!* (see also Kassel and Austin).¹⁹⁸ The translation of the words σκυταλίου < > καὶ τῆς

¹⁹⁶ Boring 1979, 39.

¹⁹⁷ Anderson 1970, 68; West 1988, 43-44.

¹⁹⁸ Edmonds 1957, 935; Kassel & Austin 1989, 64.

διφθέρας as ‘stick-and-parchment’ suggests a reference to the Spartan practice of either wrapping letters or dispatches around a *scytale* for transport as Jeffery suggests, or to the practice of using them to communicate secret messages.¹⁹⁹ However, Storey in his 2011 translation of *Fragments of Old Comedy*, translates the sentence as: ‘*Why don’t you take your hands off the [“my”?] staff and jacket and go to hell?*’, implying that the person who was being cursed was holding the other person’s cloak.²⁰⁰ However, the word ἱμάτιον (*himation*) was more commonly used to describe a cloak or coat in ancient Greece (see e.g.: Aristophanes, *Ecclesiazusae*, 333; Demosthenes, *In Timocratem*, 24.114; *De Falsa Legatione*, 19.314; *Inscriptiones Graecae*, 22.1524.205) – while according to Herodotus, paper or parchment was sometimes referred to as ‘skin’ as it was made from animal skin (*Histories*, 5.58) – an argument in favour of Edmonds’ translation of a ‘stick-and-parchment’. Since the passage is only one line long and completely out of context it is very hard to reconstruct what Nicophon may have meant. Kelly presumes that nothing in the passage directly refers to *scytalae* being used as cryptographic devices and, therefore, asserts that Nicophon does not have secret communication in mind here.²⁰¹ However, absence of evidence is not evidence of absence, and nothing about the *scytale* in this source can be said with any certainty based on the evidence provided.

2.3.5: Thucydides (2nd half 5th century BCE)

Although the earliest sources on the *scytale* are highly ambiguous, offering little concrete evidence on whether or not the *scytale* was used for secret communication, the Athenian historian Thucydides in the second half of the 5th century BCE ostensibly offers a slightly

¹⁹⁹ Edmonds 1957, 935; Jeffery 1961, 57.

²⁰⁰ Storey 2011-I, 401.

²⁰¹ Kelly 1998, 248.

clearer picture. In chapter 1.131 of the *History of the Peloponnesian War* Thucydides discussed how the Spartans summoned their general Pausanias home, because of misbehaviour – by sending him a *scytale* message. After being dislodged from Byzantium by the Athenians, instead of returning home, Pausanias had settled in the Troad (Anatolia) where he was tarrying for no purpose and intriguing with local inhabitants – who Thucydides calls ‘barbarians’ (Thucydides, *History of the Peloponnesian War*, 1.131.1; compare with Herodotus *Histories*, 6.58-60) – when he received a *scytale* summoning him home (Thucydides, *History of the Peloponnesian War*, 1.131.1). Smith in his translation of the work translates the word as ‘*scytale* message’, while Hammond translates it as ‘dispatch-stick’.²⁰² Both scholars then align these references to the Spartan practice of using a *scytale* as a cryptograph, whereby Smith explicitly describes the *scytale* as a special staff used to send cryptographic messages.²⁰³ Rhodes and Lattimore simply use the word ‘*scytale*’ in their translations.²⁰⁴ Rhodes adds that the *scytale* stick was not used as a cryptograph in this context, but for easy transport of a dispatch instead (see also Jeffery), while Lattimore (aptly) points out that it is unclear how the *scytale* as message stick would have worked or how a stick (as opposed to a bag, say) would have made transporting a written message easy.²⁰⁵ Yet, in a commentary on Thucydides Andrewes argues that in the letters and situations that Thucydides describes, it must be assumed that secret communication – in this case *scytale* messages – was commonly used.²⁰⁶ However, although it is clear that the Spartan *scytale* discussed in Thucydides’ passage conveyed some kind of official dispatch and message, and although it is plausible that a coded letter – a *scytale* message – was sent (because of the politically and military sensitive content and intent of the

²⁰² Hammond 2009, 63; Smith 1919, 220-221.

²⁰³ Hammond 2009, 63; Smith 1919, 220-221.

²⁰⁴ Lattimore 1998, 63; Rhodes 2014, 161; 271.

²⁰⁵ Jeffery 1961, 57; Lattimore 1998, 63; Rhodes 2014, 161; 271.

²⁰⁶ Andrewes 1981, 120, in: Gomme, Andrewes & Dover 1981.

letter), since the passage is not a complete and clear description of the use of the *scytale* as a cryptographic device we cannot tell whether the *scytale* in this case was used for the purpose of secret communication.

2.3.6: Xenophon (late 5th/ early 4th century BCE)

2.3.6.1: Hellenica 3.3.8

The next source is once more Athenian: Xenophon's *Hellenica* – written in roughly the same period as Aristophanes' and Thucydides' work (late 5th to early 4th century BCE) – in which the word *scytale* is used four times. The first two references to the word can be found in *Hellenica* 3.3.8-9. In *Hellenica* 3.3 Xenophon discussed how a conspiracy led by Cinadon became known to the Spartan *ephors* (3.3.4-5). To prevent the conspiracy from happening, upon hearing about this, the *ephors* decided to send Cinadon together with some of his fellow conspirators away from Sparta to the town of Aulon on some errand. Cinadon had to bring back to Sparta certain Aulonians and Helots whose names were written in an official dispatch – a *scytale* – (mentioned twice at 3.3.8-9; for the complete passage see Appendix 1, page 299). Once more a *scytale* here apparently refers to an official Spartan dispatch, rather than a device for secret communication. Therefore, it is aptly translated as 'official dispatch' by Brownson and as 'despatches' by Warner and Cawkwell.²⁰⁷ It is notable in this context, however, that the dispatch under discussion appears to have been very simple indeed in terms of the text of its message. In fact, it seems to have simply comprised certain 'names'. Perhaps we see here evidence once more of the Athenian stereotype of the Spartans as semi-illiterate and able only to read and write their own names. What we do not see is evidence for the *scytale* being used in this source or this context for the purposes of secret communication.

²⁰⁷ Brownson 1918, 223; Warner & Cawkwell 1979, 162.

2.3.6.2: *Hellenica* 5.2.33-37

The other two references to *scytalae* in Xenophon's work can be found in Book 5, the first one in chapter 5.2.33-35 – in which Leontiades addressed the Spartans proposing a new alliance between Thebes and Sparta. With this alliance, according to Leontiades, if the Thebans ever found themselves in need of help from their allies, they would only have to send a short message – a *scytale* – to Sparta and help would immediately come (ἀλλ' ἀρκέσει ὑμῖν μικρὰ σκυτάλη ὥστ' ἐκεῖθεν πάντα ὑπηρετεῖσθαι ὅσων ἂν δέησθε, ἐὰν ὥσπερ ἡμεῖς ὑμῶν, οὕτω καὶ ὑμεῖς ἡμῶν ἐπιμελῆσθε [...] *a brief message from you [the Thebans] will suffice to secure from that quarter all the support that you may desire, provided only you show as much concern for us as we have shown for you*; Xenophon, *Hellenica*, 5.2.34-35; for the complete passage see Appendix 1, page 299). Because of the non-secret context here, and the two different states involved, Brownson translates the word σκυτάλη as 'brief message', and Warner and Cawkwell translate it as 'short message'.²⁰⁸ Once again, it is notable in this context that the dispatch under discussion appears to have been simple and short. Perhaps we see here further evidence of the stereotype of the Spartans as semi-illiterate and able only to read and write short messages. Once again, what we do not see is evidence for the *scytale* being used for the purposes of secret communication. The same applies to the second reference to a *scytale* in Xenophon's work at 5.2.37, in which Xenophon described how the Spartans – after the speech of Leontiades – sent *scytalae* to various allied – non-Spartan – states (εἰς τὰς συμμαχίδας πόλεις σκυτάλας διέπεμπον [...] *[The Lacedaemonians] transmitted official dispatches to the various allied states*; 5.2.37; for the complete passage see Appendix 1, page 300). In this context the term has again been translated by Brownson as 'official dispatches' and simply as 'despatches' by Warner and Cawkwell and it seems unlikely that these *scytalae* were secret or encrypted messages.²⁰⁹

²⁰⁸ Brownson 1921, 49; Warner & Cawkwell 1979, 268.

²⁰⁹ Brownson 1921 49; Warner & Cawkwell 1979, 268.

2.3.7: Aristotle (4th century BCE)

The broad semantic range and ambiguity of the term ‘*scytale*’ as it appears in various ancient contexts, as we have seen above, makes it difficult to determine sometimes whether a writer is referring to a simple staff or baton, a walking stick, a ‘dispatch stick’, a cryptographic device – or, in at least one instance, a phallus. From another group of sources it seems that there was another meaning attached to the term *scytale* in antiquity, which merits our particular consideration and analysis here. In a passage from Photius’ *Lexicon*, written in the 9th century CE (but recording much earlier lexical definitions), Photius gave various meanings of the word *scytale* (Photius, *Lexicon*, entry: σκυτάλη (I) and (II)). According to Photius, the principal meaning of the word *scytale* was ‘a thick-ended rod’ or a ‘whip’ (βακτηρία ἄκρο πάχη ἢ φραγέλλιον; Photius, *Lexicon*, entry: σκυτάλη (I)). However, Photius then added a secondary meaning, discussing how the Spartans used *scytalae* for their secret communication in a description that is very similar to those of Plutarch and Aulus Gellius and is clearly derived from these sources (see § 2.3.10; 2.4; 4.1.3; Photius, *Lexicon*, entry: σκυτάλη (II); Plutarch, *Life of Lysander*, 19.5-7; Aulus Gellius, *Attic Nights*, 17.9-15; for the complete passage see Appendix 2, page 305). However, in a third definition of the word *scytale*, Photius also described how – according to Dioscorides in his now lost 1st-century CE work *On Customs* – the Spartans also used *scytalae* to set up contracts (Photius, *Lexicon*, entry: σκυτάλη (II)). A money lender in Sparta would divide a *scytale* into two pieces and write the same contract onto the two *scytalae* – thereby creating two copies. One copy would be given to a witness while the other copy stayed with the money-lender (Διοσκουρίδης δὲ ἐν τοῖς περὶ νομίμων τοὺς δανείζοντας ἐν Σπάρτῃ διαιρεῖν σκυτάλην δύο παρόντων μαρτυρῶν καὶ γράφειν τὸ συμβόλαιον ἐν ἑκατέρῳ τμήματι; [...] Dioscorides in *On Customs* [says] that lenders in Sparta divide a ‘skytale’, with two witnesses being present, and write the contract on each piece. And that [a lender] gave the one to one of the witnesses but kept the other by himself; Photius, *Lexicon*,

entry: σκυτάλη (II)). According to Photius, Aristotle had already described this practice as occurring among the Ithacans in his *Constitution of the Ithacans* (Ἐχρῶντο δ' αὐτῷ καὶ ἄλλοι. Ὡς Ἀριστοτέλης ἐν τῇ Ἰθακησίων πολιτείᾳ μῆβ [...]) *Others too used to use it, as Aristotle [says] in the Constitution of the Ithacans 42*; Photius, *Lexicon*, entry: σκυτάλη (II)); for the complete passage see Appendix 2, page 305). Diels seems to misinterpret his sources when arguing that this passage shows that the Ithacans used *scytalae* for secret communication like the Spartans did.²¹⁰ Yet, this use of *scytalae* to set up contracts as discussed by Photius was clearly not the same as the Spartan practice of using the *scytale* as a cryptographic device and clearly no secret communication per se is involved in this ingenious scheme.

2.3.8: Theophrastus (4th century BCE)

A similar association with the word *scytale* appears in a Vatican palimpsest containing two short fragments dealing with the political and legal antiquities of several Greek states (*Biblioteca Apostolica Vaticana*; *Vat. Gr. 2306*). From their contents, Aly and Sbordone conclude that the fragments came from a work of Theophrastus (*Nomoi*) – a pupil of Aristotle – and draw heavily upon Aristotle's *Politeia*.²¹¹ In a passage on judicial procedures in Sparta that has only partly survived, it becomes clear that *scytalae* were regularly used to keep records during commercial, financial, and contractual processes (*Biblioteca Apostolica Vaticana*; *Vat. Gr. 2306*). This does not preclude their use in these contexts as tools for secret (or private) communication but clearly their form and function here is very different to the encoding required for a full cryptographic function. Keaney and Szedegy-Maszak – in their translations of Theophrastus' work based on the works of Aly and Sbordone – therefore, simply use the

²¹⁰ Diels 1914, 65.

²¹¹ Aly 1943; Keaney 1974, 179-194; Sbordone 1950.

word ‘*scytale*’.²¹² Again it shows that *scytalae* – in this case, it seems, ‘sticks’ of some kind – were used for a range of different purposes and that we must examine context closely in order to ascertain whether any encryption or secret communication is implied.

2.3.9: Ephorus (4th century BCE)

Diodorus Siculus’ *Library of History* – written in the 1st century BCE – and *Excerpta Constantiniana* – a Byzantine encyclopaedia written in *Ancient* Greek in Constantinople in the 10th century CE appear to preserve some references to *scytalae* attributed to the 4th century-BCE author Ephorus – who wrote a universal history of the Greek and non-Greek world, which has not survived.²¹³ In these sources we see the word *scytale* once as well as the word *scytalida* (‘little stick’; *σχυταλίδα*). In the first passage – in which we find the word *scytalida* – it is discussed how the Spartans – when going into battle – wrote their names on *scytalida* (little sticks) that they fastened to their arms in order that – if they died on the battlefield – their kinsmen could identify them (Diodorus Siculus, *Library of History*, 8.27; *Excerpta Constantiniana* 4). According to Polyaeus – writing in the 2nd century CE – the 7th-century BCE Spartan poet Tyrtaeus also referred to this practice – potentially making this the only Spartan reference to a *scytale* (ἵνα δὲ ὑπὸ τῶν οἰχείων ἐν τῇ τῶν νεχρῶν ἀναιρέσει γνωρίζοιτο ἕχαστος, ἐπὶ [τας] σχυταλίδας τοῦνομα γραψάντων καὶ τῇ λαῖᾳ χειρὶ φερόντων [...] if they [soldiers] died, they might easily be recognised amongst the bodies by their friends, they engraved their names on their [*scytalae* – *skytalidas*], which were fastened to their left arms; Polyaeus, *Stratagems of War*, 1.17; see also page 84). In this example, *scytalae* were used not for the purpose of securing confidential details, but were instead used for identification purposes – the ancient

²¹² Keaney 1974, 179-180; Szedegy-Maszak 1981, 91-95.

²¹³ Kelly 1998, 251; Stylianou 2013, 262-263.

equivalent of name badges or military ‘tags’. Significantly, Boring sees this as a rather curious custom and wonders if, given the closeness of Spartan society and the relatively small numbers often involved in battles, such a device would have been necessary for identification of the dead.²¹⁴ Boring – while he is not convinced about the practicality of the system – suggests that a *scytale* could have been cut in half or that two *scytalae* of the same size were taken – with the soldier’s name being written on both halves. One half could then be given to the soldier to be identified on the battlefield if necessary – while the other half was kept in Sparta and served as a sort of register of participants in any given battle or expedition. Those soldiers who failed to return home – and who perhaps could not be found on the battlefield – could later be identified with these sticks.²¹⁵ In Ephorus’ second passage – in which we find the word *scytale* – it is discussed how the Spartan general Lysander – when campaigning against the Athenians – sent his man Gylippus back to Sparta with booty and 1500 talents of silver. The money was in bags – each of which contained a *scytale* – which carried a notation of the amount of money in the bags (Ὅντος δὲ τοῦ χρημάτων ἐν σακίοις, καὶ ταῦτ’ ἔχοντος ἐκάστου σκυτάλην ἔχουσαν τὴν ἐπιγραφὴν τὸ πλῆθος τοῦ χρημάτων δηλοῦσαν [...] *The money was in small bags, each of which contained a skytalê which carried the notation of the amount of the money*; Diodorus Siculus, *Library of History*, 13.106.8-9; *Excerpta Constantiniana* 4; see for the complete passage Appendix 1, page 266). Gylippus – who apparently did not know about this – took money out of the bags for himself. The *ephors* – who instead knew about the *scytalae* in the bags – soon discovered Gylippus’ crime and condemned him to death (Diodorus Siculus, *Library of History*, 13.106.8-9). In this case, *scytalae* are used to indicate the amount of money in bags. However, Oldfather – in his translation of Diodorus’ work – presumes that there were also secret *scytale* dispatches in the bags and refers to this as a customary Spartan practice.

²¹⁴ Boring 1979, 18.

²¹⁵ Boring 1979, 18.

According to Oldfather, even if Gylippus had found the dispatches, he would not have been able to read them as they would have been encrypted.²¹⁶ However, Diodorus does not explicitly mention any dispatches in this case. He simply states that the *scytalae* indicated the amount of the money in the bags. Nevertheless, Oldfather's interpretation points to an intriguing possibility: that the Spartans employed a form of encryption to help ensure the security of important financial transfers and transactions. The financial 'tagging' use of *scytalae* allegedly described by Aristotle, Theophrastus, Ephorus, and re-described by others, may well have included a cryptographic element, too – but, if so, this is not described in the surviving sources.

2.3.10: Plutarch (late 1st/early 2nd century CE)

In the late 1st century/early 2nd century CE we see the first complete description of the *scytale* being used explicitly and unequivocally as a Spartan cryptograph in Plutarch's *Life of Lysander* (19.5-7; see: § 2.4). However, Plutarch's descriptions of the *scytale* suggest that he knew (either directly or indirectly) of various uses to which the *scytale* was put in antiquity. Set within in a wider context of messages sent by the Spartan *ephors* to their men in the field, Plutarch discussed the use of the *scytale* for some kind of communication purpose a total six times in his works (*Life of Lysander*, 19; 20; *Life of Alcibiades*, 38; *Life of Artaxerxes*, 6; *Life of Agesilaus*, 10; 15), thereby offering one of the most detailed pictures we have of the *scytale* – including as a device for secret and encrypted communication in antiquity. The range of Plutarch's sources is considerable and the scholarship on the use that Plutarch makes of his sources is equally extensive, but it has been suggested that Plutarch's description of the *scytale* (*Life of Lysander*, 19) is likely to have been based on a work of the 4th century BCE Greek historian and rhetorician Theopompus – potentially the historical work *Hellenica*, since this

²¹⁶ Oldfather 1950, 425.

work (which exists now only in fragments) seems to have been an important source for Plutarch's *Life of Lysander* more widely.²¹⁷ Indeed, Plutarch referred to Theopompus directly at least twice in his *Life of Lysander* (17.2-3; 30.2) and may well have used more material from the historian that remains unattributed. On this basis Candau Morón is convinced that 'In preparing his *Life of Lysander* Plutarch must have used the *Hellenica* of Theopompus'.²¹⁸

Verdegem is more cautious but similarly acknowledges the Theopompan source for parts of this *Life*: 'We cannot determine with certainty in which parts of his *Life of Alcibiades* Plutarch made use of Theopompus' *Hellenica*' – but we can with certainty say that he did use Theopompus in some parts of this text.²¹⁹ Indeed, Luft is certain that Plutarch used Theopompus as his primary source in this case and offers a detailed source-criticism analysis of Plutarch's text to confirm this.²²⁰ For example, he concludes that 'the *Hellenica* of Theopompus supplied Plutarch with the greater part of his material for the *Life of Lysander*' (particularly *Lysander* 2.1-2; 11.12; 21.7) on the grounds that 'Theopompus gave Plutarch the information that Lysander went on to Thrace after the fall of Athens, and sent back Gylippus to Sparta with his money'.²²¹ By examining the extant fragments, Luft identifies what he considers to be Theopompus' Spartan 'predilections', here taking the form of a particular interest in Sparta's distinctive national identity and a special fondness for stories about her national heroes – especially characters such as Cimon, Alcibiades, Lysander, and Agesilaus.²²² In fact, Luft sees some of Theopompus' distinctive stylistic devices, such as 'quick

²¹⁷ On Theopompus as Plutarch's key source for his *Life of Lysander* and thus for his description of the Spartan *scytale* see in particular Luft 1952; Russell 1966; Flower 1988; Candau Morón 2000; Verdegem 2010; and Schettino 2013.

²¹⁸ Candau Morón 2000, 461.

²¹⁹ Verdegem 2010, 74.

²²⁰ Luft 1952, 442-443.

²²¹ Luft 1952, 82.

²²² Luft 1952, 111 and 114, based on a survey of the fragments by Von Fritz 1941.

characterisation’ and a talent for writing in ‘vivid detail’, as helping to explain why Plutarch would have found him such a useful source for his own character-focused histories. Luft, therefore, concludes that in a number of his *Lives* (but especially in the *Lysander*), ‘Plutarch borrowed extensively from Theopompus’ and that ‘Plutarch was familiar with the *Hellenica* of Theopompus at first hand (the *Life of Lysander* is obviously based upon a first-hand knowledge of the *Hellenica* of Theopompus)’.²²³

If, as seems likely, Plutarch used Theopompus as his source on the Spartan *scytale*, it would make Plutarch’s late 1st/ early 2nd century CE description of the *scytale* and its use in the 5th and 4th centuries BCE a more reliable source. For, although Plutarch himself would not have witnessed the use of the *scytale*, and we must therefore treat his testimony to its use as cryptographic device with some caution, recognition of Plutarch’s own historical sources helps to lend authority to his account – and lends further weight to the argument that the *scytale* was, indeed, used for cryptographic communications by the Spartans. Only fragments of Theopompus’ work have survived, none of which refer directly to the *scytale* (see Storey 2011-II: *Fragments of Old Comedy* 3). However, we know from a short biography written by Photius (*Bibl.* 176 = T 2) that Theopompus was born around 378/377 BCE, and that both he and his father Damasistratus were allegedly exiled from their home in Chios for *lakōnismos* (that is, for ‘sympathizing with Sparta’). There is good reason to believe, therefore, that the Greek Theopompus (and his father) would have had closer dealings with Sparta than many other Greeks of the time and would have had particular (perhaps even unique) opportunities to witness or to hear first hand about the Spartan *scytale* and its use. We also know, by comparing Plutarch’s reworking of passages from Theopompus that have been preserved (for example, Plutarch *Moralia* 210d and Theopompus F22 = Athenaeus 14.657b-c), that Plutarch – although not repeating his source word for word – accurately and reliably preserves the details of the

²²³ Luft 1952, 181.

original in his paraphrase. Plutarch – based on this earlier Theopompean source – therefore, offers one of the most useful accounts of how the Spartans could and would have used the *scytale* as a deceptively simple cryptographic device to send encoded message (see § 2.4)

2.3.10.1: *Life of Lysander*

In chapter 19.4 of *Life of Lysander* Plutarch described how the Persian statesman Pharnabazus complained to the Spartan *ephors* that Lysander was pillaging his territories for no purpose. Therefore, they subsequently sent a message by *scytale* to Lysander summoning him to come home – or be sentenced to death on account of this misbehaviour. Plutarch confirms that this was an example of a message created by *scytale* – which the *ephors* often used when they wanted to communicate on confidential matters with generals in the field:

ὅταν οὖν ἀπόρρητόν τι καὶ μέγα φράσαι βουλευθῶσι, βιβλίον ὥσπερ ἱμάντα μακρὸν καὶ στενὸν ποιοῦντες περιελίττουσι τὴν παρ’ αὐτοῖς σκυτάλην, οὐδὲν διάλειμμα ποιοῦντες, ἀλλὰ πανταχόθεν κύκλω τὴν ἐπιφάνειαν αὐτῆς τῷ βιβλίῳ καταλαμβάνοντες. τοῦτο δὲ ποιήσαντες ἃ βούλονται καταγράφουσιν εἰς τὸ βιβλίον (Plutarch, *Life of Lysander*, 19.7; for the complete passages see Appendix 1, page 291-292).

Whenever [...] they [the *ephors*] wish to send some secret and important message, they make a scroll of parchment long and narrow, like a leathern strap, and wind it round their “*scytale*” [...]. After doing this, they write what they wish on the parchment [...].

Perrin translates the word *scytale* here as ‘dispatch-scroll’, as Plutarch observes that both the *scytale* stick and the message were known as a *scytale* since the thing measured – the message or letter – had the same name as the measure – in this case the stick (*καλεῖται δὲ ὁμωνύμως τῷ ξύλῳ σκυτάλη τὸ βιβλίον, ὡς τῷ μετροῦντι τὸ μετρούμενον; [...] the parchment, like the staff, is called "scytale," as the thing measured bears the name of the measure; Life of Lysander 19.7*). However, it is not clear from the context whether the secret message (*ἀπόρρητόν*) was encrypted or not. Lysander – being much disturbed upon receiving the dispatch – then went to

Pharnabazus asking him to send another letter to the *ephors* stating that he had not misbehaved. Pharnabazus, however, fooled Lysander by sending the *ephors* two letters: one written openly in which he stated that he had not been wronged by Lysander, and a second one – written in secret – in which he complained about Lysander’s misbehaviour once more. He then sent Lysander back to Sparta with the second letter (Plutarch, *Life of Lysander*, 20; cf. Homer, *Iliad*, 6.166-170; 178 for the story of Bellerophon who carried his own death sentence in a message from Proetus to Iobates). This second letter was not necessarily a cryptographic secret communication (Plutarch, *Life of Lysander*, 19.4). Instead, it may simply have been written in secret without Lysander knowing about it (*κρύφα γεγραμμένην*; Plutarch, *Life of Lysander*, 20). Since Lysander had seen Pharnabazus writing a letter in which the claims of serious misbehaviour and pillaging had been nullified, he felt confident going back to Sparta with Pharnabazus’ letter, which he carried openly. After the *ephors* showed Lysander the ‘secret’ letter he understood that he had been misled and left the city (Plutarch, *Life of Lysander*, 20.4; see also: Polyaeus, *Stratagems of War*, 7.19; Cornelius Nepos, *The Book on the Great Generals of Foreign Nations*. Pausanias, 4.3.4).²²⁴ Singh and Bauer – modern historians of cryptography – believe that Plutarch’s account indicates that another *scytale* message was sent to Lysander: a message warning the Spartans that Pharnabazus was planning an attack on the Greeks. They suggest that, thanks to this *scytale* message, Lysander was prepared for the attack and could repulse it.²²⁵ However, Plutarch only mentions the letter that Lysander received from the *ephors* and the two letters that Pharnabazus subsequently wrote (Plutarch, *Life of Lysander*, 19.4-20). There is no indication that Lysander also received a *scytale* message informing him

²²⁴ This example can be compared to Thucydides’ story of the Spartan general Pausanias who was also summoned home by the *ephors* because of misbehaviour by means of a *scytale* message (*History of the Peloponnesian War*, 1.131.1).

²²⁵ Bauer 2013, 4; Singh 1999, 9.

about a planned attack, let alone that a single *scytale* message prevented this attack. We cannot, then, take this as an unambiguous example of cryptographic secret communication.

2.3.10.2: *Life of Alcibiades*

However, Plutarch's writings elsewhere offer a more likely reference to the sending of a *scytale* message that is not merely secret but also encrypted. This can be found in his *Life of Alcibiades*. For his *Life of Alcibiades*, Plutarch used a range of sources belonging to various genres. He again used Theopompus' *Hellenica* (*Life of Alcibiades*, 23.3-5; 27-39), but also Thucydides' *History of the Peloponnesian War* (6.3; 11.2; 13.4; 20.6), Xenophon's *Hellenica* (23.7-9; 27-39) and Ephorus' *Library of History* (27-39), among other sources.²²⁶ According to Plutarch, the same general Lysander – at another point in his life – was among the leaders of the Athenians (his enemies) when he received a message by *scytale* – which Perrin once more translates as 'dispatch-scroll'²²⁷ – from the *ephors* urging him to kill the Athenian statesman Alcibiades (ὁ Λύσανδρος ἢ παρὰ τῶν οἴκοι τελῶν σκυτάλην ἐλθεῖν κελεύουσιν ἐκ ποδῶν ποιήσασθαι τὸν Ἀλκιβιάδην [...] *Lysander was not persuaded by these arguments until a dispatch-roll [scytale] came from the authorities at home bidding him put Alcibiades out of the way*; Plutarch, *Life of Alcibiades*, 38; for the complete passage see Appendix 1, page 289). For the *Life of Alcibiades* Plutarch certainly made some use of Theopompus: in chapter 32 Plutarch explicitly names Theopompus as a source, although it is not clear whether he has accessed Theopompus directly or through a later intermediary source (possibly Ephorus).²²⁸ Schettino has suggested that Plutarch's main source for the *Alcibiades* is actually Thucydides ('at least until chapter 27, that is, for the deeds accomplished up to 411 (the date to which Thucydides'

²²⁶ Verdegem 2010, 339ff.

²²⁷ Perrin 1916, 113.

²²⁸ See Luft 1952, 109 and 181.

work extends))’ but concedes that ‘in successive chapters a close link is likewise evident with the *Hellenica* of Xenophon’ and that ‘Ephorus and Theopompus are, nevertheless, also used as sources by Plutarch’ here.²²⁹ Verdegem, however, concludes that: ‘After a century of scholarly debate, the only serious candidates left [as important sources for the *Life of Alcibiades*] are Theopompus and Cratippus, a fourth-century Athenian continuator of Thucydides’.²³⁰ Whatever other sources Plutarch may have drawn upon for his *Life of Alcibiades*, therefore, it is likely that Plutarch’s story of the Spartan *scytale* in this case is based on Theopompus’ earlier account of the *scytale* here too. Yet, to return to the passage itself, since Lysander was among his Athenian enemies when he received the *scytale* message from the Spartan *ephors*, there is good reason to believe that this message would have been an encrypted message so as to prevent the Athenians from intercepting and reading it. However, this interpretation must be inferred from context only and there is no concrete reference in the text describing this *scytale* as a secret *cryptographic* message here.

2.3.10.3: *Life of Artaxerxes*

The third reference to the sending of a *scytale* message – again, most likely secret – can be found in Plutarch’s *Life of Artaxerxes*. Again, one of the sources for this narrative is *likely* to have included Theopompus, but here Plutarch gives us no direct evidence to show this and the modern secondary scholarship suggests that ‘Plutarch’s reconstitution of Artaxerxes’ life seems to have been based on literary sources from Dinon, Ctesias and Xenophon’.²³¹

According to Plutarch, when Cyrus the younger started a war against his brother Artaxerxes II, he requested help from the Spartans, who, accordingly, sent a message by *scytale*

²²⁹ Schettino 2013, 426.

²³⁰ Verdegem 2010, 74.

²³¹ Soares 2007, 86.

to their general Clearchus ordering him to aid Cyrus (*Λακεδαιμόνιοι μὲν οὖν σκυτάλην πρὸς Κλέαρχον ἀπέστειλαν ὑπηρετεῖν Κύρῳ πάντα κελεύοντες [...]* *The Lacedaemonians, accordingly, sent a dispatch-roll to Clearchus ordering him to give Cyrus every assistance*; Plutarch, *Life of Artaxerxes*, 6.3-4; see also Xenophon, *Anabasis*, 1.1.9; 1.2.21; 1.4.3; for the complete passage see Appendix 1, page 289-290). Perrin simply translates the word as ‘dispatch-roll’.²³² Yet, although the war between Cyrus the Younger and his brother Artaxerxes II was a war between two Persian brothers in which the Greeks only sent mercenary troops, the information communicated between the *ephors* in Sparta and Clearchus would still have been highly confidential, and of major importance to the Spartan campaign and strategy. If any enemies of the Spartans had intercepted this message, they could have decided to attack Sparta at the same time, knowing that most, if not all, of the Spartan troops would have been away at war in Persia at that time. In such a context, it seems sensible to assume that the *scytale* message in question would have been encrypted. However, once again, this can only be inferred from the context and is not an explicit description of the *scytale* as a form of secret communication here.

2.3.10.4: *Life of Agesilaus*

Finally, two further references to the sending of secret *scytale* messages are mentioned in Plutarch’s *Life of Agesilaus*. For this work Plutarch relied heavily on Xenophon’s *Agesilaius*, *Anabasis*, and *Hellenica*.²³³ However, Theopompus is also referred to at least four times (10.5;

²³² Perrin 1926, 130.

²³³ Plutarch, *Life of Agesilaus*, 4.1 = Xenophon, *Agesilaius*, 6.4; 11.7 = 5.4-7; 14.1 = 5.7; 20.5 = 8.7; 36.1 = 2.28-31; Plutarch, *Life of Agesilaus*, 18.1 = Xenophon, *Anabasis* 5.3.6; Plutarch, *Life of Agesilaus*, 5.1 = *Hellenica*, 3.3.2; 6.6 = 3.4.3f.; 7.1 = 3.4.7; 9.4 = 3.4.15; 10.1 = 3.4.16; 10.5 = 3.4.27; 11.1 = 4.1.1; 11.3 = 3.4.20; 12.5 = 4.1.28-38; 13.3; 4.1.39; 16.4 = 4.2.18-4.3.1; 16.5 = 4.3.9; 18.1 = 4.3.16; 21.1 = 4.5.5; 22.2 = 4.5.11-18; 22.3 = 4.5.8; 22.5 = 4.5.3-4.7.1; 23.1 = 4.8.10; 23.3 = 5.1.26ff.; 24.1 = 5.4.2-12; 24.2 = 5.3.13-25; 26.1 = 5.4.24-34; 26.2 = 5.4.35; 27.1 = 5.4.47-58; 27.3 = 6.3.3-20; 29.4 = 6.4.16; 30.5 = 6.5.10-21; 31.4 = 6.5.28; 33.8 = 6.5.50; 33.4 = 7.1.28-32; 34.3 = 7.5.10; 34.6 = 7.5.12-14; 35.1 = 7.5.22-24.

31.3; 32.8; 33.1), prompting Schettino to suggest that ‘Plutarch has ... integrated his principal source with Theopompus’.²³⁴ The first reference to a *scytale* can be found in chapter 10 of Plutarch’s *Life of Agesilaus*. Here, Plutarch described how the Spartan commander Agesilaus received word from the *ephors* in Sparta – while he was on campaign in Lydia and Phrygia – requesting him to take control of the Spartan army and navy (καθ’ ὁδὸν ὧν σκυτάλην δέχεται παρὰ τῶν οἴκοι τελῶν κελεύουσιν αὐτὸν ἄρχειν ἅμα καὶ τοῦ ναυτικοῦ. [...]) *On the road he [Agesilaus] received a dispatch-roll from the magistrates at home, which bade him assume control of the navy as well as of the army*; Plutarch, *Life of Agesilaus*, 10.5; see also Xenophon, *Hellenica*, 3.4.27ff.; for the complete passage see Appendix 1, page 288). Theopompus is mentioned in a subsequent section of this passage, although not in relation to the *scytale* message (10.5). And, the story that Plutarch tells us here on the *scytale* message, can also be found in Xenophon (*Hellenica*, 3.4.27ff). Therefore, it is once more highly plausible that Plutarch used one or both of these sources here for his detail of the *scytale*. Although the *scytale* message discussed here can be seen as an official request whereby Agesilaus was promoted by the *ephors* – it was also an example of a politically and strategically sensitive and important message sent from the *ephors* in Sparta to a commander in the field who was on campaign. Because of the sensitive content we might assume that the message would have been sent in encrypted form so that no one other than its intended recipient would have been able to read and act upon it. We find a parallel scenario in chapter 15 where Plutarch discussed how Agesilaus received another *scytale* message from the *ephors* in Sparta while still campaigning in Asia. As soon as Agesilaus received the *scytale* message, he acted upon its contents (ὅς ἅμα τῷ τὴν σκυτάλην ἐλθεῖν εὐτυχίαν τοσαύτην καὶ δύναμιν παροῦσαν καὶ τηλικαύτας ἐλπίδας

²³⁴ Schettino 2013, 426. See also Luft 1952, 351 who also concludes that in his ‘*Life of Agesilaus* Plutarch seems to have been greatly indebted to Theopompus’.

ὕφηνται ἀφ' ἑαυτοῦ καὶ προέμενος εὐθὺς ἀπέπλευσεν “ἀτελευτήτω ἐπὶ ἔργῳ [...] No sooner had the dispatch-roll come to him [Agesilaus] than he renounced and abandoned the great good fortune and power already in his grasp, and the great hopes which beckoned him on, and at once sailed off; Plutarch, *Life of Agesilaus*, 15.5; for the complete passage see Appendix 1, page 289). As in the previous examples from Plutarch's *Lives*, confidential information is sent between the *ephors* in Sparta and commanders in the field during wars and revolts. Although Perrin translates the word *σκυτάλη* (*scytale*) simply as ‘dispatch-roll’ both times, given the campaign context it is likely that all these messages would have been encrypted *scytale* messages.²³⁵ Indeed, Plutarch's clear and detailed description of the *scytale* (see § 2.4) as a cryptographic device, and his discussion of the sensitive contents of the messages sent between the *ephors* of Sparta and their commanders in the field show that *scytalae* could – and likely would – have been used for secret encrypted communication in warfare.²³⁶ Supporting this reading is the fact that Plutarch's accounts of the letters of Pharnabazus to the Spartans because of Lysander's misbehaviour (*Life of Lysander*, 19-20) can also be found in Polyaeus' 2nd-century CE work *Stratagems of War* (7.19), where again we see three letters: a secret *scytale*-letter sent from the *ephors* to Lysander to summon him home and the two conventional letters from Pharnabazus to the *ephors*. Significantly, only for the presumably encrypted *scytale* message does Polyaeus use the word *σκυτάλην* (*scytale*; οἱ δὲ ἀπὸ τῆς Ἀσίας αὐτὸν ἀνεκαλέσαντο σκυτάλην πέμπαντες [...] The Lacedaemonians recalled Lysander from Asia by means of sending him a *scytale* message; Polyaeus, *Stratagems of War*, 7.19; for the complete passage see Appendix 1, page 294) while for the two non-encrypted letters – one ‘secret’ and

²³⁵ Perrin 1917, 25; 41.

²³⁶ Although, it must also be borne in mind that Plutarch is not offering us eye-witness testimony of the *scytale* in these descriptions: Plutarch wrote about the sending of *scytale* messages in the 2nd century CE, about 500-600 years after Lysander, Clearchus, and Agesilaus – who allegedly received these encrypted *scytale* messages – lived.

one open – he used the words *ἐπιστολὴν* (*epistolè*), *βιβλία* (*biblia*), and *γράμματα* (*grammata*) respectively.²³⁷

2.4: The *scytale* in practice²³⁸

Plutarch does provide us with one of the only two full descriptions of the working of the *scytale* (*Life of Lysander*, 19.5-7; for the complete passage see Appendix 1, page 291-292) – and will provide the basis of the analysis of the device as a practical tool that is offered in this section of this chapter. The second description comes from Aulus Gellius (*Attic Nights*, 17.9.6-16). Both authors were active in the 2nd century CE, so are writing at some considerable temporal distance from Herodotus (upon whose accounts of the Spartan use of steganographic secret communications the majority of later sources clearly draw) and from both the Peloponnesian War in 431 BCE and the Battle of Leuctra in 371 BCE (in which even those modern historians of cryptography sceptical of the ancient use of the *scytale* acknowledge that the *scytale* would most likely have been first used).²³⁹ As discussed in § 2.3.10, Plutarch must have used an earlier source for his description of the *scytale* – most likely Theopompus. The same applies to Aulus Gellius – writing in the late 2nd century CE – who identifies a great number of earlier sources for his work from both well known and less well known authors, including literary authors like Homer and Hesiod (*Attic Nights*, 3.11), grammarians including Fronto (*Attic Nights*, 2.26), and Publius Nigidius (3.12), and scholarly authors including Pliny (3.16; 9.5; 9.16; 10.12; 17.15), and Varro (3.10). However, by far and

²³⁷ Shepherd 1793, 280. Shepherd – in his translation of the work – only used the word ‘letter’ for all the letters that were sent in the passage, and suggested that Pharnabazus simply wrote his second letter in private.

²³⁸ See also: Diepenbroek 2020 (forthcoming).

²³⁹ See, for instance, Kelly 1985, 143.

away the most influential historical source for Aulus Gellius is Plutarch himself – who is quoted in no fewer than 11 passages (*Attic Nights*, 1.1.1; 1.3.5; 1.4.31; 1.26.4-8; 2.8-9; 3.5-6; 4.11; 11.16; 15.10.1; 17.11; 20.8.7) – including in chapter 17 in which we find Aulus Gellius’ description of the Spartan *scytale*.²⁴⁰ So important is Plutarch as a source for Aulus Gellius, that he shows his indebtedness by making the word ‘Plutarch’ the very first word of his *Attic Nights* (1.1: *Plutarchus in libro quem de Herculis [...] Plutarch, in the book which he wrote on Hercules ...*).²⁴¹ Like Plutarch, Aulus Gellius likes to illustrate his work with biographical narratives and anecdotes, and his *Attic Nights* features all the same Greek, Spartan, and Roman characters that Plutarch wrote about (such as Pericles, Themistocles, and Alcibiades).²⁴² The reasons for Plutarch’s great influence upon Aulus Gellius’ writing are therefore clear. However, as Cavazza observes: Aulus Gellius ‘depends on his sources, but has a mind of his own; he does not merely weigh up other people’s ideas, he judges them, filters them, and [...] He not only quotes his sources but corrects them’.²⁴³

He does this, typically, by taking multiple sources for each chapter.²⁴⁴ However, he does not always tell us which sources he has consulted, and even when he does, we can never be sure whether he has consulted a source at first or second hand.²⁴⁵ Similarly, even when he

²⁴⁰ See further on Aulus Gellius’ sources Oikonomopoulou 2019; Howley: 2018; Grafton, Most & Settis 2013; Cavazza 2004; Holford-Strevens 2003; 2019-I; 2019-II (especially page 590); Holford-Strevens & Vardi 2004; Rolfe 1927, xvii.

²⁴¹ On this point see also Grafton, Most & Settis 2013, 748.

²⁴² See Oikonomopoulou 2019, 45.

²⁴³ Cavazza 2004, 66.

²⁴⁴ See Holford-Strevens 2003, 72-78 on Aulus Gellius’ sources. Holford-Strevens dismisses the idea that there is only one identifiable source for each chapter of *Attic Nights* (2003, 77): ‘Even if, for the sake of argument, we agreed that everything in Gellius, unlike our own writings, must have a written source that he could have specified had he so chosen, and that what was source for the fact must also be the source for the comment, we should find the Kretzschmerian hypothesis of a single source for single chapters to be a leaky dwelling’.

²⁴⁵ Holford-Strevens 2003, 78.

is clearly quoting from an older source text, Aulus Gellius does not always record that source. For example, Thucydides is an obvious source for a significant portion of the Greek history incorporated in *Attic Nights*. Yet, as Holford-Strevens points out: ‘Thucydides (1.11.1) [is mentioned by Aulus Gellius] only once, for the Spartans’ marching to the aulos.’²⁴⁶ Theopompus also appears in *Attic Nights* only once (and in a similarly trivial context): in 16.15, Aulus Gellius reports that Theopompus believed the Bisaltian hare possessed two livers. This comparison with Thucydides suggests that, even if Aulus Gellius were consulting Theopompus at first hand for his account of the *scytale*, he would not necessarily name him as a source.

Although Aulus Gellius did not identify his particular sources for his passage on the *scytale*, then, (*Attic Nights*, 17.9.6-16; for the complete passage see Appendix 1, page 267), he will certainly have drawn upon earlier sources for his description here too – including (given the close similarity of both accounts) both Plutarch’s description of the *scytale* and possibly Plutarch’s own original source(s) on the topic – most likely Theopompus (see also § 4.3.2). So, although Aulus Gellius may have been writing several centuries after the Spartans used their *scytalae*, he very likely had access to much earlier sources that are now lost to us and which he drew on for his description of the *scytale*. Since these sources would certainly have included Plutarch, we can say with some confidence that they also included – whether

²⁴⁶ Holford-Strevens 2003, 247. See Holford-Strevens 2003, 246 on Aulus Gellius’ considerable indebtedness to the Greek historians (including Herodotus and Thucydides). Intriguingly, Holford-Strevens speculates here that the reason Aulus Gellius offers such a confused misreading of Herodotus on Spartan history (in *Attic Nights* 17 in particular) – including the steganographic stratagems practised by Histiaeus of Miletus and by Demaratus – may be because Aulus Gellius was simultaneously referring to another set of technical treatises (*stratagemata*) which focused on descriptions of the devices and stratagems (rather than the characters and stories, which were Herodotus’ main concern). So, Holford-Strevens suggests (2003, 246): ‘Gellius would have relied on a collection of *stratagemata* that concentrated on the stratagems themselves.’ This raises the possibility that Aulus Gellius (and Plutarch before him) both had access to a now lost technical treatise on ancient steganographic and cryptographic stratagems when writing their descriptions of the Spartan *scytale*.

directly or indirectly – Theopompus.²⁴⁷

Drawing upon much earlier source(s) from the 4th century BCE that are now lost or survive only in fragments, then, Plutarch and Aulus Gellius offer usefully detailed accounts of the *scytale* and can tell us much about how this deceptively simple cryptographic device could and would have been used to send encoded messages in field operations. According to Plutarch, writing in the late 1st/early 2nd-century CE (but, in all likelihood, drawing upon Theopompus as his source):

[...] ἐπὶ ἀν ἐκπέμπωσι ναύαρχον ἢ στρατηγὸν οἱ ἔφοροι, ξύλα δύο στρογγύλα μήκος καὶ πάχος ἀκριβῶς ἀπιδόσαντες, [...], τὸ μὲν αὐτοὶ φυλάττουσι, θάτερον δὲ τῷ πεμπομένῳ διδόντες. ταῦτα δὲ τὰ ξύλα σκυτάλας καλοῦσιν. ὅταν οὖν ἀπόρρητόν τι καὶ μέγα φράσαι βουλευθῶσι, βιβλίον ὥσπερ ἱμάντα μακρὸν καὶ στενὸν ποιοῦντες περιελίττουσι τὴν παρ' αὐτοῖς σκυτάλην, οὐδὲν διάλειμμα ποιοῦντες, [...] τοῦτο δὲ ποιήσαντες ἃ βούλονται καταγράφουσιν εἰς τὸ βιβλίον, ὥσπερ ἐστὶ τῇ σκυτάλῃ περικείμενον· ὅταν δὲ γράψωσιν, ἀφελόντες τὸ βιβλίον ἄνευ τοῦ ξύλου πρὸς τὸν στρατηγὸν ἀποστέλλουσι (Plutarch, *Life of Lysander*, 19.5-6; for the complete passage see Appendix 1, page 291-292).

When the *ephors* send out an admiral or a general, they make two round pieces of wood exactly alike in length and thickness, [...] and keep one themselves, while they give the other to their envoy. These pieces of wood they call “*scytalae*.” Whenever [...] they wish to send some secret and important message, they make a scroll of parchment long and narrow, like a leathern strap, and wind it round their “*scytale*” [...]. After doing this, they write what they wish on the parchment [...]; and when they have written their message, they take the parchment off, and send it, [...] to the commander.

Aulus Gellius’ later 2nd-century CE description is very similar to Plutarch’s:

Lacedaemonii [...], cum dissimulare et occultare litteras publice ad imperatores suos missas volebant, [...], epistulas id genus factas mittebant. Surculi duo erant teretes, oblonguli, pari crassamento eiusdemque longitudinis [...]; unus imperatori in bellum proficiscenti dabatur, alterum domi magistratus [...] circum eum surculum lorum [...]. Litteras deinde in eo loro per transversas iuncturarum oras versibus a summo ad

²⁴⁷ Cavazza 2004; Holford-Strevens 2003; 2019-I; 2019-II; Holford-Strevens & Vardi 2004; Rolfe 1927, xvii.

imum proficiscentibus inscribebant; id lorum litteris ita [...] imperatori [...] mittebant; [...]. Hoc genus epistulae Lacedaemonii *σκυτάλην* appellant (Aulus Gellius, *Attic Nights*, 17.9.6-16; for the complete passage see Appendix 1, page 267).

[When the] ancient Lacedaemonians [...] wanted to conceal and disguise [...] public dispatches sent to their generals [they][...] used to send letters written in the following manner. There were two thin, cylindrical wands of the same thickness and length, [...]. One of these was given to the general when he went to war, the other the magistrates kept at home [...]. [Then] [...] they bound about the staff a thong [and] [...] they wrote the dispatch on that thong [...] When the letter had been written [...], the thong was unrolled from the wand and sent to the general, [...]. This kind of letter the Lacedaemonians called *σκυτάλη* [*scytale*].

From the descriptions of Plutarch and Aulus Gellius it becomes clear that around a *scytale* (stick) a long and narrow strip of writing material was wrapped, cut either from papyrus or parchment on which a message was written. Plutarch in his early 2nd-century CE work used the word *βιβλίον* (*biblion*) to describe this writing material and its text, which may be translated in this context as ‘a strip of papyrus’ (*Life of Lysander*, 19.5) – adding that it was like a long and narrow leathern strap (*ἰμάντα μακρὸν*). Aulus Gellius also believed it to have been a strip of parchment. In his later 2nd-century CE description of the *scytale* we find the word *lorum* to describe the strip of material, which can be translated as ‘leather’ (*Attic Nights*, 17.9.9) – that is, in this context, a thin strip of leather parchment. However, these material distinctions are not always preserved in translations and modern works on the history of cryptography.

Erasmus in his early 16th-century work *Adages*, believed that both the stick and a leather thong wrapped around the stick together were called a *scytale* (Desiderius Erasmus, *Adages*, Edition Mynors Volume 33, 1991, p.78; Volume 34, 1992, p.50). Erasmus here, potentially confused Plutarch’s and Aulus Gellius’ descriptions of the *scytale* since while Aulus Gellius mentioned that the letter that was sent to the general was called a *scytale* (Aulus Gellius, *Attic Nights*, 17.9.6-16), Plutarch suggested that either the stick or the leathern strap (or in fact, the

message) were both called *scytale* (Plutarch, *Life of Lysander*, 19.7). Cardano in his 1550 work *De Subtilitate* – simply mentioned cylinders (*scytalae*) that were used for secret communication by the Spartans without giving any details on how this worked and what materials were used for it – something that may indicate that Cardano knew about Plutarch’s and Aulus Gellius’ descriptions, but found it unnecessary to repeat them in his own work (*De Subtilitate*, 17.1036; for the complete passage see Appendix 2, page 304). Perrin translates the word *βιβλίον* (*biblion*) as ‘parchment’ in the Loeb version of Plutarch’s *Life of Lysander* as Poe already did in his 1841 work *A Few Words on Secret Writing*.²⁴⁸ And Smith, Kahn and Mollin – modern historians of cryptography – seem certain that parchment was used instead of papyrus.²⁴⁹ However, both papyrus and leather parchment were typically used as writing materials in antiquity, so there seems to be no particular significance attaching to the use of either as the medium for the *scytale*’s encrypted messages. It seems plausible that leather parchment would offer a more robust material for messages that might need to be sent over long distances, over difficult terrain, and in conflict situations – since, according to Plutarch and Aulus Gellius, the *ephors* in Sparta used the *scytale* method to communicate with commanders in the field (Plutarch, *Life of Lysander*, 19.5; Aulus Gellius, *Attic Nights*, 17.6).²⁵⁰ Yet, while on campaign one obviously had to be able to write and send messages simply and quickly, so where papyrus was readily to hand this would presumably have offered a convenient alternative medium. Although neither Plutarch nor Aulus Gellius mentions it, the message could have been written in either plaintext or ciphertext – with the latter option making the message doubly secret and, therefore, doubly secure. However, nothing in their descriptions proves that the text was written in cipher. It will, therefore, be presumed that the *scytale* messages were written in plaintext.

²⁴⁸ Perrin 1916, 287; Poe 1841, 33.

²⁴⁹ Smith 1955, 16; Kahn 1967, 75-76; Mollin 2005, 9.

²⁵⁰ Jeffery 1961, 57; Sherwood 2006, 536-537.

After a message was written on the strip of parchment or papyrus, the strip was then unwrapped from the *scytale* stick (Plutarch, *Life of Lysander*, 19.5; Aulus Gellius, *Attic Nights*, 19.7.6-10). By unwrapping the text strip from the *scytale* all letters in the original message were transposed to a different position, as Plutarch and Aulus Gellius described. Thus, according to Plutarch, when a general in the field received a *scytale* message:

δεξάμενος δὲ ἐκεῖνος ἄλλως μὲν οὐδὲν ἀναλέξασθαι δύναται τῶν γραμμάτων συναφὴν οὐκ ἔχόντων, ἀλλὰ διεσπασμένων [...] (Plutarch, *Life of Lysander*, 19.7; for the complete passage see Appendix 1, page 291-292).

He, [could not] get any meaning out of it, —since the letters have no connection, but are disarranged [...].

While Aulus Gellius additionally mentioned partial and broken letters:

resolutio autem lori litteras truncas atque mutilas reddebat membraque earum et apices in partis diversissimas spargebat (Aulus Gellius, *Attic Night*, 17.9.12-13; for the complete passage see Appendix 1, page 267).

the unrolling of the thong made the letters imperfect and broken, and their parts and strokes were divided and separated.

This transposing of the letters in the message makes the *scytale* the first military transposition cipher known in history. As Singh states:

[A] form of transposition is embodied in the first ever military cryptographic device, the Spartan *scytale*.²⁵¹

The following example shows how the transposition encryption achieved by this wrapping and unwrapping would have worked – according to Plutarch’s and Aulus Gellius’ descriptions – and how the strip of writing material may have looked during the subsequent steps in the process. For this example, the text ‘*Enemy attacks at Dawn Tomorrow*’ will be used. First, a

²⁵¹ Singh 1999, 7.

strip of writing material was wrapped about the *scytale*. In this way small rectangular columns are created. Since the wrapping was done by hand, it is likely that the edges of the strip overlapped each other. Therefore, the columns were not all exactly the same in size.



FIGURE 6: SCYTALE WITH STRIP OF WRITING MATERIAL WRAPPED ABOUT IT.²⁵²

Then the text – in my example, ‘*Enemy attacks at Dawn Tomorrow*’ – would have been written on the strip of writing material. In Figures 7 and 8 (below), the text is written from left to right and top to bottom on two lines.

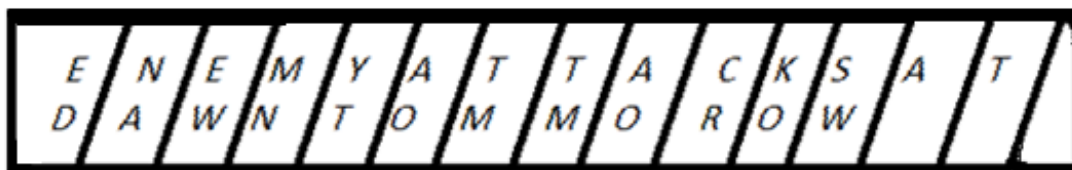


FIGURE 7: TEXT: ‘ENEMY ATTACKS AT DAWN TOMORROW’, WRITTEN ON SCYTALE.²⁵³

As Plutarch describes in his account of the *scytale*, once the strip of writing material had been unwrapped from the *scytale*, all letters would have been rearranged (*Life of Lysander*, 19.7):

δὲ ἐκεῖνος ἄλλως μὲν οὐδὲν ἀναλέξασθαι δύναται τῶν γραμμάτων συναφὴν οὐκ ἐχόντων, ἀλλὰ διεσπασμένων [...] (Plutarch, *Life of Lysander*, 19.7; for the complete passage see Appendix 1, page 291-292).

²⁵² Author’s illustration.

²⁵³ Author’s illustration.

when [the recipient] has received [the strip], [he] cannot [...] get any meaning out of it,—since the letters have no connection, but are disarranged [...].

By unwrapping the strip, the letters would now appear per column, instead of per row. So, instead of reading *E-N-E-M-Y*, the first word of the message, one would now read *E-D-N-A-E* et cetera (see Figure 8). In Figure 8, every letter of the message has been written on a complete piece of material strip. In other words, no letters were written over the edges of the strip, meaning that when the strip was subsequently removed from the *scytale* stick, all the letters would have remained intact and would simply have been rearranged in their order of sequence.

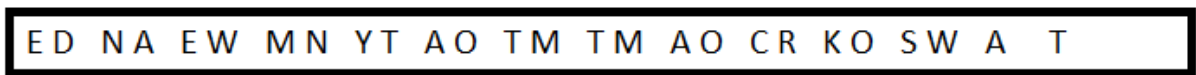


FIGURE 8: STRIP OF WRITING MATERIAL WITH TEXT UNWRAPPED FROM SCYTALE.²⁵⁴

However, according to Plutarch, the complete *scytale* was covered in the writing material (στενὸν ποιοῦντες περιελίττουσι τὴν παρ’ αὐτοῖς σκυτάλην, οὐδὲν διάλειμμα ποιοῦντες, ἀλλὰ πανταχόθεν κύκλῳ τὴν ἐπιφάνειαν αὐτῆς τῷ βιβλίῳ καταλαμβάνοντες [...]) they make a scroll of parchment long and narrow, like a leathern strap, and wind it round their “scytale” leaving no vacant space thereon, but covering its surface all round with the parchment; Plutarch, *Life of Lysander*, 19.6). This makes it more plausible that the sender of a message did not in practice write with all letters neatly contained upon complete pieces of the *scytale*’s material strip, but that the letters of the message would also have been written across the edges of the strip (Figure 9).

²⁵⁴ Author’s illustration.

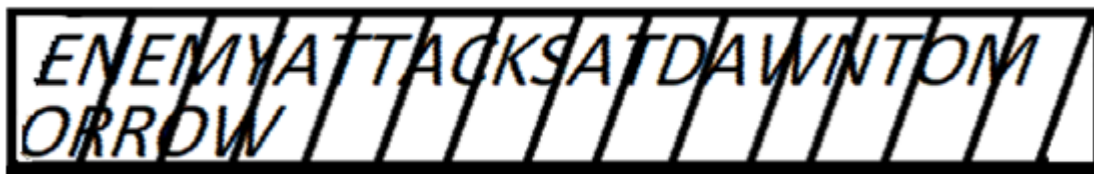


FIGURE 9: TEXT 'ENEMY ATTACKS AT DAWN TOMORROW' WRITTEN ACROSS COMPLETE STRIP OF WRITING MATERIAL.²⁵⁵

Since Plutarch's description indicates the likelihood that the whole strip was used for writing, at least some of the letters on the strip would have been written whole and on a complete piece of strip. These letters would have remained intact and recognisable once the strip was unwrapped from the *scytale*. Yet, since some of the letters on the strip would have been written overlapping the edges of the strip, these letters would not have remained intact once the strip was unwrapped from the *scytale*. And indeed, according to Aulus Gellius, this is what happened in practice: the unrolling of the strip made the letters imperfect and broken (see Figure 10):

resolutio autem lori litteras truncas atque mutilas reddebat membraque earum et apices in partis diversissimas spargebat; propterea, si id lorum in manus hostium inciderat, nihil quicquam coniectari ex eo scripto quibat (Aulus Gellius, *Attic Nights*, 17.9.12-14; for the complete passage see Appendix 1, page 267).

The unrolling of the thong made the letters imperfect and broken, and their parts and strokes were divided and separated. Therefore, if the thong fell into the hands of the enemy, nothing at all could be made out from the writing [...].

If the strip from Figure 8 – for example – was unwrapped from the *scytale*, the strip would look like the following figure (Figure 10). In this figure the strip is cut into pieces to show the difference between the partial and complete letters.

²⁵⁵ Author's illustration.



FIGURE 10: COMPLETE STRIP OF WRITING MATERIAL CUT INTO PIECES TO SHOW PARTIAL AND COMPLETE LETTERS.²⁵⁶

We can see from this reconstruction just how challenging it would have been to attempt to reconstruct the original text from this scrambled ciphertext. It would certainly not be impossible, but – without a *scytale* rod of the same size as the one used in the original encryption – would have been time-consuming. A good modern parallel might be the paper shredder, which offers one way of ‘encrypting’ or scrambling a confidential source text. With patience, skill, and time, the original text can be reconstructed from the shredded strips of paper. The advantage of the *scytale* device, however, is that it offers the opportunity for that reconstruction to be managed much more quickly and easily.

At the beginning of this chapter the following research question was posed: *How did non-Spartan sources present the Spartan scytale, and what evidence is there in these sources to suggest that the scytale was (or was not) used as a device for secret communication in the 5th and 4th centuries BCE?* It has been shown that Greek sources vary widely in their discussions of the *scytale* and, although they are broadly consistent in associating the *scytale* with messaging, they typically do not associate it with secret messaging. The clearest descriptions of the *scytale* as a cryptographic device come from later sources: Plutarch and Aulus Gellius (§ 2.3.10; 2.4; 4.3.2; Plutarch, *Life of Lysander*, 19.5-7; Aulus Gellius, *Attic Nights*, 17.9.6-16). Yet, although these authors were active in the late 1st to late 2nd century CE, at a considerable

²⁵⁶ Author’s illustration.

distance from the time in which the Spartans used *scytalae* for their secret communication in the 5th and 4th centuries BCE, they drew their descriptions of the *scytale* from more contemporary sources. In particular, their detailed accounts of the *scytale* as a cryptographic device are likely to have derived from the 4th century BCE historian Theopompus. Theopompus not only shared a name with one of Sparta's early Eurypontid kings (who reigned in the 7th century BCE) but came from a Greek family famously charged with *lakōnismos* ('sympathizing with Sparta'). There is good reason to believe, then, that Theopompus may have had particular (possibly unique) first hand access to the Spartan *scytale* and its use and wrote about it with authority. Plutarch – based on this earlier Theopompean source – and Aulus Gellius – largely based on Plutarch and Plutarch's sources (including Theopompus) – therefore, offer the most useful accounts of how the Spartans could and would have used the *scytale* as a deceptively simple cryptographic device to send encoded messages. Although Plutarch's and Aulus Gellius' descriptions – albeit based on their earlier sources – alone do not prove that *scytalae* were used in practice for secret communication, the ingenious rearrangement of the letters that they describe as the key feature of *scytale* communication makes the *scytale* a candidate for the earliest known theoretical transposition cipher in history. Taking together all the extant sources on the *scytale*, this chapter has shown that it is wholly plausible that Spartan *scytalae* were actually used for secret communication – among other purposes – even though the concrete evidence for this use remains largely inaccessible. Indeed, the ingenuity and importance of the transposition system of the *scytale* cannot and should not be overlooked here. In fact, some modern cryptographers see the *scytale* as a forerunner of modern transposition ciphers.²⁵⁷ Reinke, for example, describes it as '*the forerunner of the simple transposition (ciphers) of today*', while Luenberger suggests that '*practical transposition ciphers are similar*

²⁵⁷ Raggo & Hosmer 2012, 9; Reinke 1962, 116; Singh 1999, 8-9.

to those produced by the scytale'.²⁵⁸ How the principle of the use of *scytalae* can still be found in modern transposition ciphers (particularly those used in warfare) will be discussed in the concluding chapter, but now we turn to consider why the *scytale* – with such obvious potential as a simple yet secure device for secret communication should apparently be overlooked by one of the most important classical Greek sources on ancient forms of secret communication – Aeneas Tacticus' *How to Survive Under Siege*.

²⁵⁸ Luenberger 2012, 167; Reinke 1962, 116.

Chapter 3: Cryptography and steganography in Aeneas Tacticus' *How to Survive Under Siege*

The 4th-century BCE Greek military author Aeneas Tacticus does not seem to have discussed the *scytale* in his influential writings on secret communication techniques in antiquity. Modern historians of cryptography argue that the *scytale* cannot, therefore, have actually been used as a cryptographic device in the ancient Greek world since Aeneas Tacticus did not discuss it in his otherwise broadly comprehensive survey of classical stratagems and devices for secret communication. However, as will be argued and demonstrated in this chapter, Aeneas Tacticus had other reasons for not discussing the *scytale* in his treatise – the principal reason being that, as the author of a handbook on strategies for siege warfare, Aeneas Tacticus was far more interested in steganography than cryptography. Therefore, in this chapter, the following key research question will be answered: *What are the reasons that the 4th-century BCE Greek military author Aeneas Tacticus – who dedicated a chapter of his work How to Survive Under Siege to secret communication – excluded the Spartan scytale from his treatise?*

Modern historians of cryptography often presume that the *scytale* is unlikely to have been used for secret communication in antiquity since Aeneas Tacticus – whose work has already been introduced in the prologue to this thesis – did not discuss the device. Whitehead, in his translation of Aeneas Tacticus' work argues that:

The omission of the well-known Spartan *skytale* need occasion no surprise, since it was not, as has almost universally been supposed, a cryptograph.²⁵⁹

²⁵⁹ Whitehead 1990, 183-184.

While Whitehead assumes that Aeneas Tacticus did not discuss the *scytale* because it was never used as a cryptographic device, West argues that Aeneas did not discuss it in his work because he was personally unfamiliar with the device :

We should [...] note that Aeneas Tacticus has nothing to say about the device [the *scytale*] in his chapter on secret messages [...], though would it have been known to him, he would certainly have mentioned it, if only to criticise its defects.²⁶⁰

Sheldon also argues that Aeneas Tacticus must have been unfamiliar with the Spartan *scytale* since he made no mention of it in *How to Survive Under Siege*:

it is telling that Aeneas [...], our single most important source of information on ancient Greek cryptography, does not mention the *skytale* once. [...]. We can only conclude that it was unknown to [him].²⁶¹

However, in this chapter it will be argued that there are a number of other reasons to justify the fact that Aeneas Tacticus did not discuss the Spartan *scytale* in his work. The most important of these is the fact that Aeneas Tacticus focuses his attention upon *siege* warfare and therefore upon the stratagems and devices for secret communication most suited to this particular military context.

Very little is known about the life (and therefore of the direct military, cryptographic or steganographic experiences) of Aeneas Tacticus. Aeneas Tacticus, or Aineias the Tactician – often identified as Aineias of Stymphalos, an Arcadian general from the 4th century BCE who is mentioned in Xenophon's *Hellenica* (Xenophon, *Hellenica*, 7.3.1)²⁶² – wrote a treatise on

²⁶⁰ West 1988, 42.

²⁶¹ Sheldon 1987, 45.

²⁶² Barends 1955; 171; Bliese 1994, 108; Brownson 1918, 281; Chaniotis 2013, 441; Dain & Bon 1967, vii; xii; David 1986 (I), 343; Delebecque, 1957, 430; Hug 1877, 28 ff.; Hunter & Handford, 1927 ix-x.; xxii; xxiv-xxv; 264; Millett 2013, 65; Oldfather 1923 7; Rawling 2007, 13; Star 1957; 68; Vela Tejada 2004, 141-142; Usher 1970, 210-211; Whitehead 1990, 10-12; Winterling 1991, 196. See also Vela Tejada 1991.

tactics known as *How to Survive Under Siege* or *On the Defence of Fortified Positions* (Περὶ τοῦ πῶς χρὴ πολιορκουμένων ἀντέχειν) around 360-355 BCE.²⁶³ A date around 360-355 BCE makes Aeneas Tacticus' work not only the oldest known military manual in history but also the oldest known work on cryptography and steganography.²⁶⁴ Chapter 31 of the work is specifically dedicated to recommendations regarding the use of cryptographic and steganographic devices and methods during sieges – and it is here that West, Whitehead, Strasser et al. insist that we would expect to find a discussion of the *scytale* had its use as a cryptographic device been known to Aeneas Tacticus. In the course of chapter 31 the author discussed twenty-one different methods for secret communication, offering us a detailed catalogue of ancient cryptography whereby – according to West, Kelly and Whitehead – the absence of the *scytale* is straightforwardly explained on the grounds that it was not a cryptographic device known to Aeneas Tacticus.²⁶⁵ Given Aeneas Tacticus' (presumed) extensive military experience, these scholars extrapolate from this that the *scytale* was, therefore, not a cryptographic device that was used in Greece in this period. However, there are other reasons that might explain this absence of a discussion of the *scytale* in Aeneas

²⁶³ Hunter & Handford 1927; Oldfather 1928; Whitehead 1990. It is likely that Aeneas wrote at least four other works on military strategy that have been lost. Three of the works are referred to in *How to Survive Under Siege*: a work on military preparations (7.4; 8.5; 21.1; 40.8); a work on procurement (14.2); and a work on encampment (21.2). Scholars presume that Aeneas also wrote a work on conducting siege operations (Aelian, *The Tactics*, 1.2; 3.4; Julius Africanus, *Kestoi*, 37; Bliese 1994, 108; Hanson 2007, 3; Hunter & Handford 1927, xii-xiii; Oldfather 1923, 4; 8-9; Vela Tejada 2004, 142-143; Rawling 2007, 139; Whitehead 1990, 14-15; see also Vela Tejada 1991).

²⁶⁴ Chaniotis 2013, 446; Jenkins 1999, 35; Moore 2013, 462; Vela Tejada 2004, 141-142. See also Vela Tejada 1991.

²⁶⁵ Kelly 1985, 141-169; West 1988, 42; Whitehead 1990, 184. In a previous publication based on my research for this thesis I suggested sixteen different methods (Diepenbroek 2019). I have since identified a total of twenty-one different methods catalogued in Aeneas Tacticus' work. In D'Agapeyeff's work we see the name of the Roman Tacitus being connected to the invention of these methods of secret communication (D'Agapeyeff 193, 16). D'Agapeyeff potentially confuses the names Aeneas Tacticus and Tacitus, an example of how some modern historians of cryptography can seem to misinterpret original sources.

Tacticus' work. It will be argued that, although Aeneas Tacticus did not directly discuss the *scytale* in his chapter on secret communication, his writings reveal that he was familiar with the principle of transposition ciphers and the key concept of transposition-based cryptography that the Spartan *scytale* had already introduced to Greece, but that he preferred simpler steganographic modes of secret communication. Aeneas Tacticus, namely, concentrates exclusively upon modes of secret communication that would have been suited to the military siege contexts which form the focus for his work – and as such values steganographic over cryptographic devices and methods.²⁶⁶ For, out of twenty-one methods for secret communication one can only see two examples of cryptography (Aeneas Tacticus, *How to Survive Under Siege*, 31.30-31; 31.31). And although Aeneas Tacticus does not directly discuss the *scytale* in his chapter on secret communication, his writings do reveal that he was familiar with the principle of transposition ciphers. He discussed three different transposition ciphers (Aeneas Tacticus, *How to Survive Under Siege*, 31.16-19; 31.20; 31.21-22) – and was also familiar with the key concept of transposition-based cryptography that the Spartan *scytale* had already introduced to Greece. Yet, he seems to have preferred simpler steganographic modes of secret communication – presumably since hidden messages would have attracted less attention than encrypted message in a siege context in which many enemies could always have been nearby.

3.1: Reasons for the absence of the *scytale* in *How to Survive Under Siege*

There are a number of conceivable reasons to explain the fact that Aeneas Tacticus did not discuss the Spartan *scytale* directly in his work *How to Survive Under Siege*. First, it is possible

²⁶⁶ See also Kahn 1996b, xvii; Reba & Shier 2015, 480; Singh 1999, 11.

(though perhaps not probable) that he simply did not know of the *scytale*'s potential or actual use by the Spartans as a cryptographic device at the time of writing *How to Survive Under Siege*. For if, as this thesis maintains, the *scytale* was used by the Spartans for secret encrypted communication, it was most likely used in the late 5th and early 4th centuries BCE – that is, between the outbreak of the Peloponnesian War and the Battle of Leuctra, since in this period Spartan commanders were away from home and would have therefore been in need of such devices to enable long distance communications during their operations in the field.²⁶⁷ This period also matches with the time-frame in which Plutarch later maintains that key Spartan figures – including Lysander and Agesilaus – received coded messages by *scytale* (Plutarch, *Life of Lysander*, 20; *Life of Agesilaus*, 10.5; 15.4-6). Aeneas Tacticus wrote his work *How to Survive Under Siege* in the mid-4th century BCE, so it is just possible that the military use of the *scytale* for secret communication by the Spartans in the early 4th century BCE was not yet known by the Greeks – since the Spartans would obviously not have wanted the secret of the *scytale* to be written about at the time when the device was in actual use for secret communication.²⁶⁸ Secondly, and more importantly, the *scytale* would have been used by the Spartans for long distance communication and field warfare, while Aeneas Tacticus instead focused on surviving a siege in the closed quarters of a besieged town. In his work he showed the inhabitants of a *polis* whose city and homeland were endangered – especially those inhabitants who were in charge of maintaining the *polis*' security – that there was the constant danger of treachery from *within* the city itself during sieges. The main focus in *How to Survive Under Siege* is upon hiding messages so as to smuggle them in and out of the besieged *polis* and not upon encoding them so as to prevent their being read and understood by hostile agents (either within or without the city walls). Indeed, this is a recurring theme throughout Aeneas

²⁶⁷ Kelly 1985, 143.

²⁶⁸ David 1986 (I), 343; Spence 2010, 26; Whitehead 1990, 9-12.

Tacticus' whole work, in which he made clear that establishing secure and mutually-comprehensible means of secret communication were of vital importance. The *polis*' inhabitants had to secure all forms of communication that went in and out of the city (Aeneas Tacticus, *How to Survive Under Siege*, 4.1-4; 5.1; 9.2; 10.6; 10.11; 10.18-19; 10.25-26; 11.3-6; 12; 18.3-6; 18.8-11 (see also Polyaeus, *Stratagems of War*, 2.36); 18.13-21; 20; 22.5; 22.7; 23.7-11; 29.3-10).²⁶⁹ Given the significant risk of citizens within the *polis* conspiring and communicating with the enemy, it was vital for the commanding forces to be able to communicate between themselves secretly and securely in Aeneas Tacticus' view. All methods for secret communication that Aeneas Tacticus discussed in chapter 31 of the work are related to this theme of internal treachery, and to his idea of an enemy who is always nearby. As the sources discussed in the previous chapter demonstrate, *scytalae* would typically have been used for long distance communication rather than for the sort of local communications that concerned Aeneas Tacticus. Aeneas Tacticus, therefore, might well have known the use of the *scytale* for long distance communication, but he would not have seen it as a fit subject for his own work, with its particular focus on local communication in a time of siege. Moreover, it seems that Aeneas Tacticus did not have much knowledge of Sparta. From the textual evidence supplied by *How to Survive Under Siege* it appears that Aeneas Tacticus' military experience is almost wholly confined to the geographical limits of parts of the Peloponnese and the western coast of Asia Minor (Aeneas Tacticus, *How to Survive Under Siege*, 10; 11). Aeneas Tacticus never mentioned Sparta or a Spartan in his work.²⁷⁰ What is more, Aeneas Tacticus – living and writing in the middle of the 4th century BCE (that is, after the Peloponnesian War) – may well have seen Spartan devices like the *scytale* as 'un-Greek' and as unworthy of inclusion in

²⁶⁹ Burliga 2008; Pretzler 2018 (I); Liddel 2018, 123; Rawling 2007, 139; Spence 2010, 26; Shipley 2018; Whitehead 1990, 4; 20-24; Williams 1904, 390.

²⁷⁰ In 31.14 of *How to Survive Under Siege* he discussed Herodotus' story of Demaratus without mentioning any names or places. Aeneas Tacticus simply stated that someone had once written under the wax of a wax tablet.

his treatise accordingly. He might, therefore, have excluded such an alien and ‘un-Greek’ device from his list of techniques for Greeks to survive during the sieges even if he had been familiar with such stratagems. A final reason for excluding the Spartan *scytale* from the treatise may be that Aeneas Tacticus was simply more interested in steganographic practices than cryptographic practices. As will be discussed in the next section, out of twenty-one methods for secret communication we can only see two examples of cryptography (Aeneas Tacticus, *How to Survive Under Siege*, 31.30-31; 31.31). This fits in perfectly with the aim of Aeneas Tacticus’ chapter 31 which is to teach inhabitants of a *polis* how to hide messages from enemies that were always nearby. Coded yet unhidden messages would obviously have attracted too much attention in such situations (as we have already seen in Herodotus’ work; see chapter 1) making steganographic methods of communication preferable over those that were purely cryptographic.

3.2: Aeneas Tacticus’ methods for cryptography and steganography

In chapter 31 of *How to Survive Under Siege* Aeneas Tacticus discussed twenty-one²⁷¹ different methods for secret communication that can be divided into fifteen examples of steganography (31.4-5 (3x); 31.6; 31.7; 31.8; 31.9-9b; 31.10-13; 31.14; 31.15; 31.15-16; 31.23; 31.25-27; 31.28-29; 31.31-32), two examples of cryptography (31.30-31; 31.31) and a further four

²⁷¹ The *astragalos* (pl. *astragali* or *astragaloï*) is a dice-like gaming piece made from knucklebones. Hunter and Handford discuss eighteen different methods, but they do not discuss the two variations of the *astragali* method (a.k.a. as knucklebones method) separately (see 3.2.3.2). Instead, they see only one variation (Hunter & Handford 1927, 211). Yet, I believe this distinction to be crucial since the two variations are clearly different methods.

examples that are a combination of cryptography and steganography (31.1-3; 31.16-22).²⁷² Of the examples Aeneas Tacticus offers of cryptographic devices and of crypto-steganographic combinations there are three examples of transposition ciphers (31.16-19; 31.20; 31.21-22) and three examples of substitution ciphers (31.10-13; 31.30; 31.31). As Whitehead points out, this makes the collection the fullest accumulation of cryptographic and steganographic devices known from antiquity – so it is certainly striking that the *scytale* is not included within this catalogue, especially since secret communication was clearly a subject of enormous fascination for Aeneas Tacticus.²⁷³ Other scholars argue that there was no clear categorisation in the methods for secret communication discussed in Aeneas Tacticus’ work: the author simply discussed a sample range of methods covering,²⁷⁴ as Liddel argues:

a variety of (a) means of physical transference of written objects, (b) means of concealment and (c) of the materials used for writing.²⁷⁵

However, as my own classification above makes clear, Aeneas Tacticus is clearly far more knowledgeable about and interested in steganographic devices for secret communication than in encrypted messaging (i.e. cryptography). That is, his main focus in *How to Survive Under Siege* is upon hiding messages so as to smuggle them in and out of the besieged *polis* because of a constant danger of treachery from within a city during sieges (Aeneas Tacticus, *How to Survive Under Siege*, 4.1-4; 5.1; 9.2; 10.6; 10.11; 10.18-19; 10.25-26; 11.3-6; 12; 18.3-6; 18.8-11 (see also Polyaeus, *Stratagems of War*, 2.36); 18.13-21; 20; 22.5; 22.7; 23.7-11; 29.3-10),

²⁷² In another now lost work Aeneas Tacticus also discussed a method for fire signalling used in secret communication (Aeneas Tacticus, *How to survive under Siege*, 7.1-4; Polybius, *Histories*, 10.44-46). On this method, Polybius’ improvements, and its application in the German ADFGX and ADFGVX ciphers used by the German military intelligence services in the First World War see Diepenbroek 2019, 63-76 and the prologue to this work.

²⁷³ Whitehead 1990, 183; 187.

²⁷⁴ Debidour 2006; Liddel 2018, 135; Rance 2018, 313.

²⁷⁵ Liddel 2018, 135.

and not upon encoding messages so as to prevent them from being read and understood by hostile agents (either within or without the city walls) – a point that previous scholars have not picked up upon before. Various methods of secret communication discussed in the work seem to have been Aeneas Tacticus’ own inventions – especially the use of *astragali* and its variations (31.16-22), while other methods have clearly been based on reports and descriptions found in historical sources – especially Herodotus’ *Histories* (31.14 = Herodotus, *Histories*, 7.239; 31.25-27 = *Histories*, 8.128; 31.28-29 = *Histories*, 5.35; 37.6 = *Histories*, 4.200; see also 2.3-6 = Thucydides, *History of the Peloponnesian War*, 2.2-6 (esp. 4); 27.11 = Xenophon, *Anabasis*, 2.2.20), alongside other unspecified oral and/or written sources.²⁷⁶ Yet – as we will see – when Aeneas Tacticus used one of these secondary sources he then nuanced the method for secret communication discussed in the source with his own ideas – presumably since he believed that his own alternatives (based on his own first-hand tried and tested experiences, perhaps, were improvements upon the original method.²⁷⁷ Again, we can only speculate, but it may be that Aeneas Tacticus omits the *scytale* from his list because he has no direct experience of using it in military practice in the field. Indeed, in this context it makes perfect sense that Aeneas Tacticus did not devote any specific attention to the Spartan *scytale* in his treatise.

²⁷⁶ Throughout chapter 31 Aeneas Tacticus discussed many times that he knew or had heard that something had once happened without specifying his sources (*How to Survive Under Siege*, 31.1-2; 31.6; 31.8-9b; 31.10-14; 31.23; 31.24-29; 31.32-35). On Aeneas Tacticus’ sources see Bettalli 1990; Brown 1981; Dain & Bon 1967; David 1986 (I); David 1986 (II); Hunter & Handford 1927; Luraghi 1988; Vela Tejada 1991, 37-43; Vela Tejada & Garcia 1991; Whitehead 1990.

²⁷⁷ On examples of Aeneas Tacticus’ personal experience discussed in *How to Survive Under Siege*, see Burliga 2008.

3.2.1: Methods for steganography

As we have seen, a careful cataloguing of the different types of secret communication that Aeneas Tacticus discussed in his treatise indicates that he was most familiar with simple steganographic devices for secret communication – and preferred these over encrypted messaging for siege contexts. To understand why Aeneas Tacticus may have omitted the *scytale* – a relatively sophisticated cryptographic device – from his catalogue, it is useful to look in detail at those devices and stratagems which he does discuss.

3.2.1.1: Covered writing on tablets

In chapter 31.14 of *How to Survive Under Siege* Aeneas Tacticus discussed a relatively straightforward strategy of secret communication involving the concealment of writing under the wax of a wax-tablet. According to Aeneas Tacticus, a non-encrypted secret message would be written on the base of a tablet and then wax was poured over it, and a second – open message would be written on the top film of wax. When this tablet was delivered, the recipient – who knew or anticipated that a message was written under the wax – would scrape off the wax to read the message hidden underneath and send any reply in the same way:

ἤδη δέ τις ἐν δέλτου ξύλῳ γράψας κηρὸν ἐπέτηξεν καὶ ἄλλα εἰς τὸν κηρὸν ἐνέγραψεν. εἴτα ὅταν ἔλθῃ παρ' ὃν ἔδει, ἐκκνήσας τὸν κηρὸν καὶ ἀναγνοὺς γράψας πάλιν ὡσαύτως ἐπέστειλεν. ἐνδέχεται δὲ καὶ εἰς πυξίον γράψαντα μέλανι ὡς βελτίστῳ ἔαν ξηρανθῆναι, ἔπειτα λευκώσαντα ἀφανίζειν τὰ γράμματα. ὅταν οὖν ἀφίκηται παρὰ τὸν πεμπόμενον, λαβόντα εἰς ὕδωρ θείναι τὸ πυξίον· φανεῖται οὖν ἐν τῷ ὕδατι ἀκριβῶς ἅπαντα τὰ γεγραμμένα (Aeneas Tacticus, *How to Survive Under Siege*, 31.14; for the complete passage see Appendix 1, page 258).

It has actually happened that someone has written on the wooden part of a tablet, poured wax over it, and written something else on the wax. Then when it came to the appointed person, he, scraping off the wax and reading the writing, again in the same way has sent back a message.

This example is clearly based upon the story of Demaratus' message to the Spartans derived from Herodotus' *Histories* (7.239; see § 1.2.5; see also Aulus Gellius, *Attic Nights*, 17.9.6; Julius Africanus, *Kestoi*, 53; Justin, *Epitome of the Philippic History of Pompeius Trogus*, 2.10.13; Polyaeus, *Stratagems of War*, 2.20. See for a parallel from Roman times: Herodian, *History of the Empire from the Death of Marcus*, 7.6.5).²⁷⁸ However, Aeneas Tacticus did not simply follow Herodotus' earlier account verbatim. After discussing the means by which Demaratus sent a secret message to the Spartans – following the details of his Herodotean source closely – Aeneas Tacticus suggested that a message was sent back in the same way (ἔπειτα λευκώσαντα ἀφανίζειν τὰ γράμματα; Aeneas Tacticus, *How to Survive Under Siege*, 31.14) – as if this were a useful practical way of secret communication that had taken place between two parties. He then added two other possibilities, as if to show that he could improve on his sources by supplementing them with ideas of his own. It is plausible that Aeneas Tacticus (quite sensibly) believed that a seemingly empty tablet in transit would have attracted too much suspicion if it fell into the wrong hands. Instead of using an ostensibly blank wax tablet as Herodotus reports that Demaratus did, Aeneas Tacticus, therefore, suggested that a non-secret message was written on the top of the wax tablet.

Aeneas then suggested two other variations. First, that it was possible to write a message on the base of a boxwood tablet, and then whitewash the tablet and perhaps paint a picture over it to render the writing invisible. To make the writing visible again a recipient had to place the tablet in water to dissolve the paint (ἐνδέχεται δὲ καὶ εἰς πυξίον γράψαντα μέλανι ὡς βελτίστῳ ἔαν ξηρανθῆναι, ἔπειτα λευκώσαντα ἀφανίζειν τὰ γράμματα. ὅταν οὖν ἀφίκηται παρὰ τὸν πεμπόμενον, λαβόντα εἰς ὕδωρ θεῖναι τὸ πυξίον· φανεῖται οὖν ἐν τῷ ὕδατι ἀκριβῶς ἅπαντα τὰ

²⁷⁸ When using a source Aeneas Tacticus did not literally quote it. Instead he paraphrased his sources in order to bring out his own points in the clearest way, thereby omitting unessential details and sometimes adding information to the original (Brown 1981, 388; Burliga 2008; Pretzler 2018 (I); Shipley 2018).

γεγραμμένα [...] It would be possible, also, to write on a boxwood tablet with the best quality of ink, let it dry, and then by whitening the tablet to make the letters invisible. When, then, the tablet comes to the recipient, he should take it and put it into water; and so in the water there will clearly appear all that was written; Aeneas Tacticus, *How to Survive Under Siege*, 31.14-15).

Aeneas Tacticus' second alternative suggestion was to use a hero's plaque for the same purpose (γράφοιτο δ' ἂν καὶ εἰς πινάκιον ἡρωϊκὸν ἅπερ ἂν βούλῃ. ἔπειτα καταλευκῶσαι καὶ ξηράναντα γράψαι ἵππεά φωσφόρον ἢ ὅ τι ἂν βούλῃ, ἔχοντα ἱματισμὸν λευκὸν καὶ τὸν ἵππον λευκὸν [...] You might also write on a tablet for a hero's chapel whatever you desire. Then it should be whitened and dried, and a light-bringing horseman painted on it, or anything else you please; 31.15-16).²⁷⁹

Clearly Aeneas Tacticus considered that his alternatives would have worked more effectively as practical steganographic devices than the original method described by Herodotus.

3.2.1.2: The tattooed slave

As in the example of Demaratus (Aeneas Tacticus, *How to Survive Under Siege*, 31.14), Aeneas Tacticus based another example of secret steganographic communication on Herodotus. In 31.28-29 Aeneas Tacticus discussed the Herodotean story of Histiaeus' message to Aristagoras tattooed on a slave's head. Since the roads were guarded Histiaeus had to find a safe way to send his message. He did so by:

τῶν δὲ δούλων τὸν πιστότατον ἀποζυρήσας ἔστιξεν καὶ ἐπέσχεν ἕως ἀνέφυσαν αἱ τρίχες. ὥς δὲ ἀνέφυσαν τάχιστα, ἔπεμπεν εἰς Μίλητον, ἐπιστείλας τῷ ἐπεστιγμένῳ ἄλλο μὲν οὐδέν, ἐπειδὴν δ' ἀφίκηται εἰς Μίλητον πρὸς Ἀρισταγόραν, κελεύειν ζυρήσαντα κατιδεῖν εἰς τὴν κεφαλὴν. τὰ δὲ στίγματα ἐσήμαινεν ἃ ἔδει ποιεῖν (Aeneas Tacticus, *How to Survive Under Siege*, 31.28-29; for the complete passage see Appendix 1, page 260)

²⁷⁹ In this second example presumably another type of paint would be used since Aeneas Tacticus recommends that oil was needed to dissolve the painting instead of water (31.16).

shaving the head of his most faithful slave, he [then] tattooed it and detained him until the hair had grown again. And as soon as it had grown, he dispatched [the slave] to Miletus and gave the tattooed man no other orders except that when he had come to Miletus, into the presence of Aristagoras, he should request him to shave his head and examine it, whereupon the marks indicated what was to be done.

This example from Herodotus again fits in well with the broader theme of Aeneas Tacticus' work on sieges, since here we are dealing once again with a hidden message being smuggled out of a besieged city (Herodotus, *Histories*, 5.35.2-4; see also Aulus Gellius, *Attic Nights*, 17.9.18-27; Polyaeus, *Stratagems of War*, 1.24). Indeed, this case is included as an example of the importance of the use of trustworthy messengers for secret communications during a siege – a recurring theme in Aeneas Tacticus' work (Aeneas Tacticus, *How to Survive Under Siege*, 9.2; 10.6; 10.11; 10.25-26; 22.5; 22.7; 31). Unlike his reworking of the Demaratus' story reported by Herodotus, however, here Aeneas Tacticus included the names (Histiaeus; Aristagoras) and places (Miletus) that Herodotus had supplied in his version – thereby lending credibility and authority to his own account.

3.2.1.3: Hidden Messages

Aeneas Tacticus discussed seven further examples of steganographic messages that could be sent hidden in or under clothing, footwear, armour, jewellery, and even a dog collar (for the complete passages see Appendix 1, page 255-261).²⁸⁰ Amongst his simple suggestions were to hide a message under a breastplate (Aeneas Tacticus, *How to Survive Under Siege*, 31.8), to sew one into a bridle-rein (31.9-9b), or to hide it in between layers of clothing (31.23; see also Julius Africanus, *Kestoi*, 53; Philo of Byzantium, *Compendium of Mechanics*, D.78 (102.37–39) in: Thévenot, Boivin, et al., 1693, *Veterum Mathematicorum Opera*, 102. See for

²⁸⁰ Four examples seem to be based on Aeneas Tacticus' sources (31.6; 31.23; 31.25-27; 31.31-32), while three examples were his own suggestions (31.4-5; 31.7; 31.9; 31.9).

a Roman parallel: Ammianus Marcellinus, *Roman History*, 18.6.17-19; Frontinus, *Stratagems*, 3.13.3-6; Florus, *Epitome of Roman History*, 1.40.15-16; Orosius, *Seven Books of History Against the Pagans*, 6.2.14). Aeneas Tacticus also discussed how a message was once sent bound to a wound on a man's leg (31.6), and how in Epirus and Thessaly it was the custom to take a dog away from his home, hide a secret message in its collar, and then sent it back home (31.31-32; see for a parallel from Roman times: Frontinus, *Stratagems*, 3.13.5-8; Pliny, *Natural History*, 10.53 (37)).²⁸¹ A slightly more complicated method compared to these is found in 31.7 – where Aeneas Tacticus suggested to write messages on pieces of lead that could be rolled up and worn as women's earrings (see for a parallel from Roman times: Cassius Dio, *Roman History*, 46.36; Frontinus, *Stratagems*, 3.13.7). Significantly, the lead could be rolled up, making it possible to send a closed and sealed message hidden in plain sight. This makes the method a very clear example of Aeneas Tacticus' interest in hiding messages rather than encrypting them.

Another slightly more complicated method can be found in 31.4-5. Here Aeneas Tacticus discussed the sending of secret messages by using a messenger without the messenger knowing about this. Before sending out the messenger the sender had to insert a secret letter into the messenger's sandals.²⁸² He would then send the messenger to the recipient with a non-secret letter to provide a cover for his actual mission. The recipient could reply in the same way if requested (31.4-5; for the complete passages see Appendix 1, page 255-256; see also Julius Africanus, *Kestoi*, 51; Philo of Byzantium, *Compendium of*

²⁸¹ A link can be made to the use of animals as secret messengers in the 20th century. For the role of carrier pigeons in the Second World War, see e.g.: O'Connor 2018.

²⁸² To make sure that the hidden message was not affected by water and mud, Aeneas Tacticus suggested that it be written on a piece of lead (31.4). Whitehead incorrectly presumes that Ovid suggested this same method in *Ars Amatoria*, 3.624 (Whitehead 1990, 184). However, Ovid simply mentioned that one could hide a letter between a foot and a sandal amongst a selection of simple methods to quickly and easily communicate in secret (*Art of Love* 3.619-630).

Mechanics, D. 81 (102. 45-50). In: Thévenot, Boivin, et al. 1693, *Veterum Mathematicorum Opera*, 102).²⁸³ These seven examples show Aeneas Tacticus' interest in steganographic messages that were hidden in simple ways – sometimes almost in plain sight – by using commonly known household objects.

In chapter 31.10-13 Aeneas Tacticus discussed some no less simplistic though rather more laborious way of sending secret messages by using an oil-flask and a bladder. According to Aeneas Tacticus, one could inflate a bladder and write on it with ink mixed with glue. Once the writing was dry one had to deflate the bladder, press it into a flask, and inflate it again. Hereby, the glue would stick the bladder to the insides of the flask. Then one had to fill the flask – or technically the bladder lining it – with oil. In this way, the bladder would have become (nearly) invisible. Upon receiving the flask, the recipient had to pour out the oil, re-inflate the bladder and read the text.²⁸⁴ He could then wipe off the text with a sponge and reply in the same way:

κύστιν [...] ἀποδήσαντα σφόδρα ξηρᾶναι, ἔπειτα ἐπ' αὐτῆς γράψαι ὅ τι ἂν βούλη μέλανι κατακόλλω. ξηρανθέντων δὲ τῶν γραμμάτων ἐξελεῖν τὴν πνοὴν τῆς κύστιδος καὶ συμπίεσαντα [...] τὸ δὲ στόμα τῆς κύστιδος ὑπερέχτω τοῦ στόματος τῆς ληκύθο [...]. ὅταν δὲ ἔλθῃ παρ' ὃν δεῖ, ἐξεράσας τὸ ἔλαιον ἀναγνώσεται φουσίσας τὴν κύστιν· καὶ ἐκπογγίσας καὶ κατὰ ταῦτα εἰς τὴν αὐτὴν γράψας ἀποστελλέτω (Aeneas Tacticus, *How to Survive Under Siege*, 31.10-13; for the complete passage see Appendix 1, page 257-258).

Take a bladder [...]; inflate it, tie it tightly, and let it dry; then write on it whatever you wish, in ink mixed with glue. When the writing is dry, let the air out of the bladder, and press it into the flask [...]. Then inflate the bladder inside the flask [...] and [fill] it with oil [...]. When it comes to the appropriate person, he will

²⁸³ This method could have been useful if one did not trust his messenger.

²⁸⁴ This is not an example of the use of invisible ink since the recipient simply had to pour out the oil to be able to read the text again. He did not have to use e.g. charcoal to make the text visible again. For the use of invisible ink in antiquity see Ausonius, *Epistles*, 28.21-22; Ovid, *Ars Amatoria*, 3.627-630; Philo, *Compendium of Mechanics*, D. 77 (102.31-36); Pliny the Elder, *Natural History* (26.39 (62)).

pour out the oil, inflate the bladder, and read the writing. And washing it off with a sponge, let him write on it in the same manner and send it back.

This particular method of steganographic communication is not only laborious but demands access to a panoply of domestic supplies. Indeed, such a method for securing the secret communication of hidden (though not encoded) messages would have been highly impractical on a battlefield – since both parties would have needed flask, bladders, ink, glue, and oil, etc. However laborious, the method might have been useful as a means of securing a secret communication in a siege defence – and therefore offers us a salient reminder that this is the specific context of Aeneas Tacticus’ work. Aeneas Tacticus’ predominant focus in his treatise on *How to Survive Under Siege* is upon providing his readers with a catalogue of devices and stratagems suitable for secret communication under siege conditions. His priorities are upon smuggling concealed messages in and out of the *polis* or city – and he focuses upon concealment rather than encryption as the first priority in securing these communications. In fact, so confident is he in the security of these various steganographic devices, he has comparatively little to say about the risks of these messages being intercepted and read by hostile agents. In fact, there are only two examples in *How to Survive Under Siege* in which Aeneas Tacticus appears to take seriously such a risk and to mitigate against it by sending a hidden message that is also – for extra security – encrypted or encoded in some way.

3.2.2: Methods for cryptography

Aeneas Tacticus’ only two suggestions for the use of cryptography can be found in passage 31.30-31. In this passage Aeneas Tacticus suggested that, instead of marking a slave’s head – or any other medium for a secret message – with easily recognisable words or letters, one could instead write by replacing vowels with dots (Aeneas Tacticus, *How to Survive Under Siege*,

31.30-31), or any other letter or symbol (31.31).²⁸⁵ In the first part of the passage (31.30-31), Aeneas Tacticus suggested that each vowel from *alpha* to *omega* could be replaced by one to seven dots – the ancient Greek alphabet having seven vowels (*α; ε; η; ι; ο; υ; ω*):

γράμματα ἐν κεντήμασι τίθεσθαι, ὅποσον δ' ἂν τύχη ἕκαστον ὄν, ἐν τοῖς γραφομένοις τοσαύτας στιγμὰς εἶναι (Aeneas Tacticus, *How to Survive Under Siege*, 31.30-31; for the complete passage see Appendix 1, page 260-261).

It [is possible to] express the vowels by dots, and whatever the number of each vowel happens to be, so many dots are to be placed in the writing.

Aeneas Tacticus then continued by discussing that instead of substituting vowels with dots, one could have put in any letter, number or symbol (*καὶ τόδε ἄλλο· ἀντὶ τῶν φωνηέντων γραμμάτων τίθεσθαι ὃ τι δὴ [...]* *And here is another way: Instead of the vowels, put in anything whatever*; 31.31). When discussing this passage, scholars – starting with Von Gutschmid in 1880 – have typically focused upon attempting to link this example to the war between Dionysius II of Syracuse, and his opponents Dion and Heracleides in 357 BCE (see also Plutarch, *Dion*; Timonides, Fragment 1, in: Brill's New Jacoby (561)); Timaeus, Fragment 114; in: Brill's New Jacoby (566).²⁸⁶ They seem to have overlooked the fact that this short passage provides the only two suggestions of cryptographic methods out of the total sum of twenty-one methods for secret communication that Aeneas Tacticus discussed in chapter 31 of his work. Yet, the fact that we can only find these two examples of cryptographic messages here, clearly shows that Aeneas Tacticus was far more interested in steganographic (hidden) messages than in cryptographic (coded) messages. The encoded messages created here by using this very basic form of encryption through partial substitution would help to add an additional

²⁸⁵ Bauer – based on Hunt 1929 – suggests that the ancient Greeks were familiar with the cryptographic principle of replacing letters by other letters (Bauer 2017, 96).

²⁸⁶ Bengtson 1962, 460; Glotz & Cohen 1936, 410-411; Dain & Bon 1967, 75; Oldfather 1928, 5-7; Von Gutschmid 1880, 588-590; Whitehead 1990, 191.

layer of security should the messenger-slave be intercepted by hostile agents and his head shaved to reveal the message on his scalp.²⁸⁷ Aeneas Tacticus' methodology here represents the first known substitution cipher recommended for use in warfare – but it is important not to overlook the fact that it is presented by Aeneas Tacticus as a secondary device, an insurance policy of sorts, to support his primary stratagem recommending a steganographic approach as the foundation to successful secret communication.

3.2.3: Combinations of cryptography and steganography

3.2.3.1: Marking letters in text

The first example of a method that involves a combination of cryptography and steganography can be found at the start of chapter 31 of *How to Survive Under Siege*. In passage 31.1-2 Aeneas Tacticus discussed how a message could be written by marking letters in a book or document with dots and the book or document with the message then hidden in baggage. The recipient had to make a transcript of all the marked letters to understand the message (ἐν τούτῳ δὲ γέγραπται ἡ ἐπιστολὴ ἐπιστιζομένων γραμμάτων τοῦ πρώτου στίχου ἢ δευτέρου ἢ τρίτου, ἐπιστιγμαῖς δὲ ἐλαχίσταις καὶ ἀδηλοτάταις πλὴν τῷ πεμπομένῳ. εἴτα ἀφικομένου τοῦ βιβλίου παρ' ὃν δεῖ, ἐξεγράφετο καὶ τὰ ἐπισεσημασμένα γράμματα τιθεὶς ἐφεξῆς τὰ ἐκ τῶ πρώτου στίχου καὶ δευτέρου καὶ τὰ ἄλλα ὡσαύτως, ἐγνώριζε τὰ ἐπισταλέντα; [...]) In one case a message was sent in this way: in with merchandise or other baggage there was inserted a book, or some other chance document, of any size or age, and in this the message had been written by marking the letters of the first, second, or third line with dots, very small and discernible only to the recipient. Then, when the person intended received the book, he made a transcript, and by setting down in

²⁸⁷ From around 600-500 years BCE Hebrew scholars were already using a substitution system known as the *Atbash* cipher and Aeneas Tacticus may have based his simple cipher on this model. See Strasser 2007, 278.

order the marked letters from the first line and the second and the others in the same way he discovered the message; 31.1-2; for the complete passage see Appendix 1, page 255). As an alternative, Aeneas Tacticus suggested that instead of using a book or document as the vehicle for the message, one could simply write a letter and then add the markings (*ἐπιστολὴν γράψαντα περὶ τινῶν φανερώς ἐν πλείοσιν, ἐν ταύτῃ τῇ ἐπιστολῇ τὸ αὐτὸ ποιεῖν ἐπισημαινόμενον γράμματα, δι' ὅτων ἐμφανιεῖς ἅπερ ἂν βούλῃ [...]* Writing in detail and undisguisedly on some subject, in this message you may reach the same result by marking letters by which you will indicate whatever you may wish; Aeneas Tacticus, *How to Survive Under Siege*, 31.3; for the complete passage see Appendix 1, page 255) – which obviously had to be as inconspicuous as possible by placing them far apart and making them as small as possible (*τὴν δὲ ἐπισημασίαν εἶναι ὥς ἀδηλοτάτην ἐπιστιγμαῖς διὰ πολλοῦ ἢ γραμμαῖς παραμήκεσιν*; 31.1-3). Clearly marked letters in a text would have attracted suspicion – especially for trained people who would have been trying to uncover their enemy's secrets, and especially if there were a pattern in the text with e.g. every third letter being marked. One, therefore, had to avoid clear marking and patterns when using this technique. The combination of cryptographic and steganographic encryption here, as in the previous case, makes the method more secure. However, Aeneas Tacticus is clearly less confident in the protection offered by encryption than he is in the protection offered by concealment. Although he has recommended numerous steganographic techniques that work (so he suggests) on their own, here he once again recommends that the coded message or text is also hidden and concealed in a bag in order to secure its transmission. His personal preference for secure secret messaging falls clearly to the side of steganography rather than cryptography.

3.2.3.2: The use of astragali

A possible explanation for Aeneas Tacticus' comparative lack of confidence in cryptographic devices – and accordingly for his lack of interest in the Spartan *scytale* – may be traced to his account in his treatise of the use of *astragali* (also known as knucklebones or *talus* bones) to send secret messages (31.16-22). Aeneas' use of *astragali* is discussed for the first time in modern cryptographic scholarship by Hunter and Handford in 1927.²⁸⁸ As becomes clear from Aeneas Tacticus' description, one could pierce 24 holes into an *astragalus* to represent the 24 letters of the Greek alphabet. Only knucklebones of hooved animals – like sheep or goats – were useful for this purpose since these are almost square or rectangular and, therefore, have four more or less flat sides, on to which the 24-letter Greek alphabet naturally fell in to four neat groups of six letters.²⁸⁹ Whenever someone wanted to communicate a message by using an *astragalus*, this person had to draw a thread through its holes. In other words, he would 'sew' a message through an *astragalus* and this transposing of letters would compose a simple transposition cipher.²⁹⁰

ἀστράγαλον [...] τρυπήματα εἴκοσι καὶ τέτταρα [...]· ἔστω δὲ τὰ τρυπήματα τοῦ ἀστραγάλου στοιχεῖα. μετὰ δὲ ταῦτα, ὅταν τινὰ θέλῃς ἐν αὐτοῖς τίθεσθαι λόγον, [...] οὕτω τὰ ἐπίλοιπα τοῦ λόγου ἀντιγράφων ἔνθειρε εἰς τὰ τρυπήματα [...] ἀνάπαλιν [...] γίγνεται ἡ ἔξερσις τῇ ἐνέρσει (Aeneas Tacticus, *How to Survive Under Siege*, 31.16-19; for the complete passage see Appendix 1, page 258-259).

In [an] *astragal* bore twenty-four holes [...]. Let the holes stand for letters [...] whenever you wish to communicate any word by them [...] pass the thread into the holes. [...] The unthreading takes place in the reverse order to that of the threading.

²⁸⁸ Hunter & Handford 1927, 209.

²⁸⁹ Olivetti 2015, 263.

²⁹⁰ It is plausible that Aeneas Tacticus tried out the method before putting it into practice. In passage 31.18, namely, he discussed how to 'write' his own name by pulling a thread through the holes of the *astragalus*.

The unthreading obviously took place in the reverse order, since the decoding necessarily started by unthreading at the end. Consequently, all the letters of the message appeared in reverse order. Therefore, to understand the intended message properly, the recipient had to turn the letters back into their normal order. Because of its size, a message sent using an *astragalus* could not have been much longer than one or two words or a very short sentence. The message ‘*Enemy Attacks At Dawn*’ could, for example, have been abbreviated to *EAAD*. Yet, the use of such a small object must have made the use of *astragali* for this form of secret communication very time consuming and very difficult in practice. One would easily end up with a ball of thread whereby it was no longer possible to find the correct holes – making the use of *astragali* rather troublesome for the sender, and even more so for the receiver, as Whitehead, and Hunter and Handford point out.²⁹¹ Therefore, it is questionable whether the method may have functioned well. It seems plausible that Aeneas Tacticus found out for himself that using the *astragali* for secret communication was laborious, since he described the method not only as the most secret, but also the most difficult (or ‘troublesome’ as Whitehead translates it):

Πασῶν δὲ ἀδηλοτάτη πέμψις, πραγματωδεστάτη δὲ νῦν μοι ἢ δι’ ἀγραμμάτων ἐμφανισθήσεται (Aeneas Tacticus, *How to Survive Under Siege*, 31.16)

I shall now describe the most secret – and most troublesome – method of all: sending a message without writing.²⁹²

Since the method was rather complicated and very time consuming, Aeneas Tacticus accordingly suggested two simpler variations. Instead of an *astragalus* one could either use a rectangular piece of wood (εὐτρεπέστερον ἂν τοῦτο γίγνοιτο ξύλου ὥς σπιθαμιαίου τρυπηθέντος ὅσα γε τὰ στοιχεῖα τῶν γραμμάτων [...]) *this would be accomplished more easily if a piece of wood*

²⁹¹ Hunter and Handford 1927, lxxxii; Whitehead 1990, 187.

²⁹² Whitehead 1990, 87. If no actual writing is involved in cryptography, one speaks of a semagram (Chatton 2010, 43; Lunde 2012, 42).

about a span long were perforated just as many times as there are letters in the alphabet; 31.20) or a wooden disk (ἀντὶ τοῦ ἀστραγάλου καὶ ξύλου ποιήσαντα κύκλον ξύλινον λεᾶναι [...] *Instead of the astragal or the piece of wood, make a disc of wood*; 31.21-22; for the complete passage see Appendix 1, page 258-259) in which one would then pierce 24 holes as in the bone *astragalus*. When using the disk – Aeneas Tacticus suggested – one had to prick holes in the centre of the disk too. Whenever a letter occurred twice in a row, one had to pull the thread through one of the holes in the centre in between the two other letters (31.22).

Two possible reconstructions show what this disk might have looked like. Figure 11 (left) shows Diels' suggestion in which the letters α (*alpha*) to ω (*omega*) are written clockwise in their normal order at the edge of the disk. Diels incorrectly describes this as a reconstruction of an *astragalus* while it clearly represents Aeneas Tacticus' wooden disk.²⁹³ Figure 11 (right) shows Welskopf's reconstruction in which the first four letters – (α (*alpha*), β (*beta*), γ (*gamma*) and δ (*delta*)) – can be found at the top (α (*alpha*)), bottom (β (*beta*)), and left (γ (*gamma*)) and right side (δ (*delta*)) of the disk as on a compass where north, south, east and west are pointed out. The rest of the letters can be found right opposite each other on the disk starting at the top with ϵ (*epsilon*) to the right side of α (*alpha*), ζ (*zeta*) to the left side of β (*beta*), η (*eta*) to the right side of ϵ (*epsilon*), θ (*theta*) to the left side of ζ (*zeta*) and so on (see Figure 11 (right)).²⁹⁴ Aeneas Tacticus pointed out that one had to know which hole represented α (*alpha*), since from there all subsequent letters had been 'written' on the four sides (Aeneas Tacticus, *How to Survive Under Siege*, 31.17) – and presumably 'written' in alphabetical order to avoid making this already complex method yet more complex again.

²⁹³ Diels 1914, 67.

²⁹⁴ Welskopf 1974, 44.

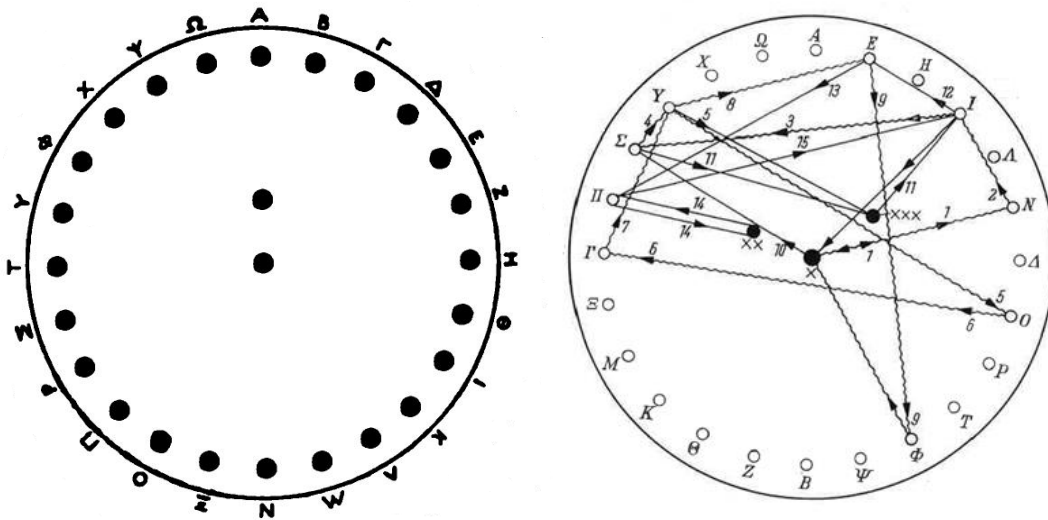


FIGURE 11: TWO POSSIBLE RECONSTRUCTIONS OF AENEAS TACTICUS' WOODEN DISK USED INSTEAD OF AN ASTRAGALUS. LEFT: RECONSTRUCTION DIELS; RIGHT: RECONSTRUCTION WELSKOPF.²⁹⁵

Aeneas Tacticus also mentioned that the extra holes in the middle were added to prevent suspicion from being raised (31.21) – though what exactly he meant by this is unclear. Translations and commentaries seem to have overlooked this point. It might be that there is an omission in the text here but another intriguing possibility is that one could have pulled a thread through the holes in the middle in order to wear the disk as a necklace – in the same way as the lead earrings described as a steganographic device in the treatise were designed to be worn as jewellery (31.7). Indeed, this interpretation fits in well with Aeneas Tacticus' wider approach to such devices and stratagems in *How to Survive Under Siege*, as we have seen: he clearly places greater emphasis upon the value of *hidden* devices than upon those that are encoded. And in this light it is easy to see why the example of the *scytale* – an encoded message carried in plain sight – would not fall within his list of recommendations for secret communications in a time of siege.

²⁹⁵ Diels 1914, 67; Welskopf 1974, 44.

At the beginning of this chapter the following research question was posed: *What are the reasons that the 4th-century BCE Greek military author Aeneas Tacticus – who dedicated a chapter of his work *How to Survive under Siege* to secret communication – excluded the Spartan scytale from his treatise?* As has been discussed in this chapter, there are various reasons to explain the fact that Aeneas Tacticus did not discuss the *scytale* in chapter 31 of *How to Survive Under Siege*. First, it is possible (though perhaps not probable) that Aeneas Tacticus did not know of the *scytale*'s potential or actual use by the Spartans as a cryptographic device at the time of writing. Secondly, as the sources discussed in the previous chapter demonstrate, *scytalae* would typically have been used for long distance communication rather than for the sort of local communications that concerned Aeneas Tacticus. Aeneas Tacticus, therefore, might well have known the use of the *scytale* for long distance communication, but he would not have seen it as a fit subject for his own work, with its focus on local communication. Thirdly, Aeneas Tacticus – living and writing in a post-war period (after the Peloponnesian War) – may well have seen Spartan devices like the *scytale* as un-Greek and as unworthy of inclusion in his treatise for Greeks. Fourthly, and perhaps most importantly, Aeneas Tacticus seemed to have been more interested in steganographic practices than cryptographic practices since the main focus in *How to Survive Under Siege* is upon hiding messages so as to smuggle them in and out of the besieged *polis* and not upon encoding them so as to prevent them from being read and understood by hostile agents (either inside or outside the city walls). We can reasonably conclude, then, that the absence of the Spartan *scytale* from Aeneas Tacticus' treatise does not in itself offer sufficient evidence to support the theory forwarded by Whitehead, West, and Sheldon that the *scytale* was unknown to Aeneas Tacticus because it was not really a form of ancient cryptography. We can, therefore, look to another significant body of ancient source material – this time one which *does* mention the *scytale* and

which *does* appear to recognise it as a useful cryptographic device – and forward our investigation by turning our attention from ancient Greece to ancient Rome in the next chapter.

Chapter 4: Roman views towards the Spartan *scytale*

It is highly likely that the Romans would have been familiar with Aeneas Tacticus' work *How to Survive Under Siege* and this text would have served an educational purpose as a manual for army commanders.²⁹⁶ Indeed, the treatise – along with Xenophon's *Art of Horsemanship* and *Cavalry Commander*, and Roman examples such as Vegetius' *Military Institutions of the Romans* – seems to have been intended as a pragmatic guide for commanders in the field.²⁹⁷ Although, as we have seen, the Romans would not have learned much about the *scytale* by studying Aeneas Tacticus, they would certainly have encountered descriptions of the device in other Greek sources, and this chapter focuses on Roman secret communication and Roman views towards the Spartan *scytale*. The corresponding research questions for this chapter are: *What view of the scytale did the Romans take and why did the Romans seemingly never adopt the Spartan scytale for cryptographic communications in their own military contexts – even though they seem to have been familiar with descriptions of the device and adopt other (less sophisticated) cryptographic systems?*

Roman sources on the *scytale* show that the Romans were familiar with the Spartan system for secret communication and accepted that it had been used by the Spartans in centuries past (see § 4.3; Cicero, *Letters to Atticus*, 10.10.3; Cornelius Nepos, *The Book on the Great Generals of Foreign Nations*. Pausanias, 4.3.4; Aulus Gellius, *Attic Nights*, 17.9.6-16; Ausonius, *Epistles*, 28.23-27). Given this knowledge of the *scytale* by the Romans, and their

²⁹⁶ Hanson 2007, 3.

²⁹⁷ Hanson 2007, 3; Pretzler 2018 (I), 68–95. See also Burliga 2008, 92-101; Pretzler 2010, 85-107; 2018 (II), 146-165; Shipley 2018. Although military manuals like Aeneas Tacticus' work were intended as pragmatic guides to commanders in the field, Burliga is uncertain to what extent, if at all, Aeneas Tacticus' work served a useful purpose in real military circumstances (Burliga 2008, 95-96).

familiarity with literary descriptions of the *scytale* as a sophisticated cryptographic device with particular benefits for use in military contexts and for communicating secretly and securely over long distances, we might question why they do not appear to have adopted the *scytale* for their own military use. The chapter starts with an analysis of Roman steganography and cryptography in order to situate the *scytale* and its Roman reception within this new context – as discussed by Ovid, Cicero, and Pliny the Elder and Ausonius (§ 4.1). Hereby, it will be shown that the Romans well understood and widely discussed the need for secrecy in the context of letter writing of various kinds. However, it will also reveal their apparent greater interest in steganographic hidden messages rather than in cryptographic coded messages (§ 4.1.4) – as we have already seen in the works of Herodotus and Aeneas Tacticus. This examination of the Roman sources is followed by an analysis of a rare example of Roman cryptography, in fact, the only Roman cryptographic substitution method that is known to us: the famous Caesar cipher (§ 4.2).²⁹⁸ The study then turns to Roman views on the Spartan *scytale* by analysing how three Roman authors discussed the device (§ 4.3). Hereby, I will offer an argument explaining why the Romans appear to have been familiar with the *scytale* and known of its potential value as a vehicle for secret communication – yet did not adapt the *scytale* for use in their own secret communications, either for private/personal correspondence or for military operations and communications in the field (§ 4.4). Hereby it will be shown that the

²⁹⁸ It is important to consider here that Caesar would, in all probability, have written most of it not all of his letters in Greek rather than Latin as a matter of course – since the medium of interpersonal written communication amongst the Roman elite at this period was predominantly Classical Greek. This makes it problematic to interpret the description of a coded letter as one ‘written in “Greek letters”’ as involving the straightforward transliteration of Roman characters into their Greek equivalents. When writing in cipher, therefore, it seems that Caesar is writing in Greek rather than Latin and substituting Greek ciphertext letters for Greek plaintext letters (possibly using the cipher system that came to bear his name). It is theoretically plausible that Caesar wrote in Latin but substituted Greek characters for Roman characters (when not actually writing in Greek) in his secret messages. In this case we would have a second method – or rather a variation of the first method – of a rudimentary substitution cipher known to the Romans.

Romans seem to have been more interested in using covered or concealed steganographic messages for securing official military correspondence rather than being interested in cryptographic devices – a preference that seems to reflect a parallel trend in their personal/private communications (such as those between friends, brothers, and lovers) too.

4.1: Secrecy and Roman letter writing

4.1.1: Ovid (43 BCE-17/18 CE) and Pliny the Elder (23-79 CE)

In many of the works of the Augustan love poet Ovid – especially in the *Amores*, *Ars Amatoria*, and *Heroides* – we find a range of suggestions for lovers to secretly communicate with each other. Significantly, no equivalent references to secret communication by lovers can be found in the earlier Greek context. This suggests that the Greeks and Romans may have had different concerns about and interests in cryptographic and steganographic messaging – in the contexts of both private discourse and official (including military) communication.

This apparent Roman interest in steganographic over cryptographic modes of secret communication is well illustrated by the variety of stratagems described by Ovid. In Ovid's work, the use of secret signs between lovers in their efforts to try to communicate with each other – especially at banquets and public gatherings – are a favourite theme with the author.²⁹⁹ A clear example of Ovid's steganographic tricks can be found in *Ars Amatoria*

²⁹⁹ *Amores*, 1.4.15-28; 1.4.55-58; 1.11; 1.12; 2.2.26; 2.5.15-20.5f.; 3.11.23f.; 3.11.23-24; 3.11a.23-24; *Epistles*, 16.258; 17.77ff.; *Ars Amatoria*, 1.91; 1.137f.; 1.341ff.; 1.351-198; 1.487-490; 1.497-502; 1.569-580; 2.131-140; 2.243; 2.246; 2.251; 2.543; 2.549; 3.514; 3.329-332; 3.394; 3.483-498; 3.619-630; 3.633; *Remedia Amoris*, 751-756; *Heroides*, 1.31-36; 17.77; 17.88; *Metamorphoses*, 3.460ff.; 4.63; *Fasti*, 1.418; *Tristia*, 2.453ff.

3.621-624, where Ovid suggests that a slave could carry a secret letter under her clothing or concealed in her sandals:

Conscia cum possit scriptas portare tabellas,

Quas tegat in tepido fascia lata sinu?

Cum possit sura chartas celare ligatas,

Et vincto blandas sub pede ferre notas? (Ovid, *Ars Amatoria*, 3.621-624; for the complete passage see Appendix 1, page 287).

When a confidant can carry a written tablet,

Concealed by a broad band on her warm bosom?

When she can hide a paper packet in her stocking

And bear your coaxing message 'twixt foot and sandal?

Similar suggestions for lovers to secretly communicate with each other are found in the elegies of Ovid's near contemporaries, the poets Propertius and Tibullus, indicating that such secret signals between lovers at dinner-parties and other such public occasions formed a stock theme for the Augustan elegists (see e.g. Propertius, *Elegies*, 3.8.25-26; Tibullus, *Elegies*, 1.2.21-22; 1.6.19; 1.8.1f.; 6.19.20).³⁰⁰ Yet, as in Ovid, none of these cases of private secret communication are examples of cryptography or steganography in the full sense, since no *written* secret messages are involved. Rather, these are simply suggestions for secret *signing*. Yet, Ovid does refer to secret letters sent between lovers in some of his works (*Amores* 2.15.15-18; *Ars Amatoria*, 2.596; 3.483-398; 3.627-630; *Heroides*, 4.3-5). In the earliest example, from *Amores* 2.15.15-18, Ovid reminded lovers of the need to seal secret missives (*arcanas possim signare tabellas [...] to help her [the female lover] seal her secret missive*; *Amores* 2.15.16-17; for the complete passage see Appendix 1, page 282) written on wax tablets in order to keep their secrets safe (see also *Amores* 1.11; 1.12; 3.496; *Ars Amatoria*, 2.396; 3.621-624).³⁰¹ Nothing in this

³⁰⁰ Green 1982, 272; McKeown 1989, 85-86.

³⁰¹ See also Brandt 1963, 208; Oliensis 2019, 100-149, especially 145-146; Munari 1959, 137.

example, however – which tells us little more than the fact that wax tablets were among the material media used by Romans for their letter writing – indicates that Ovid suggested that lovers should write their messages to each other in code.³⁰² However, potential references to coded writing can be found in two other Ovidian works. In *Ars Amatoria* 2.596 Ovid spoke of letters written ‘in a secret hand’ (*arcana verba notata manu*). And in *Heroides* 4.3-5, Phaedra – or rather, it should be remembered, Ovid writing *in propria persona* as Phaedra to her beloved Hippolytus – refers to secret or mysterious marks in her letters (*arcana notis*; *Heroides*, 4.5). Goold – in his translation of Ovid’s works – translates the Latin here as ‘secret characters’.³⁰³ However, this does not necessarily indicate coded or encrypted writing. The *arcana notis* could easily relate to Ovid’s suggestion in the *Ars Amatoria* 3.485 and 3.493 that lovers let their secret messages be written by someone else (such as a slave or confidante) in order to disguise their handwriting and thus the identity of the sender. It is also feasible that the *arcana notis/notatas/tabellas* referred to by Ovid’s Phaedra in the *Heroides* and by Ovid himself in the *Amores* and *Ars Amatoria* might have been written in a kind of ‘invisible ink’. This method of secret communication is suggested in Ovid’s *Ars Amatoria* (*Tuta quoque est fallitque oculos e lacte recenti*; [...] *A letter too is safe and escapes the eye, when written in new milk*; Ovid, *Ars Amatoria*, 3.627; for the complete passage see Appendix 1, page 287). Ovid – followed by Ausonius (4th century CE; see § 4.1.3) – suggested the use of fresh milk and moistened flax for this purpose (Ovid, *Ars Amatoria*, 3.627-630; Ausonius, *Epistles*, 28.21-22), while Pliny the Elder suggested the use of the milky juice of a plant known as the Mediterranean spurge or goat’s lettuce (*tithymalos characias*; Pliny, *Natural History*, 26.39 (62)). Ashes or linseed oil could be used to make the text visible again (*prodeuntur scripta favillis*; *with ashes the writing*

³⁰² Wax tablets seem to have been more commonly used among the Romans for writing (see Adkins & Adkins 2014, 209; Erdkamp 2011, 287; Jeffery 1961, 57; Lewis 2015, xxxix; Sherwood 2006, 536-537).

³⁰³ Goold 1914, 45.

is brought to light; Ausonius, *Epistles*, 28.21-22; *carbonis pulvere tange, leges [...]* Touch it with coal-dust and you will read; Ovid, *Ars Amatoria*, 3.628). Whitiak considers that Ovid, Pliny the Elder, and Ausonius would have been inspired by the Greek military engineer Philo of Byzantium, who provided us with the oldest known description of the use of invisible ink in the 3rd century BCE – made by mixing crushed gallnuts with water (*Compendium of Mechanics*, in: Thévenot, Boivin, et al., *Veterum Mathematicorum Opera*, 102).³⁰⁴ Whitiak further suggests that the Romans might have used various readily available substances including fruit juice and urine as their invisible inks and used as suited to various contexts.³⁰⁵ However, although it has been suggested that the *citron* could be the fruit described in Pliny's *Natural History* (12.7.15) as the *malum medicum* – the medicinal fruit – and depictions of citrus trees appear in later Roman mosaics from North Africa,³⁰⁶ it is not until the 8th century CE that Europe first discovers lemons via merchants from the Middle East.³⁰⁷ Also, although we find that lemon juice in particular has been used on a large scale in steganography in modern warfare up to and including the Second World War, we do not have any extant ancient sources mentioning the use of such substances as invisible inks (in any context) so it is difficult to assume with any confidence that any substances other than the new milk, regular ink, or 'goat's lettuce sap' would have been used by the Romans for secret messaging.³⁰⁸

Using these substances, Ovid (and, indeed, Pliny and Ausonius) clearly has in mind a secret communication through a letter written on a papyrus or paper-like medium – and not, as in the example discussed above, a wax tablet. He has adapted his steganographic methodology to suit the medium of the message in each case. Indeed, in his *Ars Amatoria* Ovid even suggests

³⁰⁴ Whitiak 2003, 1-2.

³⁰⁵ Whitiak 2003, 1-2.

³⁰⁶ See e.g. Khan 2007; Fiorentino & Zech-Matterne 2018; Feemster Jashemski & Meyer 2002.

³⁰⁷ Marks 2010, entry: *Citrus*; see also Khan 2007; Fiorentino & Zech-Matterne 2018.

³⁰⁸ Macrakis 2014, 138.

that lovers can write a secret message on the human body, either in normal ink (*pro charta conscia tergum; Praebeat, inque suo corpore verba ferat [...] Let the confidant offer her back for our note, And bear your words upon her body*; Ovid, *Ars Amatoria*, 3.625-626; for the complete passage see Appendix 1, page 287), or perhaps, once again, in invisible ink (*alii lactucam caprinam, narrantque lacte eius inscripto corpore, cum inaruerit, si cinis inspargatur, apparere litteras [...] It is said that, if letters are traced on the body with its milk and then allowed to dry, on being sprinkled with ash the letters become visible*; Pliny the Elder, *Natural History*, 26.39 (62); *Littera: carbonis pulvere tange, leges [...] A letter too is safe and escapes the eye, when written in new milk*; Ovid, *Ars Amatoria*. 3.628; for the complete passage see Appendix 1, page 287-288). The latter suggestion, that the lovers use a kind of invisible ink to write on a human body, would have made the message doubly secret since it would have been hidden under clothing and written in invisible letters. However, there is no indication in this example – or in any of Ovid’s other examples of secret messaging – that such *arcanas notas* or *arcanas tabellas* are to be written in any kind of code: this is simply another example of hidden *steganographic* messaging. Despite the ingenuity and variety of Ovid’s descriptions of secret communication in his poetry, all of his examples involve steganography and there is nothing at all to indicate any interest in cryptographic methods of messaging. In fact, this pattern – a marked preference for steganographic over cryptographic methods of communication – appears to mark a wider trend among our extant Roman sources and discussions of encrypted or encoded communications are comparatively rare.

4.1.2: Cicero (1st century BCE)

Writing in the 1st century BCE, Cicero is one such rare Roman author who appears to have referred directly to encryption as a way of securing secret communication. Indeed, he even used the word *σκυτάλη* (*scytale*) – although, as we will discover, Cicero’s reference to the

scytale may simply have been an allusion to the need for an increased attention to security and privacy in the context of letter-writing in general rather than a call for Romans to emulate the Spartans in more widely adopting a system of cryptographic messaging for important communications.

In a letter to his friend Atticus, Cicero wrote about a letter that he had himself received from Marc Anthony which Cicero described as a *σκυτάλην Λακωνικήν* (*scytale Lakoniken*; *Letters to Atticus*, 10.10.3): that is, a message created or communicated by Spartan *scytale* – or, as Shackleton Bailey translates it – a ‘Laconian dispatch’ (*Habes σκυτάλην Λακωνικήν. [...] There’s a Laconian dispatch [σκυτάλην Λακωνικήν] for you!*; for the complete passage see Appendix 1, page 270-271).³⁰⁹ In the original Latin text, the words ‘Laconian dispatch’ (*σκυτάλην Λακωνικήν*) are written in Greek instead of Latin, something that Cicero (and other Roman letter writers) often did in his actual correspondence.³¹⁰ It is possible that Cicero meant by this that he had received a secret message from Marc Anthony, but the context does not make it clear whether the Laconian dispatch (*σκυτάλην Λακωνικήν*) in question is a coded missive or merely some other form of private communication. Erasmus, in his early 16th-century work *Adages* suggested that the phrase ‘*There is a Laconian dispatch for you*’ would have meant that Cicero had received a private letter that was hard to understand, and concerned either a mysterious subject or unwelcome news (Desiderius Erasmus, *Adages*, Version Mynors Volume 33, 1991, p.77). Shackleton Bailey similarly seems to understand that Cicero’s reference to receipt of a *scytale* message merely referred to receipt of a very private letter. In his translation of Cicero’s text, the meaning ‘dispatch’ is supplied for the word *scytale*,

³⁰⁹ Shackleton Bailey 1999, 155.

³¹⁰ See on Cicero’s letter writing e.g. Butler 2012; Dunkel 2000; Hall 2009; Keeline 2018; Kelsey 2007; Poster & Mitchell 2007; Shackleton Bailey 1980; 1999 (all); 2004 (all); White 2010. See on Greco-Roman bilingual documents e.g.: Adams 2003; Dirkzwager 1976; Dunkel 2000; Elder & Mullen 2019; Kajanto 1980; Kramer 1983; Lietzmann 1968; Mullen & James 2012; Rea 1968; 1970; Sarri 2017; Trapp 2003; Wouters 1976.

favouring a more mundane interpretation of the ‘σκυτάλην Λακωνικήν’ here and distancing this reference from any allusion to its cryptographic Spartan origins.³¹¹

However, Cicero’s references to secrecy, concealment, and clandestine behaviour in this letter (*clam agam, cum paucissimis alicubi occultabor; I shall act by stealth and conceal myself; Letters to Atticus, 10.10.3*) suggest that the *scytale* in question here might well be understood as conveying a secret and coded message – whether from Anthony to Cicero, or from Cicero to Atticus. Indeed, the fact that we (like Atticus, Cicero’s ‘intended’ audience) read about the arrival of the original *scytale* dispatch here in another kind of ‘dispatch’ – Cicero’s own letter – offers the intriguing possibility that the Latin letter itself might be read as some kind of secret or even coded communication: a Roman version, perhaps, of a Laconian dispatch (σκυτάλην Λακωνικήν). The opening lines of the letter (*Habes σκυτάλην Λακωνικήν* – literally meaning ‘you have a Spartan scytale’ or as translated by Shackleton Bailey ‘There’s a Laconian dispatch for you!’)³¹² further invite this intriguing interpretation.³¹³ Yet, unfortunately, despite the fact that Cicero’s letter includes references to dates and numbers, and also includes Greek letters alongside Roman alphabetic writing, there is no way we can attempt to identify or to decode any possible coded (*scytale*) message here. Nor can we find any substantive evidence to support Donderer’s argument that Cicero regularly used coded communications, made on the grounds of a reference to communicating *διὰ σημείων*, (*dia semeion*) – ‘through signs’ – in another letter to Atticus (Cicero, *Letters to Atticus*, 13.32.2).³¹⁴ Thus, the ‘Erasmian’ reading of Cicero’s σκυτάλην Λακωνικήν remains the safest and most persuasive interpretation: for Cicero, a *scytale* meant not a secret or encrypted communication

³¹¹ Shackleton Bailey 1999, 155.

³¹² Shackleton Bailey 1999, 155.

³¹³ See also Strasser 2007, 278.

³¹⁴ Donderer 1995, 98-99. See also Nicholson 1994, 47-48.

per se – but a private letter conveying a message that was perhaps hard to understand, and concerned unwelcome news. We cannot, therefore, take Cicero’s letter(s) as evidence for any kind of Roman use of the *scytale* – although his writing does offer evidence of Roman familiarity with the key principles of the *scytale* as a device for communication.

4.1.3: Ausonius (4th century CE)

Later Roman sources also highlight the apparent Roman preoccupation with steganographic over cryptographic methods for secret communication. Indeed, although the 4th-century CE author Ausonius seems to have presented himself as an expert in secret messaging, his knowledge of such stratagems and devices is fairly limited – and largely focused upon the sorts of steganographic methods seen in Ovid and the other Latin love elegists.³¹⁵ In a letter to his pupil Paulinus, Ausonius wrote that he knew ‘*countless codes of the ancients for concealing and unlocking secret messages*’ (*Innumeras possum celandi ostendere formas et clandestinas veterum reserare loquellas*; *Epistles*, 28.28-29; for the complete passage see Appendix 1, page 269-270).³¹⁶ However, despite this expansive claim to know ‘countless forms’ (*innumeras formas*) of secret communications, Ausonius only refers directly in his writing to a scant handful of the various methods that the Greeks and Romans used, discussing only Ovid’s suggestion to use milk as invisible ink (*Epistles*, 28.21-22) and the Spartans’ use of the *scytale* (*Epistles*, 28.23-27) – discussed in greater depth and detail in § 4.3.3. In Ausonius’ description of invisible ink we clearly hear Ovid – since Ausonius, like Ovid, suggested the use of fresh milk that would become completely invisible when it had dried. Only when rubbing ashes onto

³¹⁵ See on Ausonius’ *Epistles*, e.g.: Dräger 2002; Evelyn-White 1921; Knight 2005. See on Ovid’s influence on Ausonius, e.g.: Guzmán & Martínez 2018; Fielding 2017; Martin 2004; Moroni 2010.

³¹⁶ See on the relationship between Ausonius and Paulinus, e.g.: Dräger 2002; Evelyn-White 1921; Knight 2005; Rucker 2012; Trout 1999.

the paper would the text become visible again. While Ovid, in *Ars Amatoria*, mentioned that: *A letter too is safe and escapes the eye, when written in new milk: Touch it with coal-dust and you will read* (*Tuta quoque est fallitque oculos e lacte recenti; Littera: carbonis pulvere tange, leges*; Ovid, *Ars Amatoria*, 3.627-628), Ausonius suggested to Paulinus – the receiver of his letter: *Trace letters with milk: the paper as it dries will keep them ever invisible; yet with ashes the writing is brought to light* (*lacte incide notas: arescens charta tenebit semper inaspicuas; prodentur scripta favillis*; Ausonius, *Epistles*, 28.21-22).³¹⁷ What is more, when Ausonius writes that he is familiar with ‘countless codes of the ancients for concealing and unlocking secret messages’ (*Innumeras possum celandi ostendere formas et clandestinas veterum reserare loquellas*; *Epistles*, 28.28-29) it is significant that the language he uses to characterise this secret communication clearly emphasises *hidden* rather than coded or encrypted messaging. He refers to concealing or hiding (*celandi*) and revealing or exposing (*ostendere*) messages – rather than to encoding them. Tellingly, he describes such secret communications as *clandestinas* – literally, as hidden – rather than as encrypted. Ausonius, therefore, highlights not only the relatively scant variety of options for such ‘clandestine’ communication amongst the ancient Roman sources with which he is familiar but also the focus in those sources upon *steganographic* modes.

4.1.4: The need for secrecy in Roman letter writing

The accounts of Cicero, Ovid, Pliny the Elder and Ausonius provide an interesting context for different Roman concerns with, and interest in secret communication outside of direct military contexts and might help us to understand the different choices that the Romans appear to have made about steganography and cryptography compared to the Spartans. By the end of the 1st

³¹⁷ Evelyn-White 1921, 111. See also Dräger 2002; Knight 2005.

century BCE, letter exchange was widely practised in elite Roman society. Indeed, participation in letter exchange was an essential element of Roman aristocratic culture.³¹⁸ With this emergence in the common practice of letter writing came – from the time of Cicero onward – an understanding of and need for secret and veiled communication in letters – precisely because there was an awareness that letters were not always really private. In fact, maintaining confidentiality and cautiousness in correspondence seems to have been expected of the correspondents.³¹⁹ This is, for example, why Ovid urged lovers to be as secretive as possible when sending each other letters (Ovid, *Ars Amatoria*, 3.625). In modern times the postal system protects the relative privacy of letters.³²⁰ However, in antiquity individuals had to make their own arrangements for the sending of their letters. For this, some individuals could have used the Roman imperial postal system (the *cursus publicus*; see Suetonius, *Lives of the Caesars* 2. *The Deified Augustus*, 49). Yet, this system was mainly used for official governmental and military correspondence since only those with official authorisation could use it – making it not easily accessible to other individuals.³²¹ A second option – in fact the only option for most people – was to give the letters to someone who was travelling in the direction of the intended recipient.³²² The fact that it was not always easy to find a trustworthy messenger is known from dozens of references in ancient letters, many of which can be found in Cicero’s correspondence (see for example: Cicero, *Letters to Atticus*, 1.16.16; 2.39.5; *Letters to Friends* 11.20.4; 11.26.5).³²³ Some historians further suggest that privacy in letter writing would have been compromised in the Roman world because letters were often expected to be read out loud by the intended recipient

³¹⁸ Freisenbruch 2007; Henderson 2007; Morello 2007.

³¹⁹ Malherbe 1988.

³²⁰ Sarri 2017, 125.

³²¹ Sarri 2017, 125; Sidebottom 2007, 9. See also: Kolb 2001.

³²² Sarri 2017, 125; Sidebottom 2007, 9.

³²³ See for example: Head 2009-I; 2009-II.

and addressee.³²⁴ Obviously, one could not control who might be listening in on this process – either intentionally or unintentionally. This point suggests that the Romans would have had good reason to have been interested in steganographic hidden messages. Perhaps it also helps to explain why the Romans do not appear to have been interested in cryptographic messaging – and why, despite their knowledge of the Spartan *scytale* and its operating principles, they did not apparently adopt encryption as a way of securing their secret communications.

4.2: The Caesar cipher (1st century BCE)

In fact, the only cryptographic system that seems to have been used in Roman communications, according to our available sources, is the so-called Caesar cipher – named after Julius Caesar by modern cryptographers since he is supposed to have invented and used this particular technique.³²⁵ Just as the Spartans used the *scytale* for secret cryptographic communication over long distances – so Caesar seems to have used his cipher to communicate with his generals in the same sort of contexts. The Caesar cipher is often regarded as a simple substitution technique for encryption, whereby each letter of a plaintext is replaced by a letter that can be found a fixed number of positions down the alphabet.³²⁶ In other words, in the ciphertext alphabet used for encryption and decryption there is always one shift of letters for the entire message – for example a right shift of three as in the case of Caesar’s use of the cipher (Aulus Gellius, *Attic Nights*, 17.9.2-5; Cassius Dio, *Roman History*, 40.9.4; Suetonius, *Lives of the Caesars* 1. *The Deified Julius*, 56.6; for the complete passages see Appendix 1, page 266-267; 270; 298). Significantly, the term ‘Caesar cipher’ is a term that only appears in modern books on

³²⁴ Achtemeier 1990, 15-17; Porter & Pitts 2013, 505.

³²⁵ Bishop 2003, 111; Churchhouse 2002, 13; Collard 2004; Kahate 2013, 36.

³²⁶ Mollin 2005, 11; Stinson 1995, 4.

cryptography.³²⁷ Caesar himself did not discuss the cipher – nor its potential name – in any of his surviving works. Yet, descriptions of the cipher (again without its potential name) can be found in the works of Suetonius, Aulus Gellius, and Cassius Dio (Aulus Gellius, *Attic Nights*, 17.9.1-6; Suetonius, *Life of Julius Caesar*, 56.6-7; Cassius Dio, *Roman History*, 40.9.3).³²⁸ Dio wrote that Caesar’s secret letters were unintelligible to most – but not all – people:

εἰώθει δὲ καὶ ἄλλως, ὅποτε τι δι’ ἀπορρήτων τινὶ ἐπέστελλε, τὸ τέταρτον ἀεὶ στοιχεῖον ἀντὶ τοῦ καθήκοντος ἀντεγγράφειν, ὅπως ἂν ἄγνωστα τοῖς πολλοῖς ἦ τὰ γραφόμενα (Cassius Dio, *Roman History*, 40.9.4; for the complete passage see Appendix 1, page 270).

It was his [Caesar’s] usual practice, whenever he was sending a secret message to any one, to substitute in every case for the proper letter of the alphabet the fourth letter beyond, so that the writing might be unintelligible to most persons.

Suetonius also described letters to Caesar’s intimates on confidential affairs – in both a private context and in his capacity as a general – as having been written in cipher to prevent Caesar’s enemies from reading the messages if they were intercepted:

Exstant [...], item ad omment a domesticis de rebus [...] si qua occultius perferenda ommen, per notas scripsit, id est sic structo litterarum ordine, ut nullum verbum effici posset; Suetonius, *Lives of the Caesars* 1. *The Deified Julius*, 56.6; for the complete passage see Appendix 1, page 298).

There are [...] letters [...] to his [Caesar’s] intimates on private affairs, [...] [when] he had anything confidential to say, he wrote it in cipher, that is, by so changing the order of the letters of the alphabet that not a word could be made out.

Finally, Aulus Gellius similarly mentioned the names of two of Caesar’s correspondents with whom Caesar communicated in cipher: his generals Oppius and Balbus:

³²⁷ See for example: Apelbaum 2007, 54; Bauer 2007, 382; Salomon 2003, 59; Salomon 2006, 243.

³²⁸ Mollin 2005, 8; 11; Kahate 2013, 2-9; Stinson 2002, 4. See for earlier substitution ciphers Strasser 2007, 278 (on the *Atbash* cipher used by Hebrew scholars ca. 600-500 BCE); Aeneas Tacticus’ *How to Survive Under Siege*, 31.30-31 (on replacing vowels by dots or other symbols, ca. 350 BCE).

sunt epistularum C. Caesaris ad C. Oppium et Balbum Cornelium, qui rebus eius absentis curabant. In his epistulis quibusdam in locis inveniuntur litterae singulares sine coagmentis syllabarum, quas tu putes positas incondite; nam verba ex his litteris confici nulla possunt (Aulus Gellius, *Attic Nights*, 17.9.1-2; for the complete passage see Appendix 1, page 266-267).

There are [...] letters of Gaius Caesar addressed to Gaius Oppius and Cornelius Balbus who had charge of his affairs in his absence. In certain parts of [the] letters there are found individual characters which are not connected to form syllables, but apparently are written at random; for no word can be formed from those letters.

In addition to sending secret and/or encrypted letters to his generals, Caesar would most likely also have communicated in cipher with his scouts and spies: the *exploratores* and *speculatores*.³²⁹ Indeed, communicating in cipher would have been especially important for Caesar's *exploratores* and *speculatores* since it was their task to find out everything about the enemy's strengths and whereabouts and communicate this highly sensitive information back to the central command – all without the enemy knowing about this. Such *exploratores* and *speculatores* often came up close to the enemy's camp, which made them vulnerable to being captured by the enemy. In fact, Caesar tells us that the Gauls sometimes captured his messengers (Caesar, *The Gallic War*, 5.45-46) and intercepted at least one letter sent from Caesar's general Quintus Cicero to Caesar (5.39). If *exploratores* and *speculatores* were captured with letters to or from Caesar written in plaintext, then the enemy could easily have found out what was known about their forces (see for references to *exploratores* in Caesar's work *The Gallic War*, 1.7; 1.10; 1.12; 1.19; 1.21; 1.22; 2.5; 2.11; 2.17; 3.2; 7.11; 7.44; *The*

³²⁹ The exact difference between the two groups is uncertain. Sheldon simply presumes that *speculatores* were used both as spies and as scouts (Sheldon 2008, 13; 84) – while Ezov argues that *speculatores* gathered information through spying, while *exploratores* gathered information through patrols with much less secrecy (Ezov 1996, 93). Russell presumes that *speculatores* were agents who operate more covertly than *exploratores* (Russell 1999, 485). *Speculatores* may have played an integral part of Caesar's military intelligence (Sheldon 1987, 106) – a point based on the idea that each of Caesar's legions had 10 *speculatores* under the general staff (Perkins 1953, 84).

Civil War, 1.62; 3.67; *The African War*, 12; *The Spanish War*, 28; see for references to *speculatores* *The Gallic War*, 2.11; 5.49). Therefore, it is likely that Caesar's *exploratores* and *speculatores* would have used the Caesar cipher in their own communications, as well as Caesar and his generals.

Although Caesar never directly discussed the use of the Caesar cipher in his works, we can find dozens of references to the sending and receiving of important confidential despatches in his works. There are 19 references in total in Caesar's works to the sending of important confidential despatches from Caesar to his staff;³³⁰ while Caesar's staff sent 40 highly confidential reports back to him about the enemy's strengths and whereabouts.³³¹ In addition to this, Caesar mentioned 69 times that he sent word to some of his troops in general, or to specific people, without explicitly mentioning that he sent them a written message.³³² Then there are another 67 potential references to secret letters, which are situations in which Caesar left some of his forces at a certain location, and then moved on to another place with only a small part of the forces moving with him.³³³ And, finally there are 140 situations in which

³³⁰ Caesar, *The Gallic War*, 2.35; 5.11; 5.46; 5.48; 7.9; 7.49; 8.11; *The Civil War*, 1.1; 1.9; 1.10; 2.13; 2.37; 3.25; 3.78; *The Alexandrian War*, 34; 42; 51; 56; *The African War*, 4; 26; 32; 86.

³³¹ Caesar, *The Gallic War*, 2.1; 2.10; 3.19; 4.5; 4.19; 4.37; 5.1; 5.6-7; 5.11; 5.18; 5.25; 5.40; 5.45-46; 5.47; 5.49; 7.6-7; 7.41; 7.67; 7.86; 8.1; 8.4; 8.19; 8.39; 8.46; *The Civil War*, 1.7; 1.10; 1.18; 1.26; 1.39; 1.59; 3.18; 3.43; 3.106; Caesar, *The African War*, 1; 7; 31; 63; 65; *The Spanish War*, 18-19.

³³² (Caesar, *The Gallic War*, 2.35; 4.38; 5.11; 5.46; 5.48; 7.9; 7.13; 7.49; 7.90; 8.11; *The Civil War*, 1.1; 1.9; 1.10; 2.13; 2.37; 3.25; 3.78; *The Alexandrian War*, 34; 42; 51; 56; *The African War*, 4; 26; 32; 86. For references to messages sent to specific people see Caesar, *The Gallic War*, 3.3; 3.19; 4.23; 4.25-26; 4.37; 5.1; 5.7; 5.52; 6.1; 7.49; 7.65; 8.27; Caesar, *The Civil War*, 1.8; 1.23; 1.25; 1.28; 1.82; 2.37; 3.2; 3.46; 3.62; 3.76; 3.78; 3.106-107; *The Alexandrian War*, 1; 9; 13; 51; *The African War*, 8; 12; 26; 31-32; 37; 40.

³³³ Caesar, *The Gallic War*, 1.10; 1.15; 1.24; 2.25; 2.35; 3.7; 3.10-11; 3.28; 4.7; 4.14; 4.18-19; 4.34; 4.38; 5.1-2; 5.8; 6.3; 6.5; 6.9; 6.32-33; 6.44; 7.9; 7.11; 7.40; 7.68; 7.80; 8.2; 8.38-39; 8.46; *The Civil War*, 1.8; 1.15; 1.32; 1.41; 1.64; 1.72; 1.80; 1.87; 2.1; 2.22; 3.2; 3.6; 3.16; 3.52; 3.78; 3.106; *The Alexandrian War*, 10; 11; 14; 33; 48; 66; 73; 78; *The African War*, 1; 2; 9; 63; 86; 89; 98; *The Spanish War*, 4; 40-42.

Caesar sent troops away from him or urged them to join him again.³³⁴

This brings the total number of potential references and allusions to secret messages sent to Caesar to 128, and another 207 passages in which secret messages could have been sent. Suetonius and Cassius Dio, therefore, seem to make a reasonable argument in saying that Caesar wrote in cipher whenever he had anything confidential to say (*si qua occultius perferenda errant*; Suetonius, *Life of the Caesars* 1. *The Deified Julius*, 56.6; ὁπότε τι δι' ἀπορρήτων τινὶ ἐπέστελλε, τὸ τέταρτον ἀεὶ στοιχεῖον ἀντὶ τοῦ καθήκοντος ἀντεγγράφειν, ὅπως ἂν [...] whenever he [Caesar] was sending a secret message to any one, to substitute in every case for the proper letter of the alphabet the fourth letter beyond, so that the writing might be unintelligible to most person; Cassius Dio, *Roman History*, 40.9.3). Caesar's use of the cipher has been important to him. Indeed, the use of the cipher must have been especially important during periods of conflict – such as the Gallic war, and even more important during the civil war.³³⁵

In one passage (Caesar, *The Gallic War*, 5.48) we read that Quintus Cicero was besieged by the Gauls. According to Caesar's own account, in order to let Quintus Cicero know that Caesar was about to send help, he decided to write Cicero a letter written in 'Greek letters' to prevent the Gauls from understanding the letter in case it was intercepted (*Graecis*

³³⁴ Caesar, *The Gallic War*, 1.21; 1.22; 1.24; 1.54; 2.17; 2.19-22; 2.26; 2.34-35; 3.1; 3.10-11; 3.16; 3.19; 3.28; 3.29; 4.14; 4.21-22; 4.32-33; 4.36; 4.38; 5.2; 5.10; 5.15; 5.24; 5.27; 6.1; 6.3; 6.5-6.7; 6.29; 6.33; 6.40-41; 7.34; 7.37; 7.45; 7.51; 7.56; 7.80; 7.87-88; 7.90; 8.2; 8.4; 8.5-7; 8.16-17; 8.19; 8.24-25; 8.43; 8.46; 8.52; 8.54; *The Civil War*, 1.11-12; 1.18; 1.26; 1.30; 1.32; 1.36-37; 1.39; 1.43; 1.45; 1.63; 1.66; 1.72; 1.78; 1.87; 2.5; 2.19; 2.21; 2.23; 3.8; 3.19; 3.24; 3.26; 3.34; 3.42; 3.56-57; 3.62; 3.77-78; 3.89; 3.97; 3.101; *The Alexandrian War*, 1; 9; 15; 17; 20; 21; 30; 31; 42; *The African War*, 2; 8; 10; 17-18; 20; 31; 37; 43; 51; 54; 58; 60-62; 66; 77-78; 81; 86; *The Spanish War*, 4; 26; 35; 39.

³³⁵ For references to letters sent during the civil war and situations in which secret letters could have been sent see Caesar, *The Civil War*, 1.1; 1.7; 1.8; 1.9; 1.10; 1.11-12; 1.15; 1.18; 1.23; 1.25; 1.26; 1.28; 1.30; 1.32; 1.36-37; 1.39; 1.41; 1.43; 1.45; 1.59; 1.63; 1.64; 1.66; 1.72; 1.78; 1.80; 1.82; 1.87; 2.1; 2.5; 2.13; 2.19; 2.21; 2.22; 2.23; 2.37; 3.2; 3.6; 3.8; 3.16; 3.18; 3.19; 3.24; 3.25; 3.26; 3.34; 3.43; 3.43; 3.46; 3.52; 3.56-57; 3.62; 3.76; 3.77-78; 3.89; 3.97; 3.101; 3.106-107).

conscriptam litteris mittit, ne intercepta epistola nostra ab hostibus consilia cognoscantur; Caesar, *The Gallic War*, 5.48). This letter Caesar had delivered by a Gaul who worked for him (Caesar, *The Gallic War*, 5.48). Cassius Dio presumed that Caesar simply wrote a letter in Greek to make sure that the Gauls could not understand the message (ἐλληνιστὶ ἐπέστειλεν; ἵνα ἂν καὶ τὰ γράμματα ἀλφ, ἀλλ' ἀσύνητά γε καὶ τότε τοῖς βαρβάροις ὄντα μηδὲν σφας ἐκδιδάξῃ [...]) [Caesar] wrote in Greek all that he wished to say, in order that even if the letter were captured, it should even so be meaningless to the barbarians and afford them no information; Cassius Dio, *Roman History*, 40.9.3-4). Cary and Foster also seem to adopt this idea in their translation of *Roman History* since they translate the text simply as '(Caesar) wrote...in Greek' without adding any critical notes to the text and/or referring to the Caesar cipher.³³⁶ Adams and Harris too assume that Caesar must simply have written the letter in the Greek language, without using any codes.³³⁷ However, a letter simply written in Greek in order to encrypt Caesar's message seems an inadequate interpretation of the situation in this case. Correspondence between elite Romans in this period would typically have been written in Greek as a matter of course, and Caesar knew that some of the Gauls had knowledge of the Greek language and script (*The Gallic War*, 1.19.1; 6.14). Modern historians of cryptography Pieprzyk, Hardjono and Seberry, therefore, seem to be in error when presuming that Caesar's letters, if written in Greek, would have been undecipherable to his enemies in Gaul.³³⁸ So, it seems implausible that Caesar simply wrote the letter in Greek to prevent the Gauls from comprehending its contents. Some other scholars – e.g. Singh, Bauer, and Holmes – assume that Caesar transliterated a message that was originally written in Latin, into Greek characters or letters. In this way a 'Greek'

³³⁶ Cary & Foster 1914, 419.

³³⁷ Adams 2003, 329; Harris 1989, 182-183.

³³⁸ Pieprzyk, Hardjono & Seberry 2013, 6.

meaningless message was created.³³⁹ Although this is plausible – in fact the use of different languages with different alphabets (Latin and Greek) would have made the messages even more secure – we must keep in mind that the typical medium of communication amongst the Roman elite was predominantly Greek in any case. Caesar would in all probability already have communicated with Quintus Cicero using ‘Greek letters’ in his non-secret correspondence, and he would have changed to communication in cipher if an extra layer of security was needed. Moreover, since the two men would normally communicate in Greek, and Cicero was besieged by the Gauls, Caesar could not (easily) have communicated to him that he had decided to change his method of secret communication by sending a message in Latin (in a Greek alphabet), instead of in Greek. In other words, Caesar’s secret letter to Cicero was most likely a letter already written in Greek and encrypted in a Greek substitution cipher. It seems plausible then that the language for this secret communication was not simply Greek, nor Latin with a Greek substitution cipher, but, as Reinke describes it, ‘*cryptic Greek*’.³⁴⁰ That is, a coded letter – written with a Caesar cipher using the Greek alphabet. Such an interpretation is also supported by Edwards’ translation of *The Gallic War* in which he aptly translates ‘*Graecis litteris*’ as ‘Greek characters’ instead of ‘Greek letters’.³⁴¹ So what do we learn from this slender and solitary account of Caesar apparently using ‘Greek letters’ or ‘Greek characters’ to communicate secretly with his friend Cicero? I suggest that we can decode this story as a veiled account of Caesar’s own cipher being used in the field (as does Harris)³⁴² – and that we can therefore gain fresh insights into the cryptographic principles on which the Caesar cipher

³³⁹ Bauer 2017, 99; 148; Holmes 1911, 218-219; Singh 1999, 10. See for similar examples of Greek texts written phonetically with the Latin alphabet and Latin texts written phonetically with the Greek alphabet e.g. *P.Oxy.2.244*; 36.2772; Adams 2003; Burrell 2009, 69-95; Dirkzwager 1976; Kajanto 1980; Kramer 1983; Lietzmann 1968; Rea 1968; 1970; Wouters 1976.

³⁴⁰ Reinke 1962, 114.

³⁴¹ Edwards 1917, 297.

³⁴² Harris 1995, 14.

operated. I further suggest that there is a ‘quasi-Spartan’ character to Caesar’s use of this ‘cryptic Greek’ – which invites us to recall the Spartan *scytale*.

In modern cryptography, the Caesar cipher is still regarded as a simple substitution technique for encryption whereby each letter of a plaintext is replaced by a letter taken from a fixed number of positions down the alphabet.³⁴³ Caesar most likely always used a right shift of three in the ciphertext alphabet used for encryption and decryption of his confidential correspondence – something known as monoalphabetic encryption in modern cryptography since only one ciphertext alphabet is used to encrypt and decrypt the entire message (Aulus Gellius, *Attic Nights*, 17.9.2-5; Cassius Dio, *Roman History*, 40.9.4; Suetonius, *Lives of the Caesars* 1. *The Deified Julius*, 56.6).³⁴⁴ Modern cryptographers, however, often presume that Caesar used a variety of possible ciphertext alphabets. Van Tilborg, for example, argues that Caesar shifted the alphabet over a number of places regularly to create new ciphertext alphabets – while Kahn and Oriyano presume that Caesar used up to two dozen ciphertext alphabets.³⁴⁵ Although it might have been case, theoretically speaking, that Caesar changed his shift regularly – which would have given him 23 possible ciphertext alphabets since he used the 24-letter ancient Greek alphabet (see below) – it is highly unlikely that Caesar used more than one shift of letters or changed the shift regularly since he would not have had the time nor the means to inform all of his units about this change of shift – especially not whilst on campaign.

Rather, it is known from Suetonius and Cassius Dio that Caesar – whenever using the technique to create a ciphertext alphabet – substituted every alphabetic letter of a plaintext for the alphabet letter that could be found three places further down the alphabet (moving from the left to the right): e.g. ‘A’ became ‘D’, ‘B’ became ‘E’ and so on with the rest. The Latin text

³⁴³ Mollin 2005, 11; Stinson 1995, 4.

³⁴⁴ Apelbaum 2007, 54; Bauer 2007, 382; Salomon 2003, 59; Salomon 2006, 243.

³⁴⁵ Kahn 1974, 77; Oriyano 2013, 56; Van Tilborg 2006, 9.

in Suetonius' work reads '*quae si qui investigare et persequi velit, quartam elementorum litteram, id est D pro A et perinde reliquas commutet*' (Suetonius, *Lives of the Caesars* 1. *The Deified Julius*, 56.6) – which Rolfe translates as: '*If anyone wishes to decipher these, and get at their meaning, he must substitute the fourth letter of the alphabet, namely D, for A, and so with the others*' (for the complete passage see Appendix 1, page 298).³⁴⁶ Decryption of messages written in a Caesar cipher with a right shift of three obviously worked the other way around by substituting each letter in the ciphertext for the letter that could be found three places back – to the left – in the alphabet (Suetonius, *Lives of the Caesars* 1. *The Deified Julius*, 56.6-7; Cassius Dio, *Roman History*, 40.9.3; see also Figure 12 for encryption with the Caesar cipher, and Figure 13 for decryption with the Caesar cipher). Rolfe in his translation of Suetonius' work, and Cary and Foster in their translation of Dio's work, each use the word 'substitute' to describe these operations in their respective translations.³⁴⁷ Yet in Suetonius' work we find the word '*commutet*', literally 'change'; 'alter'; or 'substitute' – while in Dio's work we see the word *ἀντεγγράφειν*, literally 'insert (one name instead of another)' (Suetonius, *Lives of the Caesars* 1. *The Deified Julius*, 56.7; Cassius Dio, *Roman History*, 40.9.3). Rolfe, and Cary and Foster, in using the word 'substitute' in their respective translations, unequivocally align Caesar's cipher with the simple substitution techniques used in modern Caesar ciphers. However, the system also reminds one of transposition in the technical sense, if the ciphertext alphabet and the plaintext alphabet are written out, one under the other. We can clearly see this in the diagrams below:

³⁴⁶ Rolfe 1914, 109.

³⁴⁷ Cary & Foster 1914, 419; Rolfe 1914, 109.

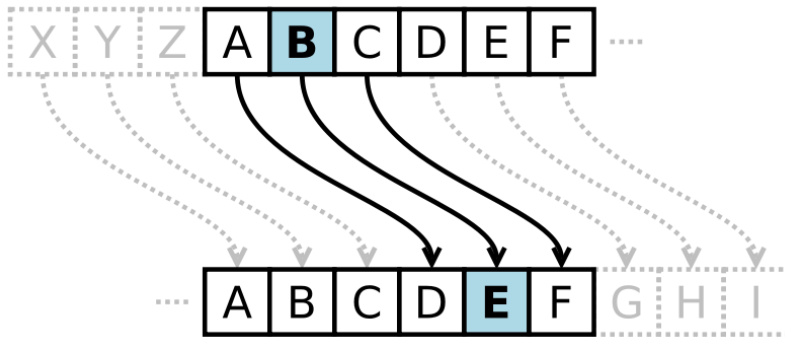


FIGURE 12: ENCRYPTING TEXT WITH A CAESAR CIPHER WITH A RIGHT SHIFT OF THREE.³⁴⁸

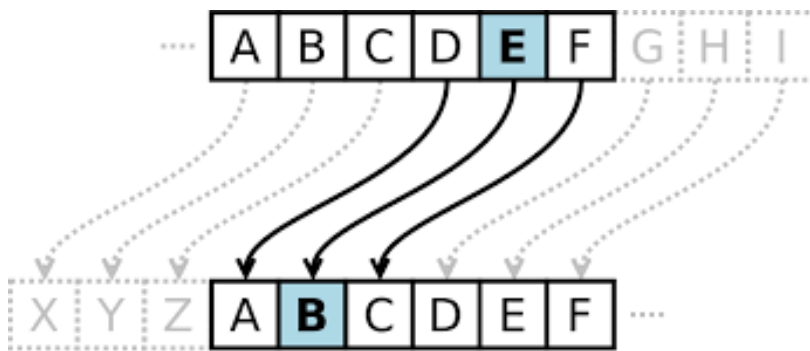


FIGURE 13: DECRYPTING TEXT WITH A CAESAR CIPHER WITH A RIGHT SHIFT OF THREE.³⁴⁹

In a simple substitution cipher, the characters of a plaintext are replaced by other characters, numbers, symbols, or a combination of those – as is the case in Caesar’s substitution of plaintext letters for ciphertext letters.³⁵⁰ This becomes especially clear when an encryption table is used, like the one presented in Figure 14.³⁵¹ And here, I have taken the insights from my study of Caesar’s own account of using such a shift cipher for encrypted secret communication

³⁴⁸ Author’s illustration based on Chesire Library Science 2013.

³⁴⁹ Author’s illustration based on Chesire Library Science 2013.

³⁵⁰ If using the Classical Latin alphabet for his cipher, Caesar had an alphabet of either 21 or 23 letters. According to Cicero, the alphabet of the late Republican period was composed of 21 letters (*On the Nature of the Gods*, 2.37): the letters ‘J’, ‘U’, ‘W’, ‘Y’ and ‘Z’ were not used – although according to Sherwood, Nikolic, et al., the Romans already added the Greek letters ‘Y’ and ‘Z’ to their alphabet after the conquest of Greece in 146 BCE (Sherwood, Nikolic et al. 2003, 525; see also Wallace 2015, 14; 16).

³⁵¹ See for example: Bauer 2013; Churchhouse 2002; Piper & Murphy 2002; Purnamaa & Rohayani 2015; Van Tilborg 2006, 9-10.

to further suggest that the alphabet used for this shift – at least in the one case we can reasonably attribute to Caesar himself (*The Gallic War*, 5.48) – was not Latin but Greek (see Figure 14).

Letter in plaintext	A	B	Γ	Δ	E	Z	H	Θ	I	K	Λ	M
Letter in ciphertext	Δ	E	Z	H	Θ	I	K	Λ	M	N	Ξ	O
Letter in plaintext	N	Ξ	O	Π	P	Σ	T	Υ	Φ	X	Ψ	Ω
Letter in ciphertext	Π	P	Σ	T	Υ	Φ	X	Ψ	Ω	A	B	Γ

FIGURE 14: CAESAR CIPHER WITH A RIGHT SHIFT OF THREE APPLIED TO ANCIENT GREEK ALPHABET.³⁵²

Indeed, I suggest that if we look further back into history and into the ancient Greek world, we can arguably see the embryo of this principle – a fractionating transposition cipher – particularly when we recall that the design of the *scytale* entailed that encrypted texts contained letters that were not merely ‘transposed’ (taken out of place by their unwrapping and re-wrapping around various diameters of *scytale* rod) but also effectively ‘substituted’ by the incomplete lines, dots, dashes, and other marks of incomplete letters.

The Caesar cipher is still mentioned in almost every book on 21st-century cryptography – where it is typically described as being a conceptual milestone in the development of modern cryptography (as in the work of Stewart, Chapple et al., for example) – albeit, without much discussion of this development.³⁵³ Yet, none of these studies consider the significance (indirect or otherwise) of earlier Greek substitution and/or transposition ciphers – including the *scytale*

³⁵² Author’s illustration.

³⁵³ Stewart, Chapple et al. 2012, 362. See also Kahn 1967, 77; Mollin 2005, 11; Oriyano 2013, 56; Stinson 2002.

– upon the development and deployment of the Caesar cipher.³⁵⁴ Such studies typically position Caesar’s Roman technique for secret communication as the embryonic form of modern cryptographic methods and ignore the fact that complex modes of encryption already existed in the classical world and were in use centuries before the Caesar cipher. It is impossible to trace a continuous line of evolution – or, indeed, any direct relationship – between the Spartan *scytale* and the development of the Caesar cipher. However, the system of the Caesar cipher nevertheless shares important conceptual principles with the encryption technique utilised in the Spartan system of the *scytale*. When messages were unwrapped from the *scytale* the alphabetic letters physically changed place according to a variable ‘shift’ determined by the diameter of the *scytale* rod used – and in the alphabet(s) used for the encryption of the Caesar cipher we see a cipher with a right shift of three.³⁵⁵ Although this later Roman cipher is less sophisticated (involving a regular, fixed, shift and not requiring any specialist equipment to supply its ‘key’) understanding the dynamics of its operation can help us to better appreciate the comparative complexity and security of the ancient Spartan *scytale* – thereby supporting the overarching argument of this thesis that the *scytale*, in theory, would have been potentially a more useful device for secret messaging than the Caesar cipher.

³⁵⁴ As discussed previously, there is ongoing debate on whether Caesar wrote his secret messages (including the message to Cicero) (1) fully in Greek (using Greek characters, accident and syntax), (2) in Latin with a Greek substitution cipher, or (3) in Greek with a Greek substitution cipher. Therefore, there are various ways in which Greek cryptographic methods may have influenced later Roman cryptographic methods. In this case I assume that Caesar’s secret letters were written in Greek with a Greek substitution cipher.

³⁵⁵ Augustus used the same principle as Caesar, yet with a right shift of one hereby writing *B* for *A*, *C* for *B*, et cetera (Suetonius, *Lives of the Caesars* 2. *The Deified Augustus*, 88). This right shift of one can again be seen in Viking texts (Bauer 2017, 118-120), and in the work of the 14th century CE Greek scholar Georgius Chrysocossas who used β for α , γ for β and so on. A partial Latin translation of the work of Georgius Chrysocossas can be found in various 15th- and 16th-century copies of a manuscript known as *Expositio In Syntaxin Persarum* (Gardthausen 1911, 302).

4.3: Roman sources on the Spartan *scytale*

As we have seen in chapter 2, 21st-century readers of Greek sources on the *scytale* may struggle precisely to identify what a Greek writer meant when he referred to a Spartan *scytale* and, in particular, to determine whether any secret communication or encryption was envisaged. Especially, modern readers are often dependent upon translators to guide them as to which meaning is intended from a wide range of possibilities suggested by the term ‘*scytale*’. In this context, Roman writers – who also had to translate these Greek sources – offer some interesting (though ultimately limited) insights (Cicero, *Letters to Atticus*, 10.10.3; Cornelius Nepos, *The Book on the Great Generals of Foreign Nations*. Pausanias, 4.3.4; Aulus Gellius, *Attic Nights*, 17.9.6-16; Ausonius, *Epistles*, 28.23-27) – leading some modern cryptographers to believe that the Romans erroneously helped to promote the myth that the *scytale* was genuinely a Spartan cryptographic device. Strasser, for example, argues that:

Roman authors – beginning with Cicero [...] – considered the Spartan *skytale* a cryptographic device. Their – apparently erroneous – assumption that such a ‘stick’ or ‘rod’ was used by the warlike Spartans, as far back as the fifth century BC, which would make the *skytale* the first cryptographic tool. It was supposed to be an ingeniously simple system [...].³⁵⁶

As will be analysed in this section, there are a number of Roman authors who discussed the *scytale* (Cicero, *Letters to Atticus*, 10.10.3) – already examined in § 4.1 (Aulus Gellius, *Attic Nights*, 17.9.6-16; Ausonius, *Epistles*, 28.23-27). Yet, as we will see, their descriptions and understanding of the *scytale* as a device for secret communication is not as straightforward (or, I argue, as erroneous) as Strasser suggests. This, it will be seen, is related to the fact that our Roman authors do not have first hand knowledge of the Spartan *scytale* but draw their

³⁵⁶ Strasser 2007; Swift 2019, 278.

knowledge from some of the same Greek sources that we have already considered in chapter 2.

4.3.1: Cornelius Nepos (1st century BCE)

Cornelius Nepos, writing in the 1st century BCE, was the first author who used the Latin equivalent of the word *scytale*, namely, *clava*. He did so in *The Book on the Great Generals of Foreign Nations* in chapter 4 on the Spartan general Pausanias (4.3.4). In this chapter we see Cornelius Nepos repeat Thucydides' story of how Pausanias – whilst campaigning in Asia – was summoned home by the Spartan *ephors* by means of a *scytale* message because of his misbehaviour (4.3; see also Thucydides, *History of the Peloponnesian War*, 1.131.1):

Id postquam Lacedaemonii rescierunt, legatos cum clava ad eum miserunt, in qua more illorum erat scriptum: nisi domum reverteretur, se capitis eum damnaturos (Cornelius Nepos, *The Book on the Great Generals of Foreign Nations*, 4.3.4-5; for the complete passage see Appendix 1, page 271).

As soon as the Lacedaemonians learned of his conduct [Pausanias' misbehaviour], they sent envoys to him with the staff [*clava*] on which it was written after their fashion that if he did not return home, they would condemn him to death.

Watson – in his translation of the work – used the Greek word '*scytale*', while Rolfe translates the Latin word '*clava*' into English as 'staff'.³⁵⁷ Like the word *σκυτάλην* ('*scytale*') in Greek, the word '*clava*' has a range of different meanings in Latin, ranging from 'stick' to 'a weapon for exercising, used by young men, and especially by soldiers'.³⁵⁸ Yet there is nothing in the

³⁵⁷ Rolfe 1929, 51; Watson 1886, 326-327.

³⁵⁸ Lewis and Short, s.v, give the following definitions for the term: *clāva*, *ae*, f. root *cel-* of *percello*; cf. Gr. *κλάω* and *clades*. 1: A knotty branch or stick, a staff, cudgel, club: "*adfer duas clavas... probas* (Plautus, *Rudens*, 3.5.20; Lucr. 5, 968: '*sternentes agmina clavā*," Verg. A. 10, 318; Curt. 9, 4, 3; Ov. F. 1, 575; Cic. Verr. 2, 4, 43, § 94; Plin. 19, 1, 3, § 18; a bar, lever, Cato, R. R. 13, 1.—As a weapon for exercising, used by young men, and esp. by soldiers, a foil, Cic. Sen. 16, 58; Veg. Mil. 1, 11.—As a badge of Hercules, Prop. 4 (5) 9, 39; Ov.

lexicon that suggests the ‘*clava*’ has any part to play in the sending (or encrypting) of messages. Rolfe’s rendering of ‘staff’, therefore, is a legitimate translation, but it is highly misrepresentative of the function that the particular ‘staff’ or ‘stick’ in this context is performing. Watson’s *scytale* (a re-translation or re-coding of the Latin not into English but into transliterated Greek) is a much better equivalent. However, neither the Latin text, nor the translation, nor the fact that Cornelius Nepos is basing his description upon one of Thucydides’ Greek stories, can help us to decipher whether or not Cornelius Nepos regards the *scytale* that is sent in this story to summon back the errant Pausanias as a regular ‘Spartan dispatch’ or as conveying a secret message.

4.3.2: Aulus Gellius (2nd century CE)

In chapter 2, Plutarch’s description of the *scytale* is discussed (§ 2.3.10; 2.4). Yet, it is not in Plutarch’s late 1st/ early 2nd century CE works, but in Aulus Gellius’ late 2nd-century CE Latin work *Attic Nights* that we see the most complete and persuasive description of a *scytale* being used as a Spartan cryptograph. Aulus Gellius was a well-educated figure who seems to have conducted extensive research on a large variety of topics for his work *Attic Nights* – as becomes clear from the fact that no less than 275 earlier Greek and Roman authors are mentioned in the work.³⁵⁹ It is crucial to keep in mind that many of Aulus Gellius’ sources have only partially survived, if at all.³⁶⁰ Moreover, it has been argued that Aulus Gellius often took his quotations

H. 9, 117; id. M. 9, 114; 9, 236; cf. Paul. ex Fest. p. 62 Müll.—Hence, prov., *clavam Herculi extorquere*, for an impossible undertaking, Macr. S. 5, 3; Don. Vit. Verg.— Also *Clava Herculis*, a plant, otherwise called *nymphæa*, Marc. Emp. 33.

³⁵⁹ Rolfe 1927, xvi-xvii. See further on Aulus Gellius’ sources Anderson 2004; Cavazza 2004 (esp. 66-68); Holford-Strevens 2003 (esp. 65-81); 2019-I; 2019-II (for the passage see especially page 590); Holford-Strevens & Vardi 2004; Keulen 2004.

³⁶⁰ Anderson 2004; Cavazza 2004 (esp. 66-68); Holford-Strevens 2003 (esp. 65-81); 2019-I; 2019-II; Holford-Strevens & Vardi 2004; Howley 2018, 113; Keulen 2004; Rolfe 1927, xvi-xvii.

from commentaries and grammatical works instead of consulting the original sources.³⁶¹ Therefore, it cannot be said with certainty which contemporary sources Aulus Gellius may have used as the basis of information for his passage on the Spartan *scytale*, especially since (in this case) he did not name his particular source or sources. However, Plutarch is quoted by Aulus Gellius 11 times in his *Attic Nights*, showing that Plutarch was certainly an important source for him. Moreover, Plutarch's description of the *scytale* has survived, allowing us to see that Plutarch's and Aulus Gellius' descriptions of the device are very similar in style, content, and specificity of detail (see § 2.3.10; 2.4). Therefore, it is highly likely either that Aulus Gellius used Plutarch's *Life of Lysander* (esp. 19.5) or that he used the same sources as Plutarch – including Theopompus in his (now lost) discussion of the Spartan *scytale*. After Cicero, Aulus Gellius was probably the only Roman author who used the Greek word *σκυτάλη* (*scytale*) in his text (*Attic Nights*, 17.9.16), instead of the Latin equivalent 'clava' that was first used by Cornelius Nepos in the 1st century BCE (*The Book on the Great Generals of Foreign Nations*. *Pausanias*, 4.3.4). Rolfe – in his translation of Aulus Gellius' work – used the Greek word 'σκυτάλη' without modifying this into the English transliteration of 'scytale' – and without giving any explanation and/or translation in any note.³⁶² Plutarch's and Aulus Gellius' descriptions of the *scytale* as a Spartan cryptographic device are very similar. Yet, while Plutarch gave examples of the specific contexts in which *scytalae* were used for this purpose (*Life of Lysander*, 19-20; *Life of Alcibiades*, 38; *Life of Artaxerxes*, 6; *Life of Agesilaus*, 10; 15), Aulus Gellius simply discussed how the Spartans used a *scytale* as a cryptograph (*Attic Nights*, 17.9.6-16). The more focused treatment of the *scytale* as a cryptograph in Aulus Gellius' work most likely has something to do with the wider scope of the *scytale*-passage in *Attic Nights*, namely,

³⁶¹ Anderson 2004; Cavazza 2004 (esp. 66-68); Holford-Strevens 2003, 65-81; 2019-I; 2019-II; Holford-Strevens & Vardi 2004. First argued in modern scholarship by Nettleship in 1883 (xiii).

³⁶² Rolfe 1927, 237. He might have done so to stay as close to the original as possible in his translation, since Aulus Gellius also used the Greek word in his Latin text.

discussing the use of cryptography and steganography among the Greeks, Romans, and Carthaginians. In fact, Aulus Gellius discussed the *scytale* as a Spartan cryptograph in a passage in which he also discussed the Caesar cipher (*Attic Nights*, 17.9.1-5); a case in which a Carthaginian – probably Hasdrubal – wrote under the wax of a wax tablet (17.9.16-17; see also Justin, *Epitome of the Philippic History of Pompeius Trogus*, 21.6); and a secret message tattooed on a slave’s head (17.9.18-27; based on: Herodotus, *Histories*, 5.35). Clearly, for Aulus Gellius, the *scytale* was a useful cryptographic device used by the Spartans not only in theory but also in practice, since he was certain that:

Lacedaemonii [...] veteres, cum dissimulare et occultare litteras publice ad imperatores suos missas volebant, ne, si ab hostibus eae captae forent, consilia sua noscerentur, epistulas [...] mittebant (Aulus Gellius, *Attic Nights*, 17.9.6-7; for the complete passage see Appendix 1, page 267).

the ancient Lacedaemonians, when they wanted to conceal and disguise the public dispatches sent to their generals, in order that, in case they were intercepted by the enemy, their plans might not be known, used to send letters written in [this] manner.

This makes Aulus Gellius and Ausonius (whose work is discussed in the next section) the only two Romans who were certain that the Spartans used *scytalae* for secret communication in the way it has been discussed in chapter 2. It is therefore to these important sources that we turn next.

4.3.3: Ausonius (4th century CE)

In a letter to his friend Paulinus – who may have been his lover (see e.g.: Ausonius, *Epistles* 19.7-8; 26; 28)³⁶³ – the 4th-century CE Latin poet Ausonius suggested various ways to send secret letters to each other to make sure that their secret was not revealed – since he knew of countless methods for cryptography and steganography from the ancient Greeks and Romans

³⁶³ A discussion on the relationship between Ausonius and Paulinus lies beyond the scope of this thesis. See on the topic e.g.: Dräger 2002; Ebbeler 2007; Knight 2005; Trout 1999.

before him (*Innumeras possum celandi ostendere formas et clandestinas veterum reserare loquellas*; countless codes of the ancients for concealing and unlocking secret messages; 28.28-29) – including tracing letters with milk as invisible ink (28.21-22; see also § 4.1.3) and the use of the Spartan *scytale* (28.23-27).³⁶⁴ As we will see, Ausonius' description of the *scytale* is very similar to Plutarch's and Aulus Gellius' descriptions (Plutarch, *Life of Lysander*, 19.5-7; Aulus Gellius, *Attic Nights*, 17.6-16). According to the author:

Lacedaemoniam *scytalen* imitare, libelli
 segmina Pergamei ommen circumdata ligno
 perpetuo inscribens versu, qui deinde solutus,
 non omment al sparso dabit ordine formas,
 donec consimilis ligni replicetur in orbem (Ausonius, *Epistles*, 28.23-27; for the complete passage see Appendix 1, page 269-270).

Imitate the Spartan *scytale*, writing on strips of parchment wound about a rounded stick in continuous lines, which, afterwards unrolled, will show characters incoherent because sequence is lost, until they are rolled again about just such another stick.

As becomes clear from the description, Ausonius described the *scytale* as a stick around which a strip of parchment was wound on which a message was subsequently written – very similar to the descriptions of Plutarch and Aulus Gellius (Plutarch, *Life of Lysander*, 17.5-7; Aulus Gellius, *Attic Nights*, 17.9.6-16). The strip was then unwrapped from the *scytale* and sent to the intended recipient whereby all letters changed placed, and therefore, the message turned into gibberish until it was wrapped about a *scytale* of the same diameter again (Ausonius, *Epistles*, 28.23-27). Plutarch also mentioned strips of papyrus, like long and narrow leathern strips (*βιβλίον [...] ἱμάντα μακρὸν*; *Life of Lysander*, 19.5) – while Aulus Gellius spoke of leather straps – in this context strips of leather parchment (Aulus Gellius, *Attic Nights*, 17.9.9). In

³⁶⁴ What other methods Ausonius was familiar with are unclear since he does not discuss them in any of his surviving letters.

Ausonius' description of the *scytale* we again find these strips of parchment referred to (*libelli segmina Pergamei*; Ausonius, *Epistles*, 28.23-24). Unlike other Roman authors, in Ausonius' Latin text we find the transliterated form of the word '*scytale*' used for the first time – instead of the use of the Greek word *σκυτάλη* or the Latin word *clava* – and the cryptographic associations of the *scytale* are thereby set out as unambiguous. We can only speculate as to the cause of this change, but it seems that the influence of Ausonius' primary Greek sources – Plutarch's and Aulus Gellius' descriptions – may help to explain this new appreciation of the *scytale* not merely as stick or staff but as a cryptographic device.

As we have seen, then, there are various extant Roman sources on the *scytale* – or its Latin equivalent *clava* – showing that the Romans were certainly familiar with this Spartan system for secret communication and believed that it had been used by the Spartans in centuries past (cf. Cicero, *Letters to Atticus*, 10.10.3; Cornelius Nepos, *The Book on the Great Generals of Foreign Nations*. Pausanias, 4.3.4; Aulus Gellius, *Attic Nights*, 17.9.6-16; Ausonius, *Epistles*, 28.23-27). Cicero seems to have made a connection between Spartan *scytalae* and the need for secrecy in his letters (Cicero, *Letters to Atticus*, 10.10.3; see also § 4.1.2). Cornelius Nepos recalled the story of how the Spartan general Pausanias received a *scytale* message urging him to come home because of misbehaviour (Cornelius Nepos, *The Book on the Great Generals of Foreign Nations*. Pausanias, 4.3.4). However, none of the Roman authors who discussed the *scytale* referred to any Roman use of the *scytale* as a cryptographic device – and there are no Roman sources known that show that the Romans ever used the *scytale* as a cryptographic device themselves. They certainly seem to have made the connection that conventionally associated the Spartan *scytale* with secrecy, but do not appear to have appreciated the value of the *scytale* as a practical device for secret communications (Cicero, *Letters to Atticus*, 10.10.3; Cornelius Nepos, *Book on the Great Generals of Foreign Nations*, 4.3.4; Aulus Gellius, *Attic Nights*, 17.9.15; Ausonius, *Epistles*, 28.28-29).

4.4: Reasons for absence of the *scytale* in sources on Roman warfare

There are a number of reasons to explain the fact that the Romans apparently did not use the *scytale* as a cryptographic device and why the Roman military, in particular, did not adopt the Spartan system of the *scytale*. In fact, Julius Caesar, followed by Augustus and his staff used the far less sophisticated Caesar cipher – even though they evidently had knowledge of the *scytale* (not least of all through their reception of Greek writings). One reason that the Romans, perhaps, did not adopt the *scytale* into their own secret communication models may have to do with the different means of sending official dispatches in Greece and Rome. In ancient Greece, the extant evidence suggests that official dispatches were often sent by a physical messenger for which a variety of terms were used: ἄγγελοι (*angeloi*; ‘messengers’), κήρυκες (*kerukes*; ‘heralds’), ἡμεροδρόμοι (*hemerodromoi*; ‘day-runners’), δρομοκήρυκες (*dromokerukes*; ‘couriers’) or δρομοκῆρυξ (*dromokerus*; ‘runner herald’). This messenger then delivered an ‘oral’ message – a message written to be read out (see e.g.: Aeneas Tacticus, *How to Survive Under Siege*, 22.3; 22.22; Archilochus, Fragment 185; Herodotus, *Histories*, 6. 105–6; 9. 12; Polyaeus, *Stratagems of War*, 5. 26. 1; Thucydides, *History of the Peloponnesian War*, 1.131.1).³⁶⁵ These messengers used an official messenger stick as a sort of authentication device (Archilochus, Fragment 185; Aristophanes, *Lysistrata*, 985-992; Pindar, *Olympian Odes*, 6.90-92) – one, possibly the original, use of the Spartan *scytale*-stick. In contrast to this method of official dispatch communication across the Greek world, in the Roman world letter writing – including official dispatches – appears to have become more of a private matter, with sealed letters sent from one individual to another (see e.g.: Cicero, *Against Catiline*, 3.5.12; *Letters to Brutus*, 2.5 = 5.4; *Letters to Friends*, 5.11.77; 6.3.8; Ovid, *Amores*, 2.15.15-18;

³⁶⁵ Carey 1981, 23-24; Ceccarelli 2013, 10-11; Gibson & Morrison 2007, 6-7.

Suetonius, *Lives of the Caesars* 2. *The Deified Augustus*, 50).³⁶⁶ However, sealed letters did not always guarantee privacy since individuals had to arrange on their own for the sending of their letters often by giving them to a traveller whereby they could only hope that this person would not read their letters – as could any unintended recipient.³⁶⁷ Cicero, for example, in his works mentions at least twice that he opened his brother's letters (Cicero, *Letters to Atticus*, 5.11.77; 6.3.8). Moreover, the Romans (especially Cicero) seem to have been aware of other issues related to the delivery of letters.³⁶⁸ Letters, for example, might fail to reach their destination (Cicero, *Letters to Atticus*, 2.8.1; 4.15.3; *Letters to Quintus* 3.7.6; *Letters to Friends*, 2.10.1; 12.19.1); their delivery could be delayed (Cicero, *Letters to Atticus*, 2.8.1), or they could be misdelivered (*Letters to Atticus*, 4.15.3). Yet, at least this idea of sealing letters shows that in Roman letter writing – as opposed to Greek – there was more of an idea of a shared individual (yet, not always private) space between the two communicating parties. Cicero, in his second Philippic oration describes a letter as a private conversation between absent friends (*amicorum conloquia absentium*; Cicero, *Marcus Tullius Cicero's Second Philippic Oration Against Marcus Antonius*, 2.7) while Henderson, in his discussion of Cicero's letters to his brother Quintus, even speaks of a 'private republic' in which the brothers communicated.³⁶⁹ Therefore, the Romans would have found the use of the *scytale* a wholly alien and inconvenient method of communication – secret or otherwise. Furthermore, wax tablets seem to have been more commonly used among the Romans for writing (as opposed to papyrus for the Greeks and the Greek speaking world).³⁷⁰ Indeed, one can assume that most – if

³⁶⁶ From the reign of Diocletian until the end of the Roman empire private letters even outnumber public letters/decrees (MacMullen 1982, 236).

³⁶⁷ Head 2009 (I); 2009 (II); Sarri 2017, 125.

³⁶⁸ See on security problems and other issues that Cicero encountered when sending his letters: Nicholson 1994.

³⁶⁹ Henderson 2007, 61.

³⁷⁰ Adkins & Adkins 2014, 209; Erdkamp 2011, 287; Jeffery 1961, 57; Lewis 2015, xxxix; Sherwood 2006, 536-537.

not all – of the secret letters discussed by Ovid, Cicero, Pliny the Elder and Ausonius and analysed in § 4.1 were written on wax tablets, as Ovid suggested (in e.g. *Amores* 1.11; 1.12; 2.5.17 and 3.496, *Ars Amatoria*, 2.396 and 3.621-624, and *Metamorphoses*, 9.450-665). Also, wax tablets were often favoured over papyrus since text could have been erased, and the tablets reused. This more common use of wax tablets for writing among the Romans would have made the use of the *scytale* – with its strips of papyrus or parchment – something rather alien and unpractical for the Romans. In addition, as has been discussed in § 4.3, like Aeneas Tacticus, the Romans apparently had a bigger interest in steganographic messages and devices than in cryptographic messages and devices.

At the beginning of this chapter, the following research question was posed: *What view of the scytale did the Roman's take and why did the Romans seemingly never adopt the Spartan scytale for cryptographic communications in their own military contexts – even though they seem to have been familiar with descriptions of the device and adopt other (less sophisticated) cryptographic systems?* First, following Herodotus and Aeneas Tacticus, the Romans seem to have had a greater interest in steganography than cryptography. Secondly, as a consequence of the environment in which letters were written and sent in the Roman world, it became more typical for sealed 'letters' (often written on folded wax tablets) to be sent from one individual to another. Letters and dispatches thereby became more of a private matter in contrast to the more open and public (because encrypted) method of official dispatch communication with a messenger carrying a *scytale* (stick) that we saw described in the sources as more common for letters and dispatches in the Greek world. Therefore, the use of the *scytale* must have seemed highly impractical and alien to the Romans. These reasons help to explain why the *scytale* model of secure and secret communication may not have been adopted by the Romans in their military field campaigns. Indeed, instead of adopting the Spartan *scytale* model the Romans instead used the far less sophisticated Caesar cipher. Roman sources, therefore, offer us our first

concrete evidence that the *scytale* was perceived as a tool for secret cryptographic communication in the classical world (as Strasser observed³⁷¹). Roman sources also give us the first solid confirmation for the operating principles of this cryptographic device, with detailed descriptions of how the *scytale* would have worked in the field. Indeed, these descriptions suggest that the *scytale* would have offered a far more sophisticated and secure encryption method than the so-called Caesar cipher (which is a very simple method to decode and –given the large number of people who must have known about Caesar’s preferred shift – surely cannot have been very secure).³⁷² However, we must look elsewhere for evidence to help us more fully appreciate the practical utility of the *scytale* as tool for secret communication and to better understand its use and value as a cryptograph for the ancient Spartans. This, I suggest, we can do best by examining the development of the transposition cipher system on which the *scytale* device was based in later periods – from the Renaissance right up to the 20th century and the Second World War.

³⁷¹ Strasser 2007, 278.

³⁷² The number of people who would have known about Caesar’s system depends on the number of correspondents with whom he used this system. There is no exact number we can readily identify in this case. Yet, since Caesar used secret communication in all his confidential correspondence – including with his relatives, generals, and *exploratores* and *speculatores* it is plausible that a large number of people knew about the cipher and its working.

Chapter 5: The development of the principle of the transposition cipher system of the *scytale* in ciphers from the Renaissance to the Second World War

In this chapter the development of the principle of the transposition cipher system of the *scytale* into Renaissance and modern 20th century transposition and substitution devices will be analysed. The research questions belonging to this chapter are the following: *How has the principle of the transposition cipher system of the Spartan scytale been used in later transposition ciphers and what does this tell us about the importance of the principle of the scytale system?*

Although the *scytale*-system did not have (direct) influence on later transposition and substitution ciphers, some connections can be seen between this Spartan fractionating transposition cipher and various later ciphers – starting with Renaissance systems using tables and cipher disks (Alberti; Bellaso), and eventually evolving into cipher machines such as the Enigma. The chapter starts with an analysis of a cipher disk invented by the Italian Renaissance scientist Leon Batista Alberti (§ 5.1); followed by a discussion of Bellaso's system – an improvement of Alberti's system (§ 5.2). Then I will analyse the first cipher machine (§ 5.3) – before finally turning to the electromechanical cipher machine: the Enigma (§ 5.4). In these discussions it will be shown that the principle of the transposition cipher system of the *scytale* has been found to be of use throughout the ages – especially in a context of warfare and for long distance communications, the same contexts in which the Spartans would have used their *scytalae* as cryptographic devices. Then it will be demonstrated that the basic idea behind the *scytale* can still be found in modern transposition ciphers that were used up to the Second World War – helping to show that the *scytale* would have been a practical and useful cryptographic device for the ancient Spartans to have used, particularly in military contexts (§ 5.5-6).

The Caesar cipher represents an important staging post in the history of cryptography, but following the fall of the Western Roman Empire, the use of cryptography and steganography in Western Europe appears to have stagnated for almost a thousand years, from before circa 500 CE to circa 1400 CE.³⁷³ During the Middle Ages in Europe, the use of cryptography and steganography even became synonymous with the use of dark arts and magic – echoing the early Egyptian tradition of using hieroglyphs for ‘mystical’ secret communications.³⁷⁴ Yet, via the Eastern Roman or Byzantine Empire – with its use of Greco-Coptic ciphers like the Caesar cipher – cryptography and steganography seem to have returned to Western Europe in the Late Middle Ages and early Renaissance.³⁷⁵ During this period we see more ciphers appear in which the basic transposition elements of the *scytale* can still be found, as will be discussed in this chapter (e.g. Alberti’s disk, Bellaso’s system). For, I want to argue that the ongoing, evolving, use of such cryptographic techniques in the Renaissance and into the 20th century offers compelling evidence for the usefulness of the basic operating principle on which the ciphertext encryption of the Spartan *scytale* was predicated – thereby supporting my central thesis that the *scytale* was indeed likely to have been used as a cryptographic device for secret encoded messaging in antiquity.

³⁷³ Dooley 2013, 12; Kahn 1967, 78; Saiber 2017, 23. See also Saltzman 2018 for a discussion of cryptography among Early medieval English monks, an exception to the rule.

³⁷⁴ Caubet 2008, 421; Mollin 2005, 4-5; Pieprzyk, Hardjono, and Seberry 2013, 6.

³⁷⁵ After the 1st century CE there is little extant evidence for the use of substitution ciphers like the Caesar cipher in the Roman empire – especially in the western part. Christians – especially in the Eastern Roman empire – continue to use Caesar ciphers in Greek, Coptic, and Syriac, the three main languages used in Christian scripts from Late Antiquity until the Middle Ages. See e.g.: Darnell & Darnell 2002; Delattre 2008; Fronczak 2013; Wisse 1979.

5.1: Alberti's cipher disk (1466-1467 CE)

In 1466-1467 Leon Battista Alberti introduced a polyalphabetic cipher in his work *De Componendis Cifris* (*A Composition of Ciphers*). In polyalphabetic ciphers more than one ciphertext alphabet is used to encrypt and decrypt an entire message – as opposed to Caesar's monoalphabetic cipher always with the right shift of three.³⁷⁶ Kahn attributes the invention of polyalphabetic ciphers to Alberti.³⁷⁷ However, it can only be said with certainty that Alberti's cipher is the first *known* polyalphabetic cipher.³⁷⁸ Evidence for earlier polyalphabetic ciphers may be lost. Alberti's cipher certainly represented a major improvement on the Caesar cipher in using multiple alphabets for encrypting messages. However, Alberti introduced a radically new – or, rather, a radically old – cryptographic principle to increase the security and sophistication of his cipher: he worked with a cipher disk in order to encode his messages using a substitution of letters in the ciphertext alphabets. This is shown in Alberti's description of the working of the cipher disk where he suggested that one had to position the two plates of the disk that contained letters relative to each other by turning them around and in that way changing the position of the letters on the disks:

sub B itidem sit index ipse k. Hinc demum caeterae omnes litterae minores in epistola inventae superiorum stabilium vim et sonos significabunt (Alberti, *De Componendis Cifris*, 14; for the complete passage see Appendix 2, page 301-304).

Positioning the mobile circle so that the B sits over the index k. Then all of the rest of the lower-case letters present in the coded text will take their meaning and sound from those of the fixed circle above them

³⁷⁶ Apelbaum 2007, 54; Salomon 2003, 59; Salomon 2006, 243; Strasser 2007, 281.

³⁷⁷ Kahn 1967, 94-95.

³⁷⁸ Apelbaum 2007, 54; Bauer 2007, 382; Salomon 2003, 59; Salomon 2006, 243.

The cipher disk that Alberti described consisted of two concentric circular plates, both made out of copper, one placed on top of the other. On the bottom plate of the disk, called ‘*stabilis*’, or ‘*stationary*’, the 20 capital letters of the 15th-century Italian alphabet were written followed by the numbers one to four (*De Componendis Cifris*, 14-15).³⁷⁹ These letters and numbers were written down in their normal order, from A to Z and from 1 to 4 and represented the plaintext (see Figure 15).³⁸⁰ On the upper plate of the disk, called ‘*mobilis*’, or ‘*moveable*’, the 23 letters of the Latin alphabet used in the 15th century were written in lower case letters and in random order together with the ampersand symbol. These letters and the symbol represented the ciphertext (*De Componendis Cifris*, 14).³⁸¹ Since the two plates of Alberti’s disk were only fixed in the middle with a pin, they could turn around. Hereby, the upper plate of the disk was used to turn, ‘to move’, while the other disk stayed in its original position.

³⁷⁹ See Figure 15 for a reconstruction of Alberti’s cipher disk. Compared to the modern 26-letter ISO Basic Latin alphabet used in English the letters H, J, K, W, and Y were not in use in Alberti’s system. The letters ‘U’ and ‘V’ were used as one letter. In the reconstruction we notice that these two letters share one place.

³⁸⁰ Strasser 2007, 281; Kahn 1996b, 128; Lunde 2012, 73.

³⁸¹ Strasser 2007, 281; Lunde 2012, 73. When discussing Alberti’s disk D’Agapeyeff incorrectly argues that cipher wheels always had to consist of an outer disk which had the letters of the alphabet in their usual order, and an inner disk containing the letters of the same alphabet in reversed order (D’Agapeyeff 1939, 119).

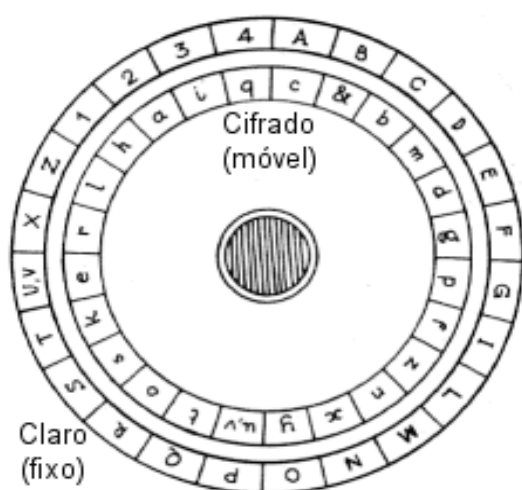


FIGURE 15: POSSIBLE RECONSTRUCTION OF ALBERTI'S CIPHER DISK BASED ON HIS DISCUSSION OF THE CIPHER DISK IN HIS WORK 'DE COMPONENTIS CIPRIS'.³⁸²

When using Alberti's disk, both sender and recipient needed an identical cipher disk – just as the Spartans needed two *scytalae* of the same size and diameter to communicate easily with each other. In Alberti's model, ciphertext sender and recipient would then need to agree on the code key by choosing an index letter – a letter on the upper disk that Alberti used as reference: in his example the lowercase letter 'k' that was positioned opposite capital 'B' on the bottom disk (*De Componentis Cifris*, 14). Both sender and recipient had to place their disks in these settings to start encryption and decryption and anyone who intercepted the message could not have deciphered it easily without having both a cipher disk identical to the one used by the sender of the message and the agreed key – as we saw in the case of the Spartan *scytale* whereby an enemy could not easily decipher an intercepted message without having a *scytale* of the exact size of the original rod himself. Moreover, just as the Spartans used the *scytale* for long distance communication, so did Alberti use his disk – which becomes clear when he discussed

³⁸² Facultad de Informática 2018. Translation of terms: 'cifrado': ciphertext (literally: 'encryption'); 'móvel': moveable; 'claro': plaintext (literally: 'clear'); fixo 'stationary' (literally: 'fixed').

how a receiver – far away – had to figure out the right settings of the disk to decipher the messages he had received:

Tu [...] in omment al interlegendum admonitus inventa maiuscula eam scies nihil aliud importare ex se nisi ut moneat mobilis circuli situm atque indicis collocationem isthic esse immutatam (Alberti, *De Componendis Cifris*, 14; for the complete passage see Appendix 2, page 301-304).

You [...], far away and receiving the message, have to look carefully in reading to find the upper-case letter, which you will know serves solely to indicate the positioning of the mobile circle and that the index has changed.

Alberti's substitution coding essentially worked in the same way as Caesar's substitution technique, whereby every letter of a plaintext message – on the bottom disk – was substituted by a ciphertext letter – on the upper disk. Yet, improving upon Caesar's fixed transposition principle in which every letter was moved precisely three places along the alphabet, in Alberti's system letters were transposed and changed places by regularly moving the upper disk relative to the bottom disk. At set intervals, Alberti rotated the upper disk to create a different setting or key:

Cum autem tres quottuorve dictiones exscripsero mutabo nostra in formula situm indicis versione circuli, ut sit index ipse k fortassis sub R. (Alberti, *De Componendis Cifris*, 14; for the complete passage see Appendix 2, page 301-304).

After I [Alberti] have written three or four words I will mutate the position of the index in our formula, rotating the disk let's say, so that the index k falls below the upper-case R.

In this way another substitution of the letters took place. What is more, Alberti's system did not only make use of letters that changed position, but also of the symbol of the ampersand (&) – on the upper disk – and four numbers on the bottom disk. On the bottom disk – next to the 20 letters of the Italian alphabet – one could find the numbers 1 to 4 (*De Componendis Cifris*, 14). According to Alberti, these numbers were permuted into groups of two, three or four digits,

e.g. 12 or 314. Numbers could also appear more often in a combination, which gave various combinations such as 11 or 4444. This gave Alberti 336 two-, three- and four-digit groups that each represented a ‘standard’ or common phrase or sentence. The numerical codes for these sentences could be found in a table which Alberti had also created to accompany his disk (*De Componendis Cifris*, 15-16). As Alberti stated, number 12, for example, meant: ‘*We have made ready the ships which we promised and supplied them with troops and grain*’ (*Naves quas polliciti sumus milite frumentoque refertas paravimus*; *De Componendis Cifris*, 16). Thus, sender and recipient also needed Alberti’s codebook to completely decipher complex messages in addition to having identical cipher disks. With the cipher disk but without the codebook anyone intercepting a ciphertext encrypted using Alberti’s device could only have partially decoded the original message. Whenever number codes were contained within the ciphertext, for instance, the first phase of decoding would have seen numbers substituted with two to four alphabetical letters – producing seemingly senseless sequences of letters that would not form a word, such as ‘*xp*’ or ‘*dkge*’. With Alberti’s description of the codebook in mind, Kahn attributes the invention of enciphered code to Alberti.³⁸³ Yet, again evidence for earlier enciphered codes may be lost. Although the changing of letters into numerical values (as seen in Alberti’s example) is a characteristic of substitution ciphers, the additional level of encryption can be compared to the encryption principles of the transposition system of the *scytale* whereby partial Greek letters were turned into gibberish when the strip was unwrapped from its original rod. Indeed, the similarities to be found between Alberti’s disk and the Spartan *scytale* are highly suggestive. First, we see the disk is rotated – as letters of a *scytale* message were transposed when the strip was unwrapped from its rod. Secondly, in both cases specific devices were needed to encipher and decipher the messages: the Spartans – and any other Greeks who tried to decipher their messages – needed two *scytalae* of the same size and

³⁸³ Kahn 1967, 94.

diameter to easily decode and understand each other's messages, while users of Alberti's disk would have needed both disk and a codebook to decipher messages completely. In fact Alberti believed his system to be the best suitable way for sending secret messages over a long distance:

tu igitur in provincia cum ad te meae pervenerint litterae [...] quo scribendi commento nihil brevius, nihil tutius, nihil ad cyfrarum usum excogitari aptius accommodatiusve potest [...] (Alberti, *De Componendis Cifris*, 16).

when you who are far away receive my letter [...] I will say that there is no invention that is quicker, more secure and nothing devised for cyphers could be more aptly suited [than my system] [...].

Although, of course, Alberti's Renaissance disk is not in itself evidence that the Spartan *scytale* was also used for secret messaging, it helps to prove that such devices would have worked efficiently and would have offered the Spartans a potentially secure method of secret communication. And, it is my contention, just as Alberti used his disk for confidential communication – and that could have been in warfare – so the Spartans would have used the *scytale* for the same purpose in the same context.

5.2: Bellaso's system (ca. 1553 CE)

In the mid-16th century Giovan (or: Giovanni) Battista Bellaso made further significant refinements to Alberti's disk – refinements which again help to illustrate the merits of the ancient Spartan *scytale* system of encryption and help to prove its practical utility as a method of secret messaging. Bellaso's system was discussed in his 1553 work *La Cifra del Sig. Giovan Battista Bellaso gentil'huomo bresciano, nuovamente da lui medesimo ridotta à grandissima brevità et perfettione* (*The cipher of Mr. Giovan Battista Bellaso, a gentleman from Brescia, once again reduced by himself to great brevity and perfection*). Since Bellaso's manuscript is not easily available, the discussion of the working of his method is based on the work of modern

scholars.³⁸⁴ In the Bellaso system eleven ciphertext alphabets are created in which the letters of the second half of the alphabet are transposed one place to the right every time. All these second halves are then jumbled around and added to the first half to create not only an incomprehensible ciphertext, but also eleven incomprehensible ciphertext alphabets available for the encryption. Just as the letters of a *scytale* message turned into an incomprehensible anagram when the encryption took place as the strip was unwrapped from the *scytale* rod, so, in Bellaso's system two incomprehensible anagrams were created: one to create the table used for encryption and one for the encrypted message itself. Also, just as Bellaso used his method for his confidential long distance communication, e.g. in warfare – so the Spartans would have used the *scytale* for the same purpose in the same context.

5.3: Cipher machines (18th-20th century CE)

In the 18th century the first cipher machines appear. An example is Jefferson's wheel cipher invented by Thomas Jefferson in 1795 (see Figure 16). In this device a set of wheels or disks was placed in a row, each disk with the letters of the alphabet arranged around their edge.³⁸⁵ For this cipher machine the modern 26-letter English alphabet was used. The order of the letters was different for each disk and was usually scrambled in a random way – as letters of *scytale* messages were scrambled when the strip was unwrapped from the *scytale*. Each disk was marked with a unique number. In case of the Jefferson wheel cipher, these were the numbers 1 to 36 since Jefferson's device had 36 disks. Every disk had a hole in its centre which allowed the disks to be stacked on an axle in the middle.³⁸⁶ Again, we can see fundamental similarities

³⁸⁴ Bauer 2007; Couto 2006; Lunde 2012; Strasser 2007.

³⁸⁵ Kahn 1996b, 194; Luenberger 2012, 176.

³⁸⁶ Kahn 1996b, 194; Luenberger 2012, 176.

with the Spartan *scytale* here. The axle can be seen as the *scytale* rod – while the removable disks are similar to the strip of writing material that could be wrapped and unwrapped from the *scytale*. As text was written on the strip on the *scytale* – so text – in this case letters – was printed on the disks. Indeed, like the strips of leather or papyrus wrapped and unwrapped around the *scytale* rod, the disks on Jefferson’s cipher machine were removable and could be mounted on the axle in any order desired. Since each disk was marked with a unique number, the order of the disks, agreed upon between sender and recipient, was indicated by a row of numbers that represented the right order of the disks.³⁸⁷ Whereas in the case of the *scytale* both parties needed a *scytale* of the same size and diameter to communicate with each other – in case of Jefferson’s method both parties needed Jefferson’s cipher machine. Sender and receiver had to arrange the disks in the same predefined order. Once the disks had been placed on the axle in the agreed upon order, the sender rotated each disk up and down until a desired message was spelled out in one row.³⁸⁸ Then the sender could copy down any row of text on the disks other than the one that contained the plaintext message. The recipient simply had to arrange the disks in the agreed-upon order, rotate the disks so that they spelled out the encrypted message on one row, and then look around the rows until he found the plaintext message, i.e. the row that is not complete gibberish.

³⁸⁷ Kahn 1996b, 194; Here one can see the principle of the key as discussed by Aeneas Tacticus once more (Aeneas Tacticus, *How to Survive Under Siege*, 31.1).

³⁸⁸ Kahn 1996b, 194; Luenberger 2012, 176.

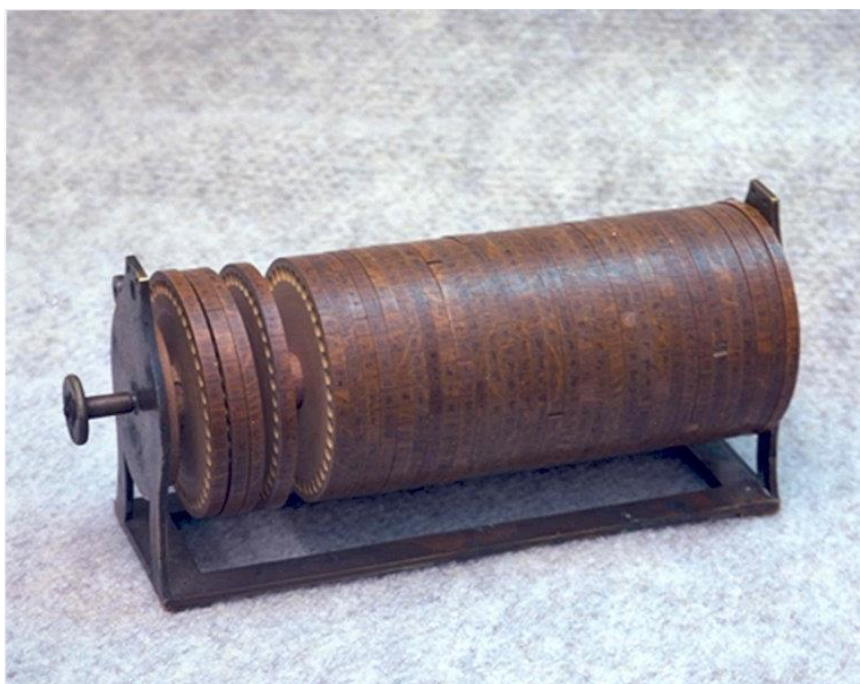


FIGURE 16: AN EXAMPLE OF THE JEFFERSON WHEEL CIPHER.³⁸⁹

When using the *scytale*, the encrypted ciphertext message became comprehensible only once the strip had been wrapped around the *scytale* again – and in the case of the Jefferson wheel cipher the message reappeared when the recipient had found the right row in the disk that corresponded with that of the plaintext. Cipher machines – such as the Jefferson wheel cipher – did not become well known until an independent invention by the French commander Etienne Bazeries (in 1891) popularised their use in military contexts about a hundred years later.³⁹⁰ Indeed, a reinvention of the system – known as the M-94 Cylinder Cipher – was used by the United States Army from 1922/1923-1942 (see Figure 17).³⁹¹ Like Jefferson’s wheel cipher, Bazeries’ device consisted of removable disks (in this case 25)³⁹² – like the removable strip with writing material that could be wrapped and unwrapped from the *scytale* – and an axle in

³⁸⁹ NSA Picture Gallery Online 2018.

³⁹⁰ Kahn 1996b, 413; Kopal 2018, 941; Kruh 1981, 197.

³⁹¹ Bauer 2013, 205.

³⁹² Kruh 1981, 195.

the middle – like the *scytale* rod. Similarly, both parties needed identical devices – both parties in the United States Army needed a M-94 cylinder to communicate with each other – just as for the Spartans both parties needed an identical *scytale* rod. And, it is my contention, just as the United States army used the M-94 Cylinder cipher for secret communication until halfway into the Second World War, so the Spartans would have used the *scytale* for secret communication in warfare.



FIGURE 17: M-94 CIPHER CYLINDER USED BY THE UNITED STATES ARMY FROM 1922/1923-1942.³⁹³

5.4: The Enigma machine (Early to mid-20th century)

Finally, there exists a superficial physical resemblance between an Enigma machine and the *scytale* rod, where the disks on the axle of the machine might be compared to the strip of writing material that was wrapped about the *scytale* rod (see Figure 18). However, the Enigma machine and the *scytale* system have nothing in common in terms of actual functionality, beyond their common use as cryptographic devices. Yet, it can be usefully kept in mind that, just as the Germans used the Enigma machine to attempt to secure their secret

³⁹³ Kopal 2018, 94

and confidential communication in warfare, so the Spartans would have used the *scytale* for the same purpose in the same context.



*FIGURE 18: ROTORS ON ENIGMA MACHINE. ENIGMA MACHINE USED BY THE GERMAN MILITARY INTELLIGENCE SERVICES IN THE SECOND WORLD WAR.*³⁹⁴

Although we have no archaeological artefacts equivalent to these modern examples of the *scytale* to demonstrate its operations, Plutarch's and Aulus Gellius' descriptions (as discussed in chapters 2 and 4) are detailed enough to determine that it is the same mode of ingenious rearrangement of the letters that makes the *scytale* a candidate for the earliest known theoretical transposition cipher in history and forerunner to all of these later models (Plutarch, *Life of Lysander*, 19.5-7; Aulus Gellius, *Attic Nights*, 17.9.6-16). When we understand how important such transposition ciphers have been in more recent history (particularly in military contexts),

³⁹⁴ Author's illustration, courtesy of the National Cryptologic Museum.

it may help us to better appreciate how the *scytale* might have been a valuable cipher system in ancient history too.

5.5: 20th century transposition and columnar transposition ciphers

In the First World War – almost 2500 years after the Spartans used the *scytale* – the German military intelligence services used a transposition cipher in all their confidential correspondence, based on a principle similar to that used in the *scytale*.³⁹⁵ In the 1920s, transposition ciphers were used by the Irish Republican Army, while during the Second World War various forms of transposition ciphers were used by both Axis and Allied powers: by Royal Air Force pilots, by Britain's Special Operations Executive (SOE), and by German troops operating in Latin America.³⁹⁶ By the end of the First World War and during the Second World War transposition ciphers had developed even further. In this period, combinations of transposition and substitution ciphers were used, by both the Axis and Allied Powers, and by resistance groups³⁹⁷ – including, perhaps, the most famous ciphers that used a combination of transposition and substitution: the German ADFGX and ADFGVX ciphers (as discussed in the prologue to this thesis).³⁹⁸

In simple modern transposition ciphers, the letters of a message are rearranged to generate an incomprehensible anagram, but remain *intact* – a crucial point in this case.³⁹⁹ Most modern transposition ciphers are created by the use of a grid composed of squares or cells.⁴⁰⁰

³⁹⁵ Dooley 2016, 62-65.

³⁹⁶ Bauer 2013, 128; 130; 136. See also Bauer 2017, 217-222.

³⁹⁷ Churchhouse 2002, 45-46; Kahn 1996b, 535; 539.

³⁹⁸ Childs 1919, 13; Diepenbroek 2019; Dooley 2016, 65.

³⁹⁹ Bishop 2003, 19; Collard 2004; Stamp & Low 2007, 5.

⁴⁰⁰ Reinke 1962, 116.

The cryptographer inscribes one letter in each cell, writing from left to right (for most Western languages), and from top to bottom (see Figure 19).

Q	U	I	S	S	I	M	S	C
I	E	S	E	X	E	O	Q	U
E	M	A	D	T	E	M	I	S
I	C	U	R	A	U	T	V	I
R	S	I	S	E	T	C	O	G
I	T	A	Q	U	E	M	I	N
L	O	C	U	M	S	I	S	P
R	O	G	R	E	S	S	U	S
V	I	D	E	Q	U	I	D	T
I	B	I	I	A	M	S	I	T
N	E	C	E	S	S	E	E	T
C	U	R	A	U	T	O	M	N
I	U	M	T	I	B	I	A	U
X	I	L	I	A	A	D	I	U
N	G	A	S	E	T	I	A	M
I	N	F	I	M	O	R	U	M

FIGURE 19: EXAMPLE OF MODERN SUBSTITUTION CIPHER. STEP 1: PLAINTEXT MESSAGE WRITTEN IN GRID, TEXT WRITTEN FROM LEFT TO RIGHT AND TOP TO BOTTOM.⁴⁰¹

With the text of the message written into the grid, a modern cryptographer still has the normal plaintext before her (see Figure 19). To make the message incomprehensible, a second step has to be taken. In other words: the transposition has to take place. To achieve this, a second rectangle is drawn in which the cryptographer re-transcribes the same message. However, now the letters in the columns, from top to bottom, are written horizontally from left to right, starting at the top left (see Figure 20). So, instead of starting the first row with the letters *Q-U-I-S*, it now starts with *Q-I-E-I*, the letters that were first in the first column and that are now transposed to another row.

⁴⁰¹ Author's illustration based on Reinke 1962, 116.

Q	I	E	I	R	I	L	R	V
I	N	C	I	X	N	I	U	E
M	C	S	T	O	O	I	B	E
U	U	I	G	N	I	S	A	U
I	A	C	G	D	I	C	R	M
L	A	F	S	E	D	R	S	Q
U	R	E	I	E	A	T	I	S
I	S	X	T	A	E	U	M	E
Q	A	S	U	I	A	E	M	I
E	E	U	T	E	S	S	U	M
S	T	B	A	T	O	M	O	M
T	C	M	I	S	I	S	E	O
I	D	I	R	S	Q	I	V	O
I	S	U	D	I	E	M	A	I
A	U	C	U	S	I	G	N	P
S	T	T	T	N	U	U	M	M

FIGURE 20: EXAMPLE OF MODERN SUBSTITUTION CIPHER. STEP 2: ENCRYPTION TEXT, TEXT FROM COLUMNS WRITTEN FROM LEFT TO RIGHT IN ROWS.⁴⁰²

Now, the cryptographer has the encrypted ciphertext – an incomprehensible anagram in which every letter has changed position. To make decryption even harder, the cryptographer can choose not only to write the letters of the columns as if they were the letters of the rows, but also to rearrange the order of the columns. This is called columnar transposition in modern cryptographic terms.⁴⁰³ If columnar transposition is applied to a grid, a numerical key or a keyword shows the intended recipient the right order of the columns. Another possibility for the cryptographer to make decryption harder is to divide the text into columns which can then be further rearranged (e.g. in Figure 21 the text is cut into three columns).

⁴⁰² Author's illustration based on Reinke 1962, 116.

⁴⁰³ Dooley 2013, 8; Klima & Sigmon 2012, 34-35.

Q I E I	R I L R	V I N C
I X N I	U E M C	S T O O
I B E U	U I G N	I S A U
I A C G	D I C R	M L A F
S E D R	S Q U R	E I E A
T I S I	S X T A	E U M E
Q A S U	I A E M	I E E U
T E S S	U M S T	B A T O
M O M T	C M I S	I S E O
I D I R	S Q I V	O I S U
D I E M	A I A U	C U S I
G N P S	T T T N	U U M M

FIGURE 21: EXAMPLE OF MODERN SUBSTITUTION CIPHER. STEP 3: ENCRYPTED TEXT DIVIDED INTO GROUPS OF FOUR LETTERS.⁴⁰⁴

Indeed, in the same way as the *scytalae* rods on which a message was enciphered and deciphered in the ancient world must be perfectly matched cylinders, the interval between the successive letters of the plaintext in a columnar cipher must always remain constant. Indeed, as Bauer cogently points out, columnar transposition ciphers can be broken by using high-tech graph paper and scissors.⁴⁰⁵

This is, in fact, how modern cryptanalysts in the First World War would try to decipher some transposition ciphers: they would cut the text in the grids into strips – either horizontally or vertically. These strips were then juxtaposed (see Figure 22).⁴⁰⁶ By sliding the strips up and down (or from side to side), the cryptanalyst would eventually have come to the point where she correctly surmised that one or more of the resulting trigraphs represented a clear text. The number of places that the cryptanalyst had to slide the strips relative to each other to get this clear text would have given her the interval that she was looking for. Then, when she had noted the interval between the letters of any one decoded trigraph, she would

⁴⁰⁴ Author's illustration based on Reinke 1962, 116.

⁴⁰⁵ Bauer 2013, 124.

⁴⁰⁶ Author's illustration based on Reinke 1962, 115-116.

have applied this same interval to the other strips to establish the sequence of the letters in the rest of the dispatch, and she would eventually have arrived at the complete solution.⁴⁰⁷ The deciphering of the encryption interval in this modern example is, perhaps, the equivalent of figuring out the exact diameter of a Spartan *scytale* in antiquity.



FIGURE 22: EXAMPLE OF MODERN SUBSTITUTION CIPHER. CIPHERTEXT CUT INTO STRIPS.⁴⁰⁸

⁴⁰⁷ Reinke 1962, 115-116.

⁴⁰⁸ Author's illustration, based on Reinke 1962, 116.

5.6: 20th century cylindrical and strip ciphers

In 1891 the French Major Etienne Bazeries developed a 20-disk cylindrical cipher device, like the Jefferson wheel cipher. In 1913 the American officer Parker Hitt (re)invented this basic cylinder cipher, (a 10-disk device based on Bazeries' system) for the United States Army. Three years later, in 1916, Hitt then decided to flatten out the cylinder cipher into a strip cipher for ease of use.⁴⁰⁹ Around the same time, in 1917, Major Joseph O. Mauborgne, invented a similar 25-disk cipher device.⁴¹⁰ This work formed the basis for the cylindrical cipher device M-94 that was adopted by the United States Army in 1922.⁴¹¹ This device consisted of:

a central shaft on which is mounted a set of 25 rotatable alphabetical disks. On the rim of each disk is stamped a different, completely disarranged alphabet.⁴¹²

As in the case of the earlier cipher machines, like the Jefferson wheel cipher, we are dealing here with a cylinder on which the disks could be stacked around the shaft in any order desired to create cryptographic messages. The fact that the M-94 worked in a similar fashion to the earlier cipher machines described above becomes clear from Kruh's description of the M-94:

After the encipherer [or sender] places the disks on the shaft in the prearranged order, he revolves one disk after another to align the first 25 letters of the message in a horizontal row. Then he selects at random any one of the other rows, which will form 25 letters of gibberish, as the ciphertext. He repeats this process in groups of 25 letters to the end of the message.⁴¹³

⁴⁰⁹ Bauer 2017, 361-364; Dooley 2018, 137-138; Kruh 1981, 195; Salomon 2003, 422; 2006; 262.

⁴¹⁰ Curley 2013, 25; Kruh 1981, 197.

⁴¹¹ Curley 2013, 25; Dooley 2018, 137-138; Kruh 1981, 193.

⁴¹² Kruh 1981, 193-194.

⁴¹³ Kruh 1981, 194.

The decipherer (or recipient) – who had knowledge of the correct order of the disks to decipher the message – would then have assembled the ‘disks on the shaft’ in the required order (turning each disk so that the ciphertext can be read across them), and would look for the line that contained the message – this was the line that was not complete gibberish.⁴¹⁴ About a decade later, in 1933, however, the army decided to move to Hitt’s flattened strip cipher and in 1934 the so-called M-138 strip cipher was officially adopted by the US military, followed by the improved version, the M-138-A, in 1938.⁴¹⁵ The M-138 and the M-138-A were ‘flat strip cipher board’ substitution ciphers that were (again) cryptologically equivalent to the Jefferson wheel cipher (similarly utilising ‘different, sliding, mixed alphabets’), and to the previously discussed M-94 cipher.⁴¹⁶ Yet, in this case paper strips were used in a flat device instead of the wheels on the M-94 cipher machine. When using the M-138-A the cryptographer had a choice between 100 strips on which the alphabet was printed twice – every time in a different order. Thirty strips were selected to use each time, as opposed to the 25 disks on the M-94 (see Figure 23).⁴¹⁷ The increasing number of strips obviously increased the security of the system. The M-138-A cipher saw a great deal of use within the American military intelligence services – especially during the Second World War – and lasted until the 1960s.⁴¹⁸ In fact, even though electromechanical cipher machines (like Enigma) were introduced during the Second World War ‘strip cipher systems continued in use by individuals, such as military attaches or units not authorised to use cipher machines’, and even as ‘standby equipment for [electromechanical cipher] machine users’.⁴¹⁹ To encipher and decipher the strip cipher M-138-A the

⁴¹⁴ Kruh 1981, 194.

⁴¹⁵ Bauer 2017, 361-364; Dooley 2018, 137-138; Kruh 1981, 195; Salomon 2003, 422; 2006; 262.

⁴¹⁶ Kruh 1981, 193. See also Bauer 2003, 119.

⁴¹⁷ Bauer 2003, 119; Kruh 1981, 195.

⁴¹⁸ Bauer 2017, 361-364.

⁴¹⁹ Kruh 1981, 196.

cryptographer would need the right device for encryption and the strips would have to be in the correct order to enable the cryptanalyst to understand the message (see Figure 21-22) – again, just as, when enciphering and deciphering a *scytale* message, both sender and recipient would have needed *scytalae* of the exact same size and diameter to be able to properly and easily communicate with each other. In this context, it is significant that (according to Kruh) the US Army distributed its own flat strip cipher devices ‘to at least six foreign governments including France, Italy, and Russia so they would maintain secure communications with United States Army personnel’.⁴²⁰

⁴²⁰ Kruh 1981, 196.

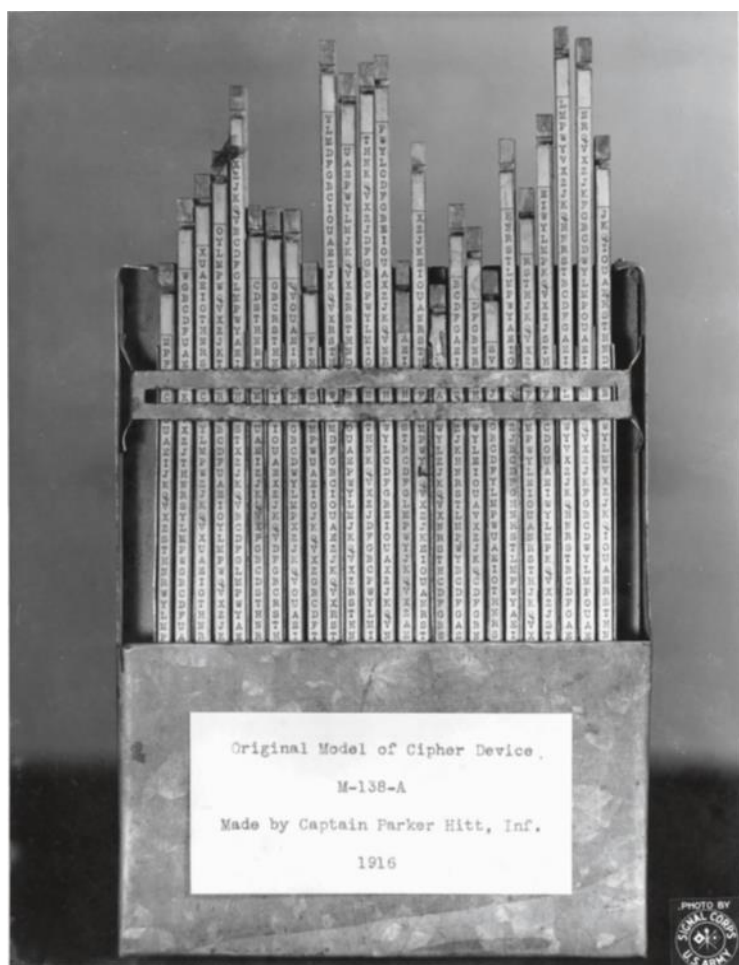


FIGURE 23: MODEL OF STRIP CIPHER M-138-A, USED BY THE AMERICAN INTELLIGENCE SERVICE FROM 1916-1960S, ESPECIALLY DURING THE SECOND WORLD WAR.⁴²¹

Although there are no direct connections between the Spartan *scytale* and these 20th-century ciphers (and a great many *operational* differences despite some ostensible *optical* similarities), just as 20th century cryptographers used (columnar) transposition ciphers, cylinders and strip ciphers for their secret and confidential communication in warfare, so – I argue – the Spartans would have used the *scytale* for the same purpose in the same context. In fact, I suggest that the Spartan system that Plutarch and Gellius described was arguably even more complicated than some of these transposition ciphers. For, when using the *scytale* the Spartan cryptanalyst would end up having many partial and broken letters in the code while,

⁴²¹ Bauer 2017, 361-364. Source: National Cryptologic Museum.

in these later ciphers, the letters retain their identity, but simply lose their position.⁴²² In other words, the cryptanalyst does not end up with partial and broken letters. When a twentieth century cryptanalyst intercepted a secret message written in a modern transposition cipher, she could decipher the message by rearranging the order of the letters. However, when a Spartan intercepted an encrypted message written by use of *scytale*, he would have had to deal with both whole and partial letters (see Figure 10). He would therefore have needed a *scytale* of the exact same diameter as the one that was used to write the original message in order to quickly restore the original place of all the scrambled letters – both complete and partial.

During the First and Second World Wars, encryption by means of transposition ciphers like the *scytale* was still done by hand. Cryptographers would use physical tables, grids, and strips of paper to encipher and decipher their confidential correspondence. Since the 1970s and 1980s, as computer systems took over from handwritten correspondence, cryptography became electronic. Instead of physical tables, grids and strips of paper, computers were used to encipher and decipher messages. However, the principle of the Spartan *scytale* can now still be seen in some modern digital transposition ciphers – as we can, for example, see in the fact that – alongside modern mathematics unknown to ancient societies – the basic principle of transposition encryption can still be found in the Advanced Encryption Standard (AES), a specification for the encryption of electronic data established by the United States National Institute of Standards and Technology (NIST) in 2001 and still used worldwide, and ultimately in the *New Scytale* algorithm in which literally, yet digitally, a secret message is wrapped around a geometric form in the same way the Spartans wrapped

⁴²² Kahn 1967, xi.

scytale messages around *scytalae*.⁴²³ These historical cryptographic examples show the fundamental and enduring usefulness of relatively simple ciphers – supporting the main argument of this thesis that the *scytale* would similarly have been useful in the ancient world as a cryptographic device. Moreover, as these various examples of the widespread use of ciphers using encryption techniques broadly analogous to those of the *scytale* attest, simple though a cipher may appear, it may not be easy to solve.⁴²⁴

At the beginning of this chapter, the following research question was posed: *How has the principle of the transposition cipher system of the Spartan scytale been used in later transposition ciphers and what does this tell us about the importance of the principle of the scytale system?* This chapter has shown that throughout the ages similar cryptographic elements keep reappearing in different cipher systems (often in the physical resemblance) recalling the design and operation of the Spartan *scytale* – either by creating incomprehensible anagrams (as seen in all devices) or by the physical design of the devices with their disks or rotors containing letters – akin to the strip of writing material on the *scytale* containing scrambled letters and alphabetic fragments. All forms of the ciphers and devices discussed in this chapter could have – and in several cases, as we have seen, definitely were – used in warfare for encrypting and decrypting secret long distance communication in the same way as the Spartans used their *scytalae*. On this basis it seems naïve for modern historians of cryptography to dismiss the ancient Spartan *scytale* as a ‘toy’ cipher and to deny its value as a real cryptographic device. In other words, as a report from the US Army Security Agency argues: *‘It is very easy for us to condemn old devices in the light of later knowledge, and the M-94 looks childishly simple to us now, but let nobody*

⁴²³ Boicea, Rădulescu et al., 2016, 2-6; Garg 2009, 387; NIST 2001, 1-51. Shannon in 1949 already showed that one needs to use both transposition and substitution to have decent security (Shannon 1949, 656–715).

⁴²⁴ Churchhouse 2002, 42.

*underestimate the good purpose that it did serve at a period when something better than the old Cipher Disk and Playfair were badly needed.*⁴²⁵ The same, I suggest, is true of the Spartan *scytale*.

⁴²⁵ Army Security Agency, 1948. 39.

Chapter 6: Summary and Conclusion

The 21st century will see transposition regain its true importance.⁴²⁶

The aim of this thesis was to reassess the extant evidence concerning the cryptographic Spartan device known as the *scytale* and to challenge the view promoted by some modern historians of cryptography that sees the *scytale* essentially as a simple ‘stick’ or staff that would have served little practical use as a vehicle for secret communication in the ancient world. I have demonstrated that, on the contrary, the cryptographic principles employed in the *scytale* are potentially more complex and secure than other known ancient ciphers (especially the system used in the so-called Caesar cipher). Indeed, as we have just seen in the preceding chapter, I have drawn comparisons with a selection of historic ciphers in order to illustrate the relative sophistication of the Spartan *scytale* as a practical device for secret communication. The overarching research question of this thesis was: *What can a comprehensive review and reassessment of the extant sources describing the cryptographic Spartan device known as the scytale do to challenge the view promoted by modern historians of cryptography that denies the scytale its deserved status as a vehicle for secret communication in the ancient world?* My answers to this question can be summarised in the following way: first, as an introductory case study to help illustrate the validity of my approach, I established common links and principles of operation comparing signalling techniques for encoded communications in the ancient world and in later periods. Thereby, I established the theoretical reliability of Aeneas Tacticus’ method for fire signalling and – more significantly – the fact that when we see the same basic technologies of coded communication exhibited in antiquity and again in the First World War, we can begin to appreciate more fully the practical efficiency and value of those basic

⁴²⁶ Bauer 2000, 100.

technologies and techniques as they might have been used in antiquity. Indeed, as we saw through the case study analysed in the prologue to this thesis, the fact that ancient core principles of cryptography were still in use in some form in 20th century methods for secret communication demonstrated that these methods would and could have worked well in antiquity too.

I then turned to examine a salient selection of the earliest examples of secret communication in the classical world, particularly Herodotus' four examples of secret communication as described in his *Histories*. I demonstrated that these early examples of secret communication are associated with non-Greeks and their use characterised as un-Greek behaviour. Hereby, I also demonstrated that Herodotus' account of Demaratus' letter to the Spartans nicely illustrates the biased ancient Greek view of the Spartans as a society familiar with the use of secret communication (in contrast to the open modes of communication preferred by other Greeks) and that the Spartans may have learned about the use of secret communication from the Persians.

This work established the groundwork for the main focus of the thesis and prepared the way for a detailed analysis of various ancient myths concerning the Spartan *scytale*. Mindful of the absence of any direct Spartan sources on the *scytale*, and of the biases in non-Spartan sources (including the contradictory stereotyping of the ancient Spartans as both practitioners of secret written communications *and* as semi-illiterate), I investigated a comprehensive range of surviving non-Spartan sources. I demonstrated that Greek sources vary widely in their discussions of the *scytale* and, although they were broadly consistent in associating the *scytale* with messaging, they typically did not associate it with secret messaging per se. The clearest descriptions of the *scytale* as a cryptographic device came only from later sources: Plutarch and Aulus Gellius. Although my analysis showed that Plutarch's and Aulus Gellius' descriptions alone did not prove that *scytalae* were used in practice for secret communication,

I argued that the ingenious transposition encryption that they described as the key feature of *scytale* communication made the *scytale* a candidate for the earliest known theoretical transposition cipher in history. Taking together all the extant sources on the *scytale*, I therefore argued that it was wholly plausible that Spartan *scytalae* were actually used for secret communication – among other purposes – even though the concrete evidence for this use remains largely inaccessible.

Having demonstrated the obvious potential of the *scytale* as a simple yet secure device for secret communication, I considered the enigma of why the *scytale* should apparently be overlooked by one of the most important classical Greek sources on practical ancient forms of secret communication – Aeneas Tacticus’ *How to Survive Under Siege*. After analysing the relevant sections of the treatise, I suggested various reasons to explain the fact that Aeneas Tacticus did not discuss the *scytale* in chapter 31 of *How to Survive Under Siege*. I observed that *scytalae* would typically have been used for long distance communications rather than for the sort of local communications that concerned Aeneas Tacticus. I further argued that Aeneas Tacticus – living and writing in a post-war period (after the Peloponnesian War) – may well have considered Spartan devices like the *scytale* as un-Greek and as therefore unworthy of inclusion in his treatise for Greeks. Finally, and perhaps most importantly, I demonstrated that Aeneas Tacticus seemed to have been more interested in steganographic practices than cryptographic practices since the main focus in *How to Survive Under Siege* is upon hiding messages so as to smuggle them in and out of the besieged *polis* and not upon encoding them so as to prevent them from being read and understood by hostile agents out in the field. I concluded, then, that the absence of the Spartan *scytale* from Aeneas Tacticus’ treatise did not in itself offer sufficient evidence to support the theory forwarded by Whitehead, West, and Sheldon that the *scytale* was unknown to Aeneas Tacticus because it was not really an ancient cryptograph.

I next tackled another apparent absence in the ancient historical record, investigating why the Romans seemingly never adopted the Spartan *scytale* for cryptographic communications in their own military contexts – even though they were evidently familiar with descriptions of the device – and I asked why they preferred to adopt other (less sophisticated) cryptographic systems such as the so-called Caesar cipher. I argued that, like Aeneas Tacticus, the Romans seem to have had a greater interest in steganography than cryptography, potentially as a consequence of the environment in which ‘sealed’ wax tablet letters were written and sent in the Roman world. I suggested that the use of the *scytale* must have consequently seemed highly impractical and alien to the Romans and helped to explain why the *scytale* model of secure and secret communication was not adopted by them. Hereby, I identified that Roman sources not only offered us our first concrete evidence that the *scytale* was perceived as a tool for secret cryptographic communication in the classical world but that Roman rather than Greek sources also give us the first solid confirmation for the operating principles of this cryptographic device. However, I concluded that we must look elsewhere for evidence to help us more fully appreciate the practical utility of the *scytale* as tool for secret communication and to better understand its use and value as a cryptograph for the ancient Spartans.

This evidence, I argued, could be achieved by examining the cipher systems in later periods – from the Renaissance right up to the 20th century, through the Second World War, and beyond. I demonstrated that, throughout the ages, analogous principles to those employed by the *scytale* system have played a major role in the history of cryptography (particularly in military contexts). On the basis of the comparisons I made, I concluded that it was naïve for some modern historians of cryptography to dismiss the ancient Spartan *scytale* as a ‘toy’ cipher and to deny its historic value as a real cryptographic device. Although modern cryptographic systems have now supplanted classical ciphers like the Spartan *scytale*, the basic concepts associated with the transposition cipher that we see in the Spartan use of the

scytale are still used today – ultimately in the *New Scytale* algorithm in which secret messages are digitally wrapped around a geometric form.⁴²⁷ The fact that this core principle can still be found in the most recent and sophisticated examples of communication security demonstrates that it would have worked well in antiquity too.

C. Bauer – in his 2017 book *Unsolved!: The History and Mystery of the World's Greatest Ciphers from Ancient Egypt to Online Secret Societies*, in which a section is dedicated to ancient Greek cryptography, including the Spartan use of the *scytale* – argues that a summary of ancient Greek cryptography must, of necessity be incomplete.⁴²⁸ This is an important caveat since we only have access to a small sample of original extant material – only a tiny proportion of which survives and which necessarily offers us only an incomplete picture of the role of cryptography in antiquity. What is more, secret communication – by its very nature – is secret. Therefore, a great deal of information about ancient cryptography is concealed from as well as unavailable to modern eyes. As this thesis has demonstrated, one of the reasons that we know so little about the Spartan *scytale* and its actual deployment is because the Spartans were (at least, according to Athenian sources) a relatively ‘secretive’ society. Yet, Bauer’s caveat has provided one of the core inspirations behind the shape and scope of this thesis. For, although it is itself also necessarily incomplete, this thesis includes the most comprehensive catalogue of classical cryptography from Greco-Roman antiquity – and represents the only study to date to seek to understand the value and operating principles of the Spartan *scytale* by analysing its cryptographic potential through comparison with modern transposition cipher systems.⁴²⁹ In setting out this research in this way, I hope to have unravelled some of the myths surrounding the Spartan *scytale* in particular and of classical

⁴²⁷ Boicea, Rădulescu et al., 2016, 2-6; Garg 2009, 387; NIST 2001, 1-51.

⁴²⁸ Bauer 2017, 99.

⁴²⁹ See for a complete list of Greek and Roman sources on cryptography and steganography: Appendix 1.

Greek and Roman cryptography more widely. And, to paraphrase F. Bauer, I hope not only that ‘the 21st century will see transposition regain its true importance’ but that the 21st century will see the ancient Spartan *scytale* regain its true importance in the history of cryptography too.⁴³⁰

⁴³⁰ Bauer 2000, 100.

Bibliography

- Achtemeier, P. J. (1990). Omne Verbum Sonat: The New Testament and the Oral Environment of Late Western Antiquity. *Journal of Biblical Literature*, 109 (1), 3-27.
- Adams, J. N. (2003). *Bilingualism and the Latin Language*. Cambridge: Cambridge University Press.
- Adkins, L., & Adkins, R. (2014). *Handbook to Life in Ancient Rome*. New York: Facts on File.
- Al-Kadi, I. A. (1992). Origins of Cryptology: The Arab Contributions. *Cryptologia*, 16 (2), 97-126.
- Aly, W. (1943). *Fragmentum Vaticanum de Eligendis Magistratibus: e Codice bis Rescripto Vat. Gr. 2306*. Vatican City: Biblioteca apostolica Vaticana.
- Anderson, G. (2004). Aulus Gellius as a Story Teller. In: Holford-Strevens, L. & A. Vardi, *The Worlds of Aulus Gellius*. Oxford: Oxford Univeristy Press, 105-117.
- Anderson, J. K. (1970). *Military Theory and Practice in the Age of Xenophon*. Berkeley/ Los Angeles: University of California Press.
- Apelbaum, Y. (2007). *User Authentication Principles, Theory and Practice*. Second Edition. Pewaukee: Fuji Technology Press.
- Aschoff, V. (1984). *Geschichte der Nachrichtentechnik: Beiträge zur Geschichte der Nachrichtentechnik von ihren Anfängen bis zum Ende des 18. Jahrhunderts*. Berlin/ Heidelberg/ New York/ Tokyo: Springer-Verlag.
- Army Security Agency (1948). *The History of Army Strip Cipher Devices (July 1934-October 1947)*. SRH-366. Washington D.C.: US Army Security Agency.
- Babbitt, F. C. (1931). *Plutarch: Moralia I. (Vol. II: Sayings of Kings and Commanders. Sayings of Romans. Sayings of Spartans. The Ancient Customs of the Spartans. Sayings of Spartan Women. Bravery of Women; Loeb Classical Library 245)*. Cambridge (Massachusetts): Harvard University Press.
- Barends, D. (1955). *Lexicon Aeneium : a Lexicon and Index to Aeneas Tacticus' Military Manual "On the Defence of Fortified Positions"*. Assen: Van Gorcum.
- Barley, S., Lewis, W., Beach, J., & Berghof, O. (2006). *The Etymologies of Isidore of Seville*. Cambridge: Cambridge University Press.
- Bartlett, J. (2002, March 17). *The Ease of Steganography and Camouflage*. SANS Institute InfoSec Reading Room.
- Bauer, C. P. (2013). *Secret History: The Story of Cryptology*. Boca Raton/ London/ New York: CRC Press - An Imprint of Taylor and Francis Group.
- Bauer, C. P. (2017). *Unsolved! The History and Mystery of the World's Greatest Ciphers from Ancient Egypt to Online Secret Societies*. New Jersey/ Woodstock: Princeton University Press.
- Bauer, F. L. (2000). *Decrypted Secret - Second Edition*. Berlin: Springer.
- Bauer, F. L. (2007). Rotor Machines and Bombes. In K. de Leeuw, & J. A. Bergstra, *The History of Information Security: A Comprehensive Handbook* (pp. 381-446). Amsterdam/ Boston/ Heidelberg/ London/ New York/ Oxford/ Paris/ San Diego/ San Francisco/ Singapore/ Sydney/ Tokyo: Elsevier.
- Bauer, F. L. (2013). *Decrypted Secrets: Methods and Maxims of Cryptology*. Berlin/ Heidelberg: Springer-Verlag.
- Bellamy, R. (1989). Bellerophon's Tablet. *The Classical Journal*, 84 (4), 289-307.
- Bengtson, H. (1962). Die griechische Polis bei Aeneas Tacticus. *Historia: Zeitschrift für Alte Geschichte*, 11 (4), 458-468.
- Bengtson, H. (ed). (1975). *Die Staatsverträge des Altertums: Die Verträge der griechisch-römischen Welt von 700 bis 338 v. Chr.* 2nd ed. Munich/ Berlin: C. H. Beck.

- Bennett, C. E., & McElwain, M. (1925). *Frontinus: Stratagems. Aqueducts of Rome* (Vol. 174 Loeb Classical Library). Cambridge (Massachusetts): Harvard University Press.
- Bettalli, M. (1990). *Enea Tattico, La Difesa di una Città assediata (Poliorketika). Introduzione, Traduzione e Commento*. Pisa: ETS editrice.
- Bishop, D. (2003). *Introduction to Cryptography with Java Applets*. Surbury/ Boston/ Toronto/ London/ Singapore: Jones and Bartlett Publishers.
- Blamire, A. (1959). Herodotus and Histiaeus. *The Classical Quarterly*, 9 (2), 142-154.
- Bliese, J. R. (1994). Rhetoric Goes to War: The Doctrine of Ancient and Medieval Military Manuals. *Rhetoric Society Quarterly*, 23 (3-4), 105-130.
- Bodel, J. P. (2001). *Epigraphic Evidence : Ancient History from Inscriptions*. London: Routledge.
- Boedeker, D. (1987). The Two Faces of Demaratus. *Arethusa*, 20 (1), 185-201.
- Boicea, A., Rădulescu, F., Truică, C.-O., & Grigore, E. (2016). New Scytale - Improving Encryption Techniques. International Business Information Management Association Conference on Visio 2020: Sustainable Growth, Economic Development, and Global Competitiveness, (pp. 1-6).
- Boring, T. A. (1979). *Literacy in Ancient Sparta*. Leiden: Brill.
- Bowie, A. (2013). "Baleful Signs": Letters and Deceit in Herodotus. In O. Hodkinson, P. Rosenmeyer, & E. Bracke, *Epistolary Narratives in Ancient Greek Literature* (pp. 71–83). Leiden: Brill.
- Bowie, A. M. (2007). *Histories: Book VIII*. Cambridge/ New York: Cambridge University Press.
- Bowie, E. (2019). Alcaeus' *stasiotica*: Catulland and Horation Readings. In B. Currie, & I. Rutherford, *The reception of Greek lyric poetry in the ancient world : transmission, canonization and paratext* (pp. 279-294). Leiden/ Boston: Brill.
- Bowman, A. K. (1975). The Vindolanda writing tablets and the development of the Roman book form. *Zeitschrift für Papyrologie und Epigraphik*, 18, 237-252.
- Bowra, C. M. (1972). *Homer*. London: Duckworth.
- Brandt, P. (1963). *P. Ovidi Nasonis: Amores Libri Tres*. Hildesheim: Georg Olms Verlagsbuchhandlung.
- Briant, P. (2002). *From Cyrus to Alexander: a History of the Persian Empire*. Winona Lake (Indiana): Eisenbrauns.
- Brown, T. S. (1981). Aeneas Tacticus, Herodotus and the Ionian Revolt. *Historia: Zeitschrift für Alte Geschichte*, 30 (4), 385-393.
- Brownson, C. L. (1918). *Xenophon: Hellenica* (Vol. I: Books 1-4; Loeb Classical Library 88). Cambridge (Massachusetts): Harvard University Press.
- Brownson, C. L. (1921). *Xenophon: Hellenica* (Vol. II: Books 5-7; Loeb Classical Library 89). Cambridge (Massachusetts): Harvard University Press.
- Burkert, W. (1983). Oriental Myth and Literature in the Iliad. In R. Hägg, *The Greek Renaissance of the Eighth Century BC: Tradition and Innovation* (pp. 51–56). Stockholm: Svenska Institutet in Athen.
- Burliga, B. (2008). Aeneas Tacticus between History and Sophistry: the Emergence of the Military Handbook. In J. Pigeon, *The Children of Herodotus. Greek and Roman Historiography and Related Genres* (pp. 92-101). Newcastle: Cambridge Scholars Publishing.
- Burrell, B. (2009). Reading, Hearing, and Looking at Ephesos. In W. Johnson, & H. Parker, *Ancient Literacies: The Culture of Reading in Greece and Rome* (pp. 69-95). Oxford: Oxford University Press.
- Butler, S. (2012). *The Hand of Cicero*. London: Routledge.
- Campbell, D. (2006). *Besieged: Siege Warfare in the Ancient World*. Oxford/ New York: Osprey Publishing.

- Candau Morón, J. M. (2000). Plutarch's *Lysander* and *Sulla*: Integrated Characters in Romans Historical Perspective. *American Journal of Philology* (121), 453-478.
- Carey, C. (1981). *A Commentary on Five Odes of Pindar*. New York: Arno Press.
- Cartledge, P. (1978). Literacy in the Spartan Oligarchy. *Journal of Hellenistic Studies* (98), 25-37.
- Cartledge, P. (2001). *Spartan reflections*. London: Duckworth.
- Cartledge, P. (2003-I). *The Spartans: The World of the Warrior-Heroes of Ancient Greece, from Utopia to Crisis and Collapse*. New York: Vintage Books.
- Cartledge, P. (2003-II). *Spartan Reflections*. Berkeley: University of California Press.
- Cartledge, P. (2009). *Ancient Greek Political Thought in Practice*. Cambridge: Cambridge University Press.
- Cartledge, P. (2013-I). Herodotus The Histories: Introduction and Notes. In T. Holland, & P. Cartledge, *Herodotus The Histories* (pp. xv-xxxvii; 641-704). London: Penguin Classics.
- Cartledge, P. (2013-II). *Sparta and Lakonia: A Regional History 1300-362 BC*. London/ New York: Routledge - An Imprint of Taylor and Francis Group.
- Cary, E., & Foster, B. (1914). *Dio Cassius: Roman History* (Vol. III: Books 36-40; Loeb Classical Library 53). Cambridge (Massachusetts): Harvard University Press.
- Catling, H. W. & Cavanagh, H. (1976). Two inscribed bronzes from the Menelaion, Sparta. *Kadmos*, 15, 145-157.
- Caubet, A. (2008). Vitreous Materials. In J. Aruz, K. Benzel, & J. Evans, *Beyond Babylon: Art, Trade, and Diplomacy in the Second Millennium B.C.* (pp. 419-434). New York/ New Haven/ London: The Metropolitan Museum of Art/ Yale University Press.
- Cavazza, F. (2004). Gellius the Etymologist. In: Holford-Strevens, L & A. Vardi, *The Worlds of Aulus Gellius*. Volume 1. Oxford: Oxford University Press, 65-104.
- Ceccarelli, P. (2013). *Ancient Letter Writing: A Cultural History (600 BC-150 BC)*. Oxford: Oxford University Press.
- Ceccarelli, P. (2019). *Athenaios* (166). (I. Worthington, Editor) Retrieved from Brill's New Jacoby, Second Edition. Consulted online on 04 January 2020. Retrieved from: http://dx.doi.org.bris.idm.oclc.org/10.1163/1873-5363_bnj2_a166
- Ceccarelli, P. (2019). *Autokrates* (297). (I. Worthington, Editor) Retrieved from Brill's New Jacoby, Second Edition. Consulted online on 04 January 2020. Retrieved from: http://dx.doi.org.bris.idm.oclc.org/10.1163/1873-5363_bnj_a297
- Chadwick, J. (1976). *The Mycenaean World*. Cambridge: Cambridge University Press.
- Chadwick, J. (1987). *Linear B and related Scripts*. Berkeley (California): University of California Press.
- Chaniotis, A. (2013). Greeks under Siege: Challenges, Experiences, and Emotions. In B. Campbell, & L. Tritle, *The Oxford Handbook of Warfare in the Classical World* (pp. 438-456). Oxford/ New York/ Auckland/ Cape Town/ Dar es Salaam/ Hong Kong/ Karachi/ Kuala Lumpur/ Madrid/ Melbourne/ Mexico city/ Nairobi/ New Delhi/ Shanghai/ Taipei/ Toronto: Oxford University Press.
- Chaniotis, A., Pleket, H. W., Stroud, R. S., and Strubbe, J. H. S. (2003). *Supplementum Epigraphicum Graecum* (Vol. 50). Amsterdam : Giebe.
- Chapman, G. A. (1972). Herodotus and Histiaeus' Role in the Ionian Revolt. *Historia: Zeitschrift für Alte Geschichte*, 21 (4), 546-568.
- Charzelis, G., & Harris, J. (2017). *A Tenth-Century Byzantine Military Manual: The Sylloge Tacticorum*. London/ New York: Routledge - An imprint of Taylor and Francis Group.
- Chatton, B. (2010). *Using Poetry Across the Curriculum: Learning to Love Language*. Santa Barbara: ABC-CLIO LLC.

- Cheshire Library Science (2013). *Caesar Cipher Encryption and Decryption tables*. Retrieved from: http://cheshirelibraryscience.files.wordpress.com/2013/03/caesa_cipher_left_shift_of_3-svg.com
- Childs, J. R. (1919). War Department Office of the Chief Signal Officer, Washington: German Military Ciphers from February to November 1918. Technical Paper of the Intelligence Section War Plans and Training Division. Washington.
- Christidis, A. F., Arapoglou, M. & Chriti, M. (2001). *A History of Ancient Greek: From the Beginnings to Late Antiquity*. Cambridge: Cambridge University Press.
- Churchhouse, R. F. (2002). *Codes and Cipher: Julius Caesar, the Enigma and the Internet*. Cambridge: Cambridge University Press.
- Clanchy, M. T. (1979). *From Memory to Written Record: England, 1066-1307*. Cambridge (Massachusetts): Cambridge University Press.
- Coles, M., & Landrum, R. (2009). *Expert SQL Server 2008 Encryption*. New York: Apress.
- Collard, B. (2004). Les Langues secrets dans l'Antiquité Gréco-Romaine. Introduction Générale, Plan et Bibliographie par Brigitte Collard. Retrieved from: Folia Electronica Classica (Louvain-la-Neuve) – Numéro 7 janvier - juin 2004. Retrieved from: <http://bcs.fltr.ucl.ac.be/FE/07/CRYPT/Intro.html>
- Cox, I., Miller, M., Bloom, J., Fridrich, J., & Kalker, T. (2008). *Digital Watermarking and Steganography* (2 ed.). Amsterdam/ Boston/ Heidelberg/ London/ New York/ Oxford/ Paris/ San Diego/ San Francisco/ Singapore/ Sydney/ Tokyo: Morgan Kaufman Publishers - An Imprint of Elsevier.
- Curley, R. (2013). *Cryptography: Cracking Codes*. New York: Britannica Educational Publishing.
- D'Agapeyeff, A. (1939). *Codes and Ciphers - A History of Cryptography*. Oxford / London / New York/ Toronto: Oxford University Press.
- Dain, A., & Bon, A. (1967). *Énée le Tacticien: Poliorcétique*. Paris: Les Belles Lettres.
- Damon, C. (2016). *Caesar: Civil War* (Vol. 39 Loeb Classical Library). Cambridge (Massachusetts): Harvard University Press.
- Darnell, J. C., & Darnell, D. (2002). Opening the Narrow Doors of the Desert: Discoveries of the Theban Desert Road Survey. In R. F. Friedman, *Egypt and Nubia: Gifts of the Desert* (pp. 132-155). London: The British Museum Press.
- David, E. (1986-I). Aeneas Tacticus, 11.7-10 and the Argive Revolution of 370 BC. *American Journal of Philology*, 107 (3), 343-349.
- David, E. (1986-II). The Oligarchic Revolution in Argos, 417 B.C. *L'Antiquité Classique* (55), 113-124.
- De Forest Allen, F., Burnet, J., Pomeroy Parker, C., & Greene, W. (1938). *Scholia Platonica*. Haverford: Societas Philologica Americana.
- Debidour, M. (2006). Le Secret et les Messages Secrets dans la Poliorcétique d'Énée le Tacticien. In H. Olivier, P. Giovannelli-Jouanna, & F. Bérard, *Ruses, Secrets et Mensonges chez les historiens grecs et latins* (pp. 213-241). Lyon: Université Jean Moulin-Lyon 3, 213-241.
- Delattre, A. (2008). Inscriptions Grecques et Coptes de la Montagne Thébaine Relatives au Culte de Saint Ammônios', in: Delattre, A, and Heilporn, P., *Et Maintenant ce ne Sont plus que des Villages. . . Thèbes et sa Région aux Époques Hellénistique, Romaine et Byzantine. Actes de Colloque Tenu à Bruxelles les 2 et 3 Décembre 2005*, Bruxelles: Association Égyptologique Reine Élisabeth, 183-188.
- Delebecque, E. (1957). Essai sur la Vie de Xénophon. *Revue des Études Anciennes Année*, 60 (3), 429-436.
- Dewald, C. (1993). Reading the World: The Interpretation of Objects in Herodotus' Histories. In R. Rosen, & J. Farrell, *Nomodeiktes: Greek Studies in Honor of Martin Ostwald* (pp. 55-70). Ann Arbor: University of Michigan Press.
- Dewald, C. (2003). Form and Content: The Question of Tyranny in Herodotus. In K. A. Morgan, *Popular Tyranny: Sovereignty and Its Discontents in Ancient Greece* (pp. 29-58). Austin: University of Texas Press.

- Dewing, H. B. (1935). *Procopius. The Anecdota or Secret History* (Vol. 290 Loeb Classical Library). Cambridge (Massachusetts): Harvard University Press.
- Diels, H. (1914). *Antike Technik. Sechs Vorträge*. Leipzig and Berlin: Teubner.
- Diepenbroek, M. L.M (2019). From Fire Signals to ADFGX. A case study in the Adaptation of Ancient Methods of Secret Communication. *KLEOS - The Amsterdam Bulletin of Ancient Studies and Archaeology* (2), 63-76. Retrieved from https://www.academia.edu/38962728/Martine_Diepenbroek_-_From_Fire_Signals_to_ADFGX._A_case_study_in_the_adaptation_of_ancient_methods_of_secret_communication
- Diepenbroek, M.L.M. (2020; forthcoming). The Spartan *scytale*. *Ancient Warfare Magazine*, 14 (3).
- Dimovski, A., & Gligoroski, D. (2003). Attacks on the Transposition Ciphers using Optimization Heuristics. *Proceedings of ICEST 2003* (pp. 1-4).
- Dirkzwager, A. (1976). Latijns Grieks. *Hermeneus Tijdschrift voor Antieke Cultuur*, 48 (2), 125-129.
- Donderer, M. (1995). Merkwürdigkeiten im Umgang mit Griechischer und Lateinischer Schrift in der Antike. *Gymnasium*, 102, 97-122.
- Dooley, J. F. (2013). *A Brief History of Cryptology and Cryptographic Algorithms*. Cham/ Heidelberg/ New York/ Dordrecht/ London: Springer.
- Dooley, J. F. (2016). *Codes, Ciphers and Spies: Tales of Military Intelligence in World War I*. New York: Copernicus Books - An imprint of Springer Nature.
- Dooley, J. F. (2018). *History of Computing*. Cham: Springer.
- Douglas Olson, S. (2009). *Athenaeus: The Learned Banqueters* (Vol. V: Books 10.420e-11; Loeb Classical Library 274). Cambridge (Massachusetts): Harvard University Press.
- Dräger, P. (2002). *D. Magnus Ausonius, Mosella, Bissula, Briefwechsel mit Paulinus Nolanus*. (P. Dräger, Ed., & P. Dräger, Trans.) Düsseldorf/Zürich: Artemis & Winkler.
- Dunkel, G. E. (2000). Remarks on Code-switching in Cicero's Letters to Atticus. *Museum Helveticum*, 57 (2), 122-129.
- Dvornik, F. (1974). *Origins of Intelligence Services: The Ancient Near East, Persia, Greece, Rome, Byzantium, the Arab Muslim Empires, the Mongol Empire, China, Muscovy*. New Brunswick/ New Jersey: Rutgers University Press.
- Eastaugh N., Walsh, V., Chaplin, T. and Siddall, R. (2004). *The Pigment Compendium: A Dictionary of Historical Pigments*, Volume 1. Amsterdam/ Boston/ Heidelberg/ London/ New York/ Oxford/ Paris/ San Diego/ San Francisco/ Singapore/ Sydney/ Tokyo: Elsevier Butterworth-Heinemann.
- Ebbeler, J. (2007). Mixed Languages: The Play of Epistolography Codes in Two Late Antique Latin Correspondences. In R. Morello, & A. D. Morrison, *Ancient Letters: Classical and Late Antique Epistolography* (pp. 301-324). Oxford: Oxford University Press.
- Edmonds, J. M. (1957). *The Fragments of Attic Comedy : after Meineke, Bergk and Kock augmented, newly edited with their Contexts, annotated, and completely translated into English Verse by John Maxwell Edmonds* (Vol. 1). Leiden: Brill.
- Edwards, H. J. (1917). *Caesar: The Gallic War* (Vol. 72 Loeb Classical Library). Cambridge (Massachusetts): Harvard University Press.
- Elder, O., & Mullen, A. (2019). *The Language of Roman Letters: Bilingual Epistolography from Cicero to Fronto*. Cambridge: Cambridge University Press.
- Eliade, M. (1970). *De Zalmoxis a Gengis-Khan : Études comparatives sur les Religions et le Folklore de la Dacie et de l'Europe Orientale*. Paris: Payot.
- Erasmus, D., & Mynors, R. (1991). *Adages* (Vol. Collected works of Erasmus Volume 33: Ili1 to Ili100). Toronto/ Buffalo: University of Toronto Press.

- Erasmus, D., & Mynors, R. (1992). *Adages* (Vol. Collected Works of Erasmus Volume 34: Ilvii1 to IIIiii100). Toronto/ Buffalo: University of Toronto Press.
- Erbse, H. (1971). *Scholia Graeca in Homeri Iliadem (scholia vetera) Recensuit Hartmut Erbse*: 2, Scholia ad libros E - I continens. Berlin: De Gruyter.
- Erdkamp, P. (2011). *A Companion to the Roman Army*. Malden: Wiley-Blackwell.
- Evans, J. A. (1976). Herodotus and the Ionian Revolt. *Historia: Zeitschrift für Alte Geschichte*, 25 (1), 31-37.
- Evelyn-White, H. G. (1921). *Ausonius, Paulinus Pellaues. Volume II: Books 18-20. Paulinus Pellaues: Eucharisticus*. (Vol. 115 Loeb Classical Library). Cambridge (Massachusetts): Harvard University Press.
- Ezov, A. (1996). 'The "Missing Dimension" of C. Julius Caesar', in: *Historia: Zeitschrift für Alte Geschichte*, 45 (1), 64-94.
- Fabule, D. K. (2011). *Information-gathering and the Strategic Use of Culture in Herodotus*. Stellenbosch: University of Stellenbosch.
- Facultad de Informática (2018). Facultad de Informática de la Universidad de Las Palmas de Gran Canaria: Leon Battista Alberti. Retrieved from: <http://serdis.dis.ulpgc.es/~ii-crypt/PAGINA%20WEB%20CLASICA/CRIPTOLOGIA/alberti>.
- Feemster Jashemski, W., & Meyer, F. G. (2002). *The Natural History of Pompeii*. Cambridge: Cambridge University Press.
- Ferrill, A. (1978). Herodotus on Tyranny. *Historia: Zeitschrift für Alte Geschichte*, 27 (3), 385-398.
- Fielding, I. (2017). *Transformations of Ovid in Late Antiquity*. Cambridge (United Kingdom)/ New York : Cambridge University Press.
- Fiorentino, G., & Zech-Matterne, V. (2018). *Agrumed: Archaeology and history of citrus fruit in the Mediterranean*. Naples: Publications du Centre Jean Bérard.
- Fischer, S. (2004). *A history of writing*. London: Reaktion Books Limited.
- Flaceliere, R. & Chambry, E. (1971). *Plutarque: Vies. Vol. VI, Pyrrhos-Marius/Lysandre-Sylla*. Paris: Les
- Flower, M. A. (1988). Agesilaus of Sparta and the Origins of the Ruler Cult. *The Classical Quarterly*, 38 (1), 123-134.
- Forster Smith, C. (2010). *A Study of Plutarch's Life of Artaxerxes - With Especial Reference to the Sources*. Morrisville: Lulu Press. First published: Forster Smith, C. (1881). *A Study of Plutarch's life of Artaxerxes with especial reference to the sources, a dissertation, by Charles Forster Smith*. Leipzig: Metzger und Wittig.
- Forrest, W. G. (1979). Motivation in Herodotos: The Case of the Ionian Revolt. *The International History Review*, 1 (3), 311-322.
- Forrester, J. M., & Henry, J. (2013). *The Subtiltate of Girolamo Cardano in two Volumes*. (J. Forrester, Ed.) Tempe: The Arizona Centre for Medieval & Renaissance Studies.
- Fowler, H. N. (1926). *Plato: Cratylus. Parmenides. Greater Hippias. Lesser Hippias* (Vol. 167 Loeb Classical Library). Cambridge (Massachusetts): Harvard University Press.
- Frazer, J. G. (1921). *Apollodorus: The Library, Volume I: Books 1-3.9* (Vol. 121 Loeb Classical Library). Cambridge (Massachusetts): Harvard University Press.
- Freisenbruch, A. (2007). Back to Fronto: Doctor and Patient in his Correspondence with an Emperor. In R. Morello, & A. Morrison, *Ancient Letters: Classical and Late Antique Epistolography* (pp. 235-256). Oxford: Oxford University Press.
- Fronczak, M. (2013). Atbah-Type Ciphers in the Christian Orient and Numerical Rules in the Construction of Christian Substitution Ciphers. *Cryptologia*, 37 (4), 338-344.
- Gardner, M. (1983). *Codes, Ciphers and Secret Writing*. New York: Dover Publications Incorporated.

- Gardthausen, V. E. (1911). *Griechische Paleographie* (Vol. 2: Die Schrift, Unterschriften und Chronologie im Altertum und im Byzantinischen Mittelalter). Leipzig: Veit & Comp.
- Garfield, S. (2013). *To the Letter: A Celebration of the Lost Art of Letter Writing*. Reprinted Edition. New York: Penguin Publishing Group.
- Garg, P. (2009). Genetic Algorithms, Tabu Search and Simulated Annealing: A Comparison between Three Approaches for the Cryptanalysis of Transposition Cipher. *Journal of Theoretical & Applied Information Technology*, 5 (4), 387-392.
- Gauthier, P. (1972). *Gauthier Symbola: les Étrangers et la Justice dans les Cités Grecques*. (Vol. Annales de l'Est, Mémoire 42). Nancy: Université de Nancy II.
- Georges, P. (1994). *Barbarian Asia and the Greek Experience*. Baltimore: Johns Hopkins University Press.
- Gerber, D. E. (1999). *Archilochus, Semonides, Hipponax: Greek Iambic Poetry: From the Seventh to the Fifth Centuries BC*. (Vol. 259 Loeb Classical Library). Cambridge (Massachusetts): Harvard University Press.
- Gerolymatos, A. (1986). *Espionage and Treason*. Amsterdam: J. C. Gieben Publisher.
- Gibson, R., & Morrison, A. (2007). Introduction: What is a Letter? In R. Morello, & A. Morrison, *Ancient Letters: Classical and Late Antique Epistolography* (pp. 1-16). Oxford: Oxford University Press.
- Glassner, J. (2003). *The Invention of Cuneiform: Writing in Sumer* (Originally published as: *Ecrive a Sumer: L'Invention du Cunéiforme*. Paris: Éditions de Seuil ed.). Baltimore: John Hopkins University Press.
- Glotz, G., & Cohen, R. (1936). *Histoire Grecque Tome III : La Grèce au IV^e siècle; la Lutte pour L'Hégémonie* (404-336). Paris: Les Presses universitaires de France.
- Godley, A. D. (1920). *Herodotus: The Persian Wars* (Vol. I: Books 1-2; Loeb Classical Library 117). Cambridge (Massachusetts): Harvard University Press.
- Godley, A. D. (1922). *Herodotus: The Persian Wars* (Vol. III: Books 5-7; Loeb Classical Library 119). Cambridge (Massachusetts): Harvard University Press.
- Godley, A. D. (1925). *Herodotus: The Persian Wars* (Vol. IV: Books 8-9; Loeb Classical Library 120). Cambridge (Massachusetts): Harvard University Press.
- Gomme, A., Andrewes, A., & Dover, K. (1981). *A Historical Commentary on Thucydides*. Oxford: Clarendon Press.
- Goody, J. (1986). *The Logic of Writing and the Organisation of Society*. Cambridge: Cambridge University Press.
- Goody, J., & Watt, I. (1968). The Consequences of Literacy. In J. Goody, *Literacy in Traditional Societies* (pp. 27-86). Cambridge: Cambridge University Press.
- Goold, G. P. (1977). *Ovid In Six Volumes I: Heroides and Amores* (Revised by G. P. Goold ed., Vol. 41 Loeb Classical Library). (G. Showerman, Trans.) Cambridge (Massachusetts): Harvard University Press.
- Gould, J. P. (2012). Herodotus (1). In S. Hornblower, A. Spawforth, & E. Eidinow, *The Oxford Classical Dictionary* (pp. 674-676). Oxford: Oxford University Press.
- Grafton, A., Most, G. W. & Settis, S. (2013). *The Classical Tradition*. Cambridge (Massachusetts)/ London (United Kingdom): The Belknap Press of Harvard University Press.
- Gray, V. (1995). Herodotus and the Rhetoric of Otherness. *The American Journal of Philology*, 116 (2), 185-211.
- Green, P. (1982). *Ovid: The Erotic Poems*. London: Penguin Classics.
- Guthrie, K. S. (1987). *The Pythagorean Sourcebook and Library: An Anthology of Ancient Writings Which Relate to Pythagoras and Pythagorean Philosophy*. (D. Fideler, Ed.) Grand Rapids: Phanes Press.
- Hall, E. (1989). *Inventing the Barbarian. Greek Self-Definition through Tragedy*. Oxford: Clarendon Press.
- Hall, J. (2009). *Politeness and Politics in Cicero's Letters*. Oxford: Oxford University Press.

- Hammond, M. (2009). *The Peloponnesian War: A New Translation by Martin Hammond*. Oxford: Oxford University Press.
- Hanson, V. D. (2007). The Modern Historiography of Ancient Warfare. In P. Sabin, H. van Wees, & M. Whitby, *The Cambridge History of Greek and Roman Warfare* (Vol. 1: Greece, the Hellenistic World, and the Rise of Rome, pp. 3-21). Cambridge: Cambridge University Press.
- Harris, R. (1995). *Enigma*. London: Arrow Books.
- Harris, W. V. (1989). *Ancient Literacy*. Cambridge (Massachusetts): Harvard University Press.
- Harvey, F. D. (1966). Literacy in the Athenian Democracy. *Revue des Études Grecques* (79), 585-635.
- Havelock, E. (1963). *Preface to Plato*. Cambridge (Massachusetts): Harvard University Press.
- Havelock, E. A. (1971). *Prologue to Greek Literacy*. Cincinnati: University of Cincinnati.
- Havelock, E. A. (1982). *The Literate Revolution in Greece and Its Cultural Consequences*. Princeton: Princeton University Press.
- Head, P. M. (2009-I). Letter-Carriers in the Ancient Jewish Epistolary Material. In C. Evans, & H. Zacharias, *Jewish and Christian scripture as artifact and canon* (Vol. 70, pp. 203-219).
- Head, P. M. (2009-II). Named Letter-Carriers among the Oxyrhynchus Papyri. *Journal for the Study of the New Testament*, 31 (3), 279-299.
- Henderson, J. (2000). *Aristophanes: Birds. Lysistrata. Women at the Thesmophoria*. (Vol. 179, Loeb Classical Library). Cambridge (Massachusetts): Harvard University Press.
- Henderson, J. (2007). ...when who should walk into the room but...': Epistoliterarity in Cicero, Ad Qfr. 3.1. In R. Morello, & A. Morrison, *Ancient Letters: Classical and Late Antique Epistolography* (pp. 37-86). Oxford: Oxford University Press.
- Herman, G. (1987). *Ritualised Friendship and the Greek City*. Cambridge: Cambridge University Press.
- Heubeck, A. (1979). *Archaeologia Homerica, Band 3, Kapitel X* (Vol. Schrift). Göttingen: Vandenhoeck & Ruprech.
- Hodges, A. (1985). *Alan Turing: The Enigma*. New York: Vintage Books.
- Hodkinson, S., & Powell, A. (2009). *Sparta: New Perspectives*. Swansea: The Classical Press of Wales.
- Hodkinson, S., & Powell, A. (2010). *Sparta: The Body Politic*. Swansea: The Classical Press of Wales.
- Holford-Strevens, L. (2003). *Aulus Gellius: An Antonine Scholar and his Achievement*. Oxford: Oxford University Press.
- Holford-Strevens, L. & Vardi, A. (2004). *The Worlds of Aulus Gellius*. Oxford: Oxford University Press.
- Holford-Strevens, L. (2019-I). *Aulus Gellius: Attic Nights: Preface and Books 1-10*. Oxford: Oxford University Press.
- Holford-Strevens, L. (2019-II). *Aulus Gellius: Attic Nights: Books 11-20*. Oxford: Oxford University Press.
- Holland, T., & Cartledge, P. (2013). *Herodotus The Histories*. London: Penguin Classics.
- Hollmann, A. (2005). The Manipulation of Signs in Herodotus' Histories. *Transactions of the American Philological Association* (1974-2014), 135 (2), 279-327.
- Holmes, T. R. (1911). *Caesar's Conquest of Gaul* (2nd edition: revised throughout and largely rewritten ed.). Oxford: Clarendon Press.
- Hondius, J. J. E. & Woodward, A. M. (1919/1920-1920/1921). Laconia I Inscriptions. *The Annual of the British School at Athens* (24: supplement), 88-143.
- Hornblower, S. (1996). *A Commentary on Thucydides*. Oxford: Clarendon Press.

- Hornblower, S. (2009). Sticks, Stones, and Spartans: The Sociology of Spartan Violence. In H. van Wees, *War and Violence in Ancient Greece* (pp. 57-82). London/ Swansea: Gerald Duckworth/ The Classical Press for Wales.
- Hornblower, S. (2010). *A Commentary on Thucydides*. Oxford: Oxford University Press.
- How, W. W., & Wells, J. (1928). *A Commentary On Herodotus* (Vol. 1 (Book I-IV); 2 (Book V-IX)). Oxford: Oxford University Press.
- Howley, J. A. (2018). *Aulus Gellius and Roman Reading Culture: Text, Presence, and Imperial Knowledge in the Noctes Atticae*. Cambridge: Cambridge University Press.
- Hug, A. (1877). *Aeneas von Stymphalos, ein Arkadischer Schriftsteller aus Klassischer Zeit: Gratulationsschrift der Universität Zürich an die Universität Tübingen zu deren vierhundertjähriger Stiftungsfeier vom VIII. - XI. August MDCCCLXXVII*. Zürich: Zürcher & Furrer.
- Hunt, A.S. (1929). A Greek Cryptogram. *Proceedings of the British Academy* 1929, 127-134.
- Hunter, L., & Handford, S. (1927). *Aineiou Poliorkētika: Aeneas on Siegecraft*. Oxford: Clarendon Press.
- Huxley, G. L. (1983). Herodotos on Myth and Politics in Early Sparta. *Proceedings of the Royal Irish Academy: Archaeology, Culture, History, Literature*, 83C, 1-16.
- Hyde, W. W. (1915). The Mountains of Greece. *The Bulletin of the Geographical Society of Philadelphia*, 13, 1-16; 47-64; 110-126.
- Illinois Greek Club. (1928). *Aeneas Tacticus, Asclepiodotus, and Onasander* (Vol. 156 Loeb Classical Library). Cambridge (Massachusetts): Harvard University Press.
- Immerwahr, H. R. (1990). *Attic Scripts, A Survey*. New York/ Oxford: Oxford University Press.
- Jacobson, H. (1974). *Ovid's Heroides*. Princeton: Princeton University Press.
- Jacoby, F., Bollansée, J., Bonnechere, P., & Radicke, J. (1969). *Die Fragmente der Griechischen Historiker* (Vol. 3B: Geschichte von Städten und Völkern (Horographie und Ethnographie); b. Kommentar zu Nr. 297-607; Text). Berlin: Weidmann.
- Jeffery, L. H. (1961). *The Local Scripts of Archaic Greece: A Study of the Origin of the Greek Alphabet and its Development from the eighth to the fifth centuries B.C.* Oxford: Clarendon Press.
- Jenkins, T. E. (1999). *Intercepted Letters: Epistles and Their Readers in Ancient Literature*. Cambridge (Massachusetts): Harvard University Press.
- Jestin, C., & Katz, P. (2000). *Ovid: Amores, Metamorphoses Selections*, 2nd Edition: *Amores, Metamorphoses : Selections*. Illinois: Bolchazy-Carducci Publishers.
- Johnson, N., Duric, Z., & Jajodia, S. (2001). *Information Hiding: Steganography and Watermarking-Attacks and Countermeasures*. Norwell: Kluwer Academic Publishers.
- Johnson, W., & Parker, H. (2009). *Ancient Literacies: The Culture of Reading in Greece and Rome*. Oxford: Oxford University Press.
- Jones, W. H., & Andrews, A. (1980). *Pliny: Natural History* (Vol. VII: Books 24-27; Loeb Classical Library 393). Cambridge (Massachusetts): Harvard University Press.
- Kahate, A. (2013). *Cryptography and Network Security*. Porur (Chennai): McGraw Hill Education.
- Kahn, D. (1967). *The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet*. London: Weidenfeld and Nicolson.
- Kahn, D. (1974). *The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet* (2nd edition, abridged). London: Weidenfeld and Nicolson.
- Kahn, D. (1996a). *The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet* (2nd edition, revised). London: Weidenfeld and Nicolson.

- Kahn, D. (1996b). The History of Steganography. In R. Anderson, *Information Hiding: First International Workshop, Cambridge, U.K., May 30 - June 1, 1996. Proceedings, Volume 1* (pp. 1-6). Cambridge: Springer-Verlag.
- Kajanto, I. (1980). Minderheiten und ihre Sprachen in der Hauptstadt Rom. In G. Neumann, & J. Untermann (Ed.), *Die Sprachen im Römischen Reich der Kaiserzeit: Kolloquium vom 8. bis 10. April 1974* (pp. 83-101). Cologne: Rheinland.
- Kartalopoulos, S. V. (2009). *Security of Information and Communication Networks*. Hoboken: Wiley-Blackwell.
- Kassel, R., & Austin, C. (1983). *Poetae Comici Graeci* (Vol. 2: Menander: Testimonia et Frangmenta apud scriptores servata). Berlin/ New York: De Gruyter.
- Kassel, R., & Austin, C. (1986). *Poetae Comici Graeci* (Vol. 5: Damoxenus - Magnes). Berlin/ Boston: De Gruyter.
- Kassel, R., & Austin, C. (1989). *Poetae Comici Graeci* (Vol. 7: Menecrates - Xenophon). Berlin/ Boston: De Gruyter.
- Kasten, J. (2001). One Fish, Two Fish, Red Fish, Blowfish: A History of Cryptography and its Application in Society. *Sans Institute InfoSec Reading Room*. Retrieved from <https://www.sans.org/reading-room/whitepapers/vpns/fish-fish-red-fish-blowfish-history-cryptography-its-application-soci-726>
- Keaney, J. J. (1974). Theophrastus on Greek Judicial Procedure. *Transactions of the American Philological Association*, 179-194.
- Keeline, T. J. (2018). *The reception of Cicero in the early Roman Empire : the Rhetorical Schoolroom and the Creation of a Cultural Legend*. Cambridge: Cambridge University Press.
- Keightley, T. (1856). *The Mythology of Ancient Greece and Italy: for the Use of Schools*. New York: D. Appleton and Company.
- Keightley, T. (1859). *The Mythology of Ancient Greece and Italy: for the Use of Schools*. New York: D. Appleton and Company.
- Kelly, T. (1985). The Spartan Scytale. In J. W. Eadie, & J. Ober, *The Craft of the Ancient Historian: Essays in Honor of Chester G. Starr* (pp. 141-169). Lanham: University Press of America.
- Kelly, T. (1998). The Myth of the Skytale. *Cryptologia*, 22 (3), 253-260.
- Kelsey, F. W. (2007). *Select orations and letters of Cicero*. Eugene: Wipf & Stock.
- Kennell, N. M. (2010). *Spartans: A New History*. Malden/ Oxford/ Chichester: John Wiley and Sons.
- Keulen, W. (2004). Gellius, Apuleius, and Satire on the Intellectual. In: Holford-Strevens, L., & A. Vardi, *The Worlds of Aulus Gellius*. Oxford: Oxford University Press, 223-246.
- Khan, I. A. (2007). *Citrus Genetics, Breeding and Biotechnology*. Wallingford: CABI.
- Kirk, G. S. (1962). *The Songs of Homer*. Cambridge: Cambridge University Press.
- Klima, R., & Sigmon, N. (2012). *Cryptology: Classical and Modern with Maplets*. Boca Raton/ London/ New York: Chapman and Hall/ CRC.
- Knight, G. R. (2005). Friendship and Erotics in the Late Antique Verse-Epistle: Ausonius to Paulinus Revisited. *Rheinisches Museum für Philologie Neue Folge* (Band 148, Herausgabe 3/4), 361-408.
- Kolb, A. (2001). Transport and Communication in the Roman State: the Cursus Publicus. In C. Adams, & R. Laurence, *Travel and geography in the Roman Empire* (pp. 95-105). London/ New York : Routledge.
- Konstan, D. (1987). Persians, Greeks and Empire. *Arethusa*, 20: *Herodotus and the Invention of History*, 59-73.
- Kopal, N. (2018). *Secure Volunteer Computing for Distributed Cryptanalysis*. Kassel: Kassel University Press.
- Kramer, J. (1983). *Glossaria Bilingua in Papyris et Membranis Reperta*. Bonn: Habelt.

- Krentz, P. & Wheeler, E. L (1994). *Polyaenus: Stratagems of War*. Chicago: Ares.
- Kruh, L. (1971). The Genesis of the Jefferson/Bazeries Cipher Device. *Cryptologia* 5 (4), 193-208.
- Ladner, G. (1979). Mediaeval and Modern Symbolism, a Comparison. *Speculum* (54), 223-256.
- Laks, A., & Most, G. W. (2016). *Early Greek Philosophy* (Vol. IX: Sophists, Part 2; Loeb Classical Library 532). Cambridge (Massachusetts): Harvard University Press.
- Lang, M. (1968). Herodotus and the Ionian Revolt. *Historia: Zeitschrift für Alte Geschichte*, 17 (1), 24-36.
- Lateiner, D. (1989). *The Historical Method of Herodotus*. Toronto: University of Toronto Press.
- Lateiner, D. (1990). Deceptions and Delusions in Herodotus. *Classical Antiquity*, 9 (2), 230-246.
- Lattimore, S. (1998). *The Peloponnesian War: Thucydides - Translated, with Introduction and Notes, by Steven Lattimore*. Indianapolis/ Cambridge: Hackett Publishing Company Incorporated.
- Leighton, A. C. (1969). Secret Communication among the Greeks and Romans. *Technology and Culture*, 10 (2), 139-154.
- Lewis, K. M. (2015). *How John wrote the Book of Revelation : from concept to publication*. Lorton: Kim Mark Lewis.
- Lewis, C. T., & Short, C. (2019). *Charlton T. Lewis, Charles Short, A Latin Dictionary Online*. Retrieved from: <http://www.perseus.tufts.edu/hopper/text?doc=clava&fromdoc=Perseus%3Atext%3A1999.04.0059>
- Liddel, P. (2018). Writing and Other Forms of Communication in Aineias' Poliorketita. In M. Pretzler, & N. Barley, *Brill's Companion to Aineias Tacticus* (pp. 123-145). Leiden/ Boston: Brill.
- Liddell, H., & Scott, R. (2014). *ἀχρημαί*. Retrieved from LSJ: The Online Liddell-Scott-Jones Greek-English Dictionary: <http://stephanus.tlg.uci.edu/ljsj/#eid=19173>
- Liddell, H., & Scott, R. (2014). *σκυτάλη* (*scytale*). Retrieved from LSJ: The Online Liddell-Scott-Jones Greek-English Dictionary: <http://stephanus.tlg.uci.edu/ljsj/#eid=98117>
- Lietzmann, H. (1968). *Kleine Texte für Vorlesungen und Übungen, 17-18. Begründet von Hans Lietzmann. Herausgegeben von Kurt Aland*. Berlin: Verlag Walter de Gruyter & Co.
- Luenberger, D. G. (2012). *Information Science*. Princeton: Princeton University Press.
- Luft, H. M. (1952). *An Examination of the Sources of Plutarch's Lives of Nicias and Lysander*, 2. Durham: Durham University E-Theses. Retrieved from http://etheses.dur.ac.uk/9656/2/9656_6445-vol2.PDF
- Lunde, P. (2012). *The Secrets of Codes: Understanding the World of Hidden Messages*. San Francisco: Weldon Owen.
- Luraghi, N. (1988). *Polieno come fonte per la Storia di Dionisio il Vecchio*. *Prometheus*, 164-180.
- Luschan, F. v., & Andrae, W. (1943). *Ausgrabungen in Sendschirli. v. 5. Die Kleinfunde von Senschirli*. Mittheilungen aus den orientalischen Sammlungen 15. Berlin: De Gruyter.
- Maas, G. S. (2012). Perseus and Bellerophon. In M. Gagarin, *The Oxford Encyclopedia of Ancient Greece and Rome* (Vol. 1, pp. 215-217).
- MacMullen, R. (1982). The Epigraphic Habit in the Roman Empire. *The American Journal of Philology*, 103 (3), 233-246.
- Macrakis, K. (2014). *Prisoners, Lovers, and Spies: The Story of Invisible Ink from Herodotus to Al-Qaeda*. New Haven/ London: Yale University Press.
- Malherbe, A. J. (1988). *Ancient Epistolary Theorists*. Atlanta: Scholars Press.
- Mallowan, M. E. (1966). *Nimrud and Its Remains I*. London: Collins.
- Manville, P. B. (1977). Aristagoras and Histiaios: The Leadership Struggle in the Ionian Revolt. *The Classical Quarterly*, 27 (1), 80-91.

- Marks, G. (2010). *Encyclopedia of Jewish Food* (eBook). Retrieved from: Encyclopedia of Jewish Food (online) https://books.google.nl/books?id=gFK_yx7Ps7cC&pg=PT458&dq=lemons+arab+sources&hl=en&sa=X&ved=0ahUKEwjy8ur6-fpAhWEM-wKHfUyB0EQ6AEIKDAA#v=onepage&q=lemons%20arab%20sources&f=false
- Martin, C. (2004). *Metamorphoses*. New York: Norton.
- McKeown, J. C. (1989). *Ovid: Amores. Text, polegomena and commentary*. Leeds: F. Cairns
- Melville, S., & Melville, D. (2008). Observations on the Diffusion of Military Technology: Siege Warfare in the Near East and Greece. In M. Ross, *From the Banks of the Euphrates: Studies in Honor of Alice Louise Slotsky* (pp. 145-168). Warsaw (USA): Eisenbrauns.
- Millender, E. G. (2001). Spartan Literacy Revisited. *Classical Antiquity*, 20 (1), 121-164.
- Miller, W. (1914). *Xenophon: Cyropaedia* (Vol. II: Books 5-8; Loeb Classical Library 52). Cambridge (Massachusetts): Harvard University Press.
- Millett, P. (2013). Writers on War: Part 1 Greece: Winning Ways of Warfare. In B. Campbell, & L. Tritle, *The Oxford Handbook of Warfare in the Classical World* (pp. 46-73). Oxford/ New York/ Auckland/ Cape Town/ Dar es Salaam/ Hong Kong/ Karachi/ Kuala Lumpur/ Madrid/ Melbourne/ Mexico City/ Nairobi/ New Delhi/ Shanghai/ Taipei/ Toronto: Oxford University Press.
- Mintz, A. I. (2018). Sparta, Athens, and the Surprising Roots of Common Schooling. *Philosophy of Education* 2018. Retrieved from: educationjournal.web.illinois.edu
- Mollin, R. A. (2000). *An Introduction to Cryptography*. Boca Raton/ London/ New York/ Washington: Chapman & Hall/ CRC.
- Mollin, R. A. (2005). *Codes: The Guide to Secrecy From Ancient to Modern Times*. Boca Raton/ London/ New York/ Singapore: Chapman & Hall/CRC - An imprint of Taylor and Francis Group.
- Montanari, F. (2015). *The Brill Dictionary of Ancient Greek*. (M. Goh, & C. Schroeder, Eds.) Leiden: Brill.
- Moore, R. (2013). Generalship: Leadership and Command. In B. Campbell, & L. Tritle, *The Oxford Handbook of Warfare in the Classical World* (pp. 457-473). Oxford/ New York/ Auckland/ Cape Town/ Dar es Salaam/ Hong Kong/ Karachi/ Kuala Lumpur/ Madrid/ Melbourne/ Mexico city/ Nairobi/ New Delhi/ Shanghai/ Taipei/ Toronto: Oxford University Press.
- Morello, R. (2007). Confidence, Invidia, and Pliny's Epistolary Curriculum. In R. Morello, & A. Morrison, *Ancient Letters: Classical and Late Antique Epistolography* (pp. 169-190). Oxford: Oxford University Press.
- Moroni, B. (2010). I Tristia di Ausonio. Pater ad filium. *Annali Della Facoltà di Lettere E Filosofia*, 75-96.
- Mozley, J. H. (1929). *Ovid: Art of Love. Cosmetics. Remedies for Love. Ibis. Walnut-tree. Sea Fishing. Consolation*. (Revised version by G. P. Goold ed., Vol. 232 Loeb Classical Library). Cambridge (Massachusetts): Harvard University Press.
- Mullen, A., & James, P. (2012). *Multilingualism in the Graeco-Roman Worlds*. Cambridge: Cambridge University Press.
- Munari, F. (1959). *Amores Testo, Indotruzione, Traduzione e Note*. Firenze: La Nuova Italia.
- Mure, W. (1854). *A Critical History of the Language and Literature of Ancient Greece* (Vol. 3). London: Longman, Brown, Green, and Longmans.
- Müri, W. (1976). *Griechische Studien. Ausgewählte Wort- und Sachgeschichtliche Forschungen zur Antike*. Basel: Friedrich Reinhardt.
- Murray, A. T., & Wyatt, W. F. (1924). *Homer: Iliad* (Revised by William F. Wyatt ed., Vol. I: Books 1-12; Loeb Classical Library 170). Cambridge (Massachusetts): Harvard University Press.
- Murray, A. T., & Wyatt, W. F. (1925). *Homer: Iliad* (Revised by William F. Wyatt ed., Vol. II: Books 13-24; Loeb Classical Library 171). Cambridge (Massachusetts): Harvard University Press.
- Murray, A. T., & Wyatt, W. F. (1999). *Homer: Iliad* (Second Edition. Revised by William F. Wyatt ed., Vol. II: Books 13-24; Loeb Classical Library 171). Cambridge (Massachusetts): Harvard University Press.

- Mylonas Shear, I. (1998). Bellerophon Tablets from the Mycenaean World? A Tale of Seven Bronze Hinges. *The Journal of Hellenic Studies* (118), 187–189.
- Nemet-Nejat, K. R. (1998). *Daily Life in Ancient Mesopotamia*. Westport/ London: Greenwood Press.
- Nettleship, H. (1883). The Noctes Atticae of Aulus Gellius. *American Journal of Philology*, 4 (1), 391-415.
- Nicholson, J. (1994). The Delivery and Confidentiality of Cicero's Letters. *The Classical Journal*, 90 (1), 33-63.
- (NIST), U. S. (2001). *Announcing the ADVANCED ENCRYPTION STANDARD (AES)*. Federal Information Processing Standards Publication 197.
- Novokhatko, A. (2015). Greek Scholarship from its Beginning to Alexandria. In: Motanari, F.; Matthaios, S. & Rengakos, A. *Brill's companion to ancient Greek scholarship* (pp. 3-59). Leiden: Brill.
- NSA Picture Gallery Online (2008). Retrieved from: <http://www.nsa.gov/gallery/thumbs/thumb00050.jpg>
- O'Connor, B. (2018). *Bletchley Park and the Pigeon Spies*. Morrisville: Lulu.com. (Online publishing company)
- Oldfather, C. H. (1950). *Diodorus Siculus: Library of History* (Vol. V: Books 12.41-13; Loeb Classical Library 384). Cambridge (Massachusetts): Harvard University Press.
- Oldfather, W. A. (1928). Introduction and Notes. In Illinois Greek Club, *Aeneas Tacticus, Asclepiodotus, Onasander*. (Vol. 156 Loeb Classical Library). Cambridge (Massachusetts): Harvard University Press.
- Oikonomopoulou, K. (2019). Plutarch in Gellius and Apuleius. In: Oikonomopoulou, K. & Xenophontos, S., *Brill's Companion to the Reception of Plutarch* (pp. 37-55). Leiden: Brill.
- Oliensis, E. (2019). *Loving Writing/ Ovid's Amores*. Cambridge (United Kingdom)/ New York: Cambridge University Press.
- Olivetti, L. (2015). *Atlas of Imaging Anatomy*. Springer / Cham / Heidelberg/ New York/ Dordrecht / London: Springer International Publishing Switzerland.
- Oriyano, S.-P. (2013). *Cryptography InfoSec Pro Guide*. New York/ Chicago/ San Francisco/ Athens/ London/ Madrid/ Mexico City/ Milan/ New Delhi/ Singapore/ Sydney/ Toronto: McGraw Hill Education.
- Osborne, R. (2011). *The History Written on the Classical Greek Body*. Cambridge: Cambridge University Press.
- O'Sullivan, N. (1995). Written and Spoken in the First Sophistic. *Mnemosyne*, 157, 115-127.
- O'Toole, J. M. (1991-1992). Herodotus and the Written Record. *Archivaria: The Journal of the Association of Canadian Archivists* (33), 148-160.
- Parke, H.W., & Wormell D. E. W. (1956). *The Delphic Oracle*. 2 vols. Oxford: Blackwell.
- Paton, W., Walbank, F., & Habicht, C. (2011). *Polybius: The Histories* (Vol. Books 9-15; Loeb Classical Library 159). Cambridge (Massachusetts): Harvard University Press.
- Pébarthe, C. (2006). *Cité, Démocratie et Écriture. Histoire de L'Alphabétisation d'Athènes à l'Époque Classique*. (Culture & Cité 3). Paris/Brussels: De Boccard/ Université Libre de Bruxelles, Centre de Recherche sur la Cité Grecque.
- Peek, W. (1974). W. Ein neuer spartanischer Staatsvertrag. *Abhandlungen der Sächsischen Akademie der Wissenschaften zu Leipzig, Philologisch-historische Klasse*, 65, 3–15.
- Pelling, C. (2002). Speech and Action: Herodotus' Debate on the Constitutions. *Proceedings of the Cambridge Philological Society*, 123-158.
- Perkins, E. J. (1953). The Military Staff – Its History and Development. *Military Review*, 33 (6), 81-88.
- Perrin, B. (1914). *Plutarch: Lives* (Vol. I: Theseus and Romulus. Lycurgus and Numa. Solon and Publicola; Loeb Classical Library 46). Cambridge (Massachusetts): Harvard University Press.
- Perrin, B. (1916). *Plutarch: Lives* (Vol. IV: Alcibiades and Coriolanus, Lysander and Sulla; Loeb Classical Library 80). Cambridge (Massachusetts): Harvard University Press.

- Perrin, B. (1917). *Plutarch: Lives* (Vol. V: Agesilaus and Pompey. Pelopidas and Marcellus; Loeb Classical Library 87). Cambridge (Massachusetts): Harvard University Press.
- Perrin, B. (1926). *Plutarch: Lives* (Vol. XI: Aratus. Artaxerxes. Galba. Otho. General Index; Loeb Classical Library 103). Cambridge (Massachusetts): Harvard University Press.
- Piccirilli, L. (1981). Licurgo e Alcandro Monoftalmia e Origine dell' "Agoge" Spartana . *Historia: Zeitschrift für Alte Geschichte*, 30 (1), 1-10.
- Pieprzyk, J., Hardjono, T., & Seberry, J. (2013). *Fundamentals of Computer Security*. Berlin: Springer Science & Business Media.
- Piper, F., & Murphy, S. (2002). *Cryptography: A Very Short Introduction*. Oxford: Oxford University Press.
- Poe, E. A. (1841). A Few Words on Secret Writing. *Graham's Magazine*, 19, 33-38.
- Poe, E. A. (1843) *The Gold-Bug*. Philadelphia: Philadelphia Dollar Newspaper.
- Porter, S. E., & Pitts, A. W. (2013). *Christian Origins and Hellenistic Judaism : Social and Literary Contexts for the New Testament*. Leiden: Brill.
- Poster, C., & Mitchell, L. (2007). *Letter-writing Manuals and Instruction from Antiquity to the Present: Historical and Bibliographic Studies*. Columbia: University of South Carolina Press.
- Powell, A. (2002). *Athens and Sparta: Constructing Greek Political and Social History from 478 BC*. London/ New York: Routledge - An Imprint of Taylor and Francis Group.
- Powell, A. (2017). *A Companion to Sparta*. Hoboken (New Jersey/ Chichester: Wiley Blackwell.
- Powell, B. B. (1997). Homer and Writing. In: Morris, I. & B. B. Powell, *A New Companion to Homer*. Leiden/ New York/ Cologne: Brill, 3-32.
- Pretzler, M. (2010). Polyaeus the Historian? Stratagems and the Use of the Past in the Second Sophistic. In K. Broderson, *Polyaeus. New Studies*. (pp. 85-107). Berlin: Verlag Antike.
- Pretzler, M. (2018-I). Aineias and History: The Purpose and Context of Historical Narrative on the Poliorketika. In M. Pretzler, & N. Barley, *Brill's Companion to Aineias Tacticus* (pp. 68 – 95). Leiden/ Boston: Brill.
- Pretzler, M. (2018-II). The Polis Falling Apart: Aineias Tacticus and Stasis. In M. Pretzler, & N. Barley, *Brill's Companion to Aineias Tacticus* (pp. 146-165). Leiden/ Boston: Brill.
- Pulak, C. (1998). The Uluburun [1] shipwreck: an overview. *The International Journal of Nautical Archaeology*, 27 (3), 188-224.
- Purnamaa, B., & Rohayani, A. H. (2015). A New Modified Caesar Cipher Cryptography Method With Legible. *Procedia Computer Science* 59, 195–204.
- Race, W. H. R. (1997). *Pindar* (Vol. 56 Loeb Classical Library). Cambridge (Massachusetts) Harvard University Press.
- Rago, M. T. & Hosmer, C. (2012). *Data Hiding: Exposing Concealed Data in Multimedia, Operating Systems, Mobile Devices and Network Protocols*. Burlington : Elsevier Science.
- Rance, P. (2018). The Reception of Aineias' Poliorketika in Byzantine military literature. In M. Pretzler, & N. Barley, *Brill's Companion to Aineias Tacticus* (pp. 290-374). Leiden/Boston: Brill.
- Rankov, B. (2007). Military Forces. In P. Sabin, H. Van Wees, & M. Whitby, *The Cambridge History of Greek and Roman Warfare* (Vol. II: Rome from the Late Republic to the Late Empire, pp. 30-75). Cambridge: Cambridge University Press.
- Rawling, L. (2007). *The Ancient Greek at War*. Manchester/ New York: Manchester University Press.
- Rea, J. (1968). Oxyrhynchus Papyri 2660/2660(a). In P. Parsons, J. Rea, & E. Turner, *The Oxyrhynchus Papyri* (Vol. XXXIII, pp. 77-79). London: The Egypt Exploration Society.

- Rea, J. (1970). Oxyrhynchus Papyri 2772: Instructions to a Banker. In R. Coles, D. Foraboschi, A. Soliman El-Mossalamy, J. Rea, & U. Schlag, *The Oxyrhynchus Papyri* (Vol. XXXVI, pp. 63-65). London: The Egypt Exploration Society.
- Reba, M. A., & Shier, D. R. (2015). *Puzzles, Paradoxes, and Problem Solving: An Introduction to Mathematical Thinking*. London/New York/ Boca Raton: CRC Press - An imprint of Taylor and Francis Group.
- Reinke, E. C. (1962). Classical Cryptography. *The Classical Journal*, 58 (3), 113-121.
- Rhodes, P. J. (2014). *Thucydides: History*. Oxford: Oxbow.
- Ribbeck, O. (1962) *Comicorum Romanorum Fragmenta : Praeter Plautum et Terentium*. Hildesheim : Olms.
- Richardson, D. P. (1984-I). *Greek Mythology for Everyone: Legends of the Gods and Heroes*. New York: Avenel Books.
- Richardson, D. P. (1984-II). *Great Zeus and All His Children: Greek Mythology for Adults*. Upper Saddle River: Prentice-Hall.
- Rihll, T. E. (2018). Technology in Aineias Tacticus: Simple and Complex. In M. Pretzler, & N. Barley, *Brill's Companion to Aineias Tacticus* (pp. 265-289). Leiden/Boston: Brill.
- Ritter, T. (1991). Transposition Cipher with Pseudo-random Shuffling: The Dynamic Transposition Combiner. *Cryptologia*, 15 (1), 1-17.
- Rolfe, J. C. (1914). *Suetonius: Lives of the Caesars* (Vol. 31 Loeb Classical Library: I: Julius. Augustus. Tiberius. Gaius. Caligula). Cambridge (Massachusetts): Harvard University Press.
- Rolfe, J. C. (1927). *Aulus Gellius: Attic Nights* (Volume 195: Loeb Classical Library: I: Books 1-5). Cambridge (Massachusetts): Harvard University Press.
- Rolfe, J. C. (1929). *Cornelius Nepos: On Great Generals. On Historians* (Vol. 467 Loeb Classical Library). Cambridge (Massachusetts): Harvard University Press.
- Rolfe, J. C. (1946). *Gellius: Attic Nights* (Vol. III: Books 14-20; Loeb Classical Library 212). Cambridge (Massachusetts): Harvard University Press.
- Rolfe, J. C. (1950). *Ammianus Marcellinus: History* (Vol. I: Books 14-19; Loeb Classical Library 300). Cambridge (Massachusetts): Harvard University Press.
- Rosenmeyer, P. A. (2001). *Ancient Epistolary Fictions: The letter in Greek Literature*. Cambridge/ New York: Cambridge University Press.
- Rösler, W. (2009). Books and Literacy. In G. Boys-Stones, B. Graziosi, & P. Vasunia, *The Oxford handbook of Hellenic studies* (pp. 432-441). Oxford: Oxford University Press.
- Ross, B. D. (2012). Krypteia: A Form of Ancient Guerrilla Warfare. *Grand Valley Journal of History*, 1 (4), 1-10. Retrieved from <http://scholarworks.gvsu.edu/gvjh/vol1/iss2/4>
- Rücker, N. (2012). *Ausonius an Paulinus von Nola: Textgeschichte und Literarische Form der Briefgedichte 21 und 22 des Decimus Magnus Ausonius*. Göttingen: Vandenhoeck & Ruprecht.
- Rundle Clark, R. T. (1959). *Myth and Symbol in Ancient Egypt*. New York: Thames and Hudson.
- Russell, D. A. (1966). On Reading Plutarch's Lives. *Greece & Rome* 13 (2), 139-154.
- Russell, F. S. (1999). *Information Gathering in Classical Greece*. Ann Arbor: University of Michigan Press.
- Saiber, A. (2017). *Measured Words: Computing and Writing in Renaissance Italy*. Toronto: University of Toronto Press.
- Salomon, D. (2003). *Data Privacy and Security: Encryption and Information Hiding*. New York: Springer.
- Salomon, D. (2006). *Coding for Data and Computer Communications*. New York: Springer.
- Saltzman, B. A. (2018). Vt hksdkxt: Early Medieval Cryptography, Textual Errors, and Scribal Agency. *Speculum: A Journal of Medieval Studies* 93 (4), 975-1009.

- Sarri, A. (2017). *Material Aspects of Letter Writing in the Graeco-Roman World : 500 BC - AD 300*. Berlin: De Gruyter.
- Savard, J. (1998/1999). *The Bifid, the Trifid, and the Straddling Checkerboard*. Retrieved from <http://www.quadibloc.com/crypto/pp1322.htm>
- Sbordone, F. (1950). Le Pergamene Vaticane 'De Eligendis Magistratibus'. *La Parola del Passato*, 269-290.
- Schaathun, H. G. (2012). *Machine Learning in Image Steganalysis*. Chichester: John Wiley & Sons Limited.
- Schettino, M. T. (2013). The Use of Historical Sources. In: Beck, M (ed.), *A Companion to Plutarch* (pp. 417-436). Oxford: Blackwell.
- Schmidt, N. (1920). Bellerophon's Tablet and the Homeric Question in the Light of Oriental Research. *Transactions and Proceedings of the American Philological Association* (5), 56-70.
- Schrader, H. (2011). *Leonidas of Sparta: A Peerless Peer*. Tucson: Wheatmark.
- Schwab, G. (2011). *Gods and Heroes of Ancient Greece*. New York: Knopf Doubleday Publishing Group.
- Sebag-Montefiore, H. (2004). *Enigma: The Battle for the Code*. London: Weidenfeld and Nicholson
- An imprint of the Orion Publishing Group Limited.
- Seyfarth, W. (1970). *Ammianus Marcellinus, Römische Geschichte. Lateinisch und Deutsch und mit einem Kommentar versehen von Wolfgang Seyfarth* (Vol. Zweiter Teil - Buch 18-21). Berlin: Akademie-Verlag.
- Shackleton Bailey, D. R. (1980). *Cicero: Select letters*. Cambridge : Cambridge.
- Shackleton Bailey, D. R. (1999). *Cicero: Letters to Atticus* (Vol. I; Loeb Classical Library 7). Cambridge (Massachusetts): Harvard University Press.
- Shackleton Bailey, D. R. (1999). *Cicero: Letters to Atticus* (Vol. II; Loeb Classical Library 8). Cambridge (Massachusetts): Harvard University Press.
- Shackleton Bailey, D. R. (1999). *Cicero: Letters to Atticus* (Vol. III; Loeb Classical Library 97). Cambridge (Massachusetts): Harvard University Press.
- Shackleton Bailey, D. R. (1999). *Cicero: Letters to Atticus* (Vol. IV; Loeb Classical Library 491). Cambridge (Massachusetts): Harvard University Press.
- Shackleton Bailey, D. R. (2001). *Cicero: Letters to Friends* (Vol. I; Loeb Classical Library 205). Cambridge (Massachusetts) : Harvard University Press.
- Shackleton Bailey, D. R. (2001). *Cicero: Letters to Friends* (Vol. II; Loeb Classical Library 216). Cambridge (Massachusetts): Harvard University Press.
- Shackleton Bailey, D. R. (2001). *Cicero: Letters to Friends* (Vol. III; Loeb Classical Library 230). Cambridge (Massachusetts) : Harvard University Press.
- Shackleton Bailey, D. R. (2004). *Cicero : Epistulae ad Quintum fratrem et M. Brutum*. Cambridge/ New York: Cambridge University Press.
- Shackleton Bailey, D. R. (2004). *Cicero's Letters to Atticus*. Vol. 1, 68-59 B.C., [letters] 1-45 (Books I and II). Cambridge: Cambridge University Press.
- Shackleton Bailey, D. R. (2004). *Cicero's Letters to Atticus*. 2, 58-54 B.C., 46-93 (Books III and IV) . Cambridge: Cambridge University Press.
- Shackleton Bailey, D. R. (2004). *Cicero's Letters to Atticus*. 3, 51-50 B.C. 94-132 (books V - VII. 9). Cambridge: Cambridge University Press.
- Shackleton Bailey, D. R. (2004). *Cicero's Letters to Atticus*. 4, 49 B.C. 133-210 (books VII. 10 - X). Cambridge: Cambridge University Press.
- Shackleton Bailey, D. R. (2004). *Cicero's Letters to Atticus*. 5, 48-45 B.C. 211-354 (books XI to XIII) . Cambridge: Cambridge University Press.

- Shackleton Bailey, D. R. (2004). *Cicero's Letters to Atticus*. 6, 44 B.C. 355-426 (books XIV - XVI). Cambridge: Cambridge University Press.
- Shackleton Bailey, D. R. (2004). *Cicero's Letters to Atticus*. 7, Indices to volumes I - VI. Cambridge: Cambridge University Press.
- Shannon, C. (1949). Communication Theory of Secrecy Systems. *Bell System Technical Journal*, 28 (4), 656–715.
- Sheldon, R. M. (1986). Tradecraft in Ancient Greece. *Studies in Intelligence*, 20 (1), 39–47.
- Sheldon, R. M. (1987). *Tinker, Tailor, Caesar, Spy: Espionage in Ancient Rome*. Ann Arbor: UMI Dissertation Information Service.
- Sheldon, R. M. (2005). *Intelligence Activities in Ancient Rome: Trust in the Gods, but Verify*. London/ New York: Routledge.
- Sheldon, R. M. (2008). *Espionage in the Ancient World: An Annotated Bibliography of Books and Articles in Western Languages*. Jefferson/ London: McFarland and Company Incorporated Publishers.
- Shepherd, R. (1793). *Polyænus's Stratagems of War; Translated from the Original Greek, by R. Shepherd, F. R. S*. London: George Nicol.
- Sherwood, A. N. (2006). Papyrus and Parchment. In N. G. Wilson, *Encyclopedia of Ancient Greece* (pp. 535-537). New York/ London: Routledge - An imprint of Taylor and Francis Group.
- Sherwood, A. N., Nikolic, M., Humphrey, J. W., & Oleson, J. P. (2003). *Greek and Roman Technology: A Sourcebook: Annotated Translations of Greek and Latin Texts and Documents*. London/ New York: Routledge.
- Shipley, D. G. (2018). Aineias Tacticus in His Intellectual Context. In M. Pretzler, & N. Barley, *Brill's Companion to Aineias Tacticus* (pp. 49–67). Leiden/ Boston: Brill.
- Shipley, G., (2002). Laconia Survey Inscriptions Catalogue. Retrieved from *The British School at Athens and the Universities of Amsterdam and Nottingham: Laconia Survey Inscriptions*: <http://archive.csad.ox.ac.uk/Laconia/catalogue.html>
- Shipley, G., Cavanagh, W. G., Crouwel, J. H, Crowther, C. & Landuyt, F. (2007). *The Laconia Survey Project*. Retrieved from: ADS Archaeology Data Service: https://archaeologydataservice.ac.uk/archives/view/laconia_ba_2004/
- Sickinger, J. P. (1994). Inscriptions and Archives in Classical Athens. *Historia* 43, 286-296.
- Sickinger, J. P. (2018). *Public records and archives in Classical Athens*. Chapel Hill: University of North Carolina Press.
- Sidebottom, H. (2007). International Relations. In P. Sabin, H. Van Wees, & M. Whitby, *The Cambridge History of Greek and Roman Warfare* (Vol. II: Rome from the Late Republic to the Late Empire, pp. 3-29). Cambridge: Cambridge University Press.
- Sinclair, T. A. (1967). *A History of Greek Political Thought*. London: Routledge.
- Singh, S. (1999). *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography*. London: Fourth Estate.
- Smart, N. (2018). *CyBOK Cryptography Knowledge Area Issue*. London: The National Cyber Security Centre, 1-34.
- Smith, C. F. (1919). *Thucydides: History of the Peloponnesian War* (Vol. I: Books 1-2; Loeb Classical Library 108). Cambridge (Massachusetts): Harvard University Press.
- Smith, L. D. (1955). *Cryptography: The Science of Secret Writing: History and Modern Use of Codes and Ciphers, together with 151 Problems and their Solutions*. Mineola: Courier Corporation: Business and Economics/Dover Publications.
- Soares, C. (2007). Rules for a good description: theory and practice in the " Life of Artaxerxes" (§§ 1-19). *Hermathena*, 182, 85-100.

- Sommerstein, A. H. (1987). *Aristophanes Birds*. Wiltshire: Aris & Phillips Limited.
- Sommerstein, A. H. (1990). *Aristophanes Lysistrata*. Wiltshire: Aris & Phillips Limited.
- Sommerstein, A. H. (2002). *The Comedies of Aristophanes: 12: Indexes*. Warminster : Aris & Philips
- Sommerstein, A. H. (2008). *Aeschylus: Oresteia: Agamemnon. Libation-Bearers. Eumenides*. (Vol. 146 Loeb Classical Library). Cambridge (Massachusetts): Harvard University Press.
- Sosin, J. D. (2018). '*Scytale (σκυτάλη)*' (I). Retrieved from Photius Online, Ongoing English Translation of the Lexicon: https://dctthree.github.io/photios/entry#urn_cts_greekLit_tlg4040_lexicon_dc3_%CF%83_389
- Sosin, J. D. (2018). '*Scytale (σκυτάλη)*' (II). Retrieved from Photius Online, Ongoing English Translation of the Lexicon: https://dctthree.github.io/photios/entry#urn_cts_greekLit_tlg4040_lexicon_dc3_%CF%83_390
- Spar, I., & Jursa, M. (2014). *Cuneiform Texts in The Metropolitan Museum of Art Volume IV: The Ebabbar Temple Archive and Other Texts from the Fourth to the First Millenium B.C*. New York/ Indiana: The Metropolitan Museum of Art/ Eisenbrauns Incorporated.
- Spence, I. G. (2010). *The A to Z of Ancient Greek Warfare* (Vol. The A to Z Guide Series, No. 199). Lanham/ Toronto/ Plymouth: The Scarecrow Press Incorporation.
- Stamp, M. & Low, R. M. (2007). *Applied Cryptanalysis: Breaking Ciphers in the Real World*. San Jose: Wiley Interscience.
- Steiner, D. T. (1994). *The Tyrant's Writ: Myths and Images of Writing in Ancient Greece*. Princeton: Princeton University Press.
- Stewart, J., Chapple, M., & Gibson, D. (2012). *CISSP: Certified Information Systems Security Professional Study Guide*. Hoboken: John Wiley and Sons Incorporation.
- Stinson, D. R. (1995). *Cryptography: theory and practice*. Boca Raton/ New York/ Washington D.C.: CRC Press.
- Stinson, D. R. (2002). *Cryptography: Theory and Practice. Second edition*. Boca Raton/ London/ New York/ Washington D.C.: Chapman and Hall - An imprint of CRC Press Company.
- Storey, I. C. (2011-I). *Fragments of Old Comedy* (Vol. II: Diopieithes to Pherecrates; Loeb Classical Library 514). (I. C. Storey, Ed.) Cambridge (Massachusetts): Harvard University Press.
- Storey, I. C. (2011-II). *Fragments of Old Comedy* (Vol. III: Philonicus to Xenophon. Adespota; Loeb Classical Library 515). (I. C. Storey, Ed.) Cambridge (Massachusetts): Harvard University Press.
- Strasser, G. F. (2007). The Rise of Cryptology in the European Renaissance. In K. De Leeuw, & J. A. Bergstra, *The History of Information Security: A Comprehensive Handbook* (pp. 277-325). Amsterdam/ Boston/ Heidelberg/ London/ New York/ Oxford/ Paris/ San Diego/ San Francisco/ Singapore/ Sydney/ Tokyo: Elsevier.
- Street, B. V. (1984). *Literacy in Theory and Practice*. Cambridge: Cambridge University Press.
- Stylianou, P. J. (2013). Ephorus. In N. Wilson, *Encyclopedia of Ancient Greece* (pp. 262-263). New York/ London: dgde - An Imprint of Taylor and Francis Group.
- Swift, L. (2019). *Archilochus: The Poems. Introduction, Text, Translation, and Commentary*. Oxford: Oxford University Press.
- Swiggers, P. (1996). Transmission of the Phoenician Script to the West. In P. Daniels, & W. Bright, *The World's Writing Systems* (pp. 261-270). Oxford: Oxford University Press.
- Szedegy-Maszak, A. (1981). *The Nomoi of Theophrastus*. New York: Arno Press.
- Thévenot, M., Boivin, J., & de La Hire, P. (1693). *Veterum Mathematicorum Athenæi, Apollodori, Philonis, Bitonis, Heronis, et Aliorum Opera : Græce et Latine pleraque nunc primum edita. Ex Manuscriptis Codicibus Bibliothecæ Regiæ*. Paris: Ex Typographia Regia.
- Thomas, C. G. (1995). Wingy Mysteries in Divinity. *Mnemosyne*, 157, 179-194.

- Thomas, R. (1989). *Oral Tradition and Written Record in Classical Athens*. Cambridge: Cambridge University Press.
- Thomas, R. (2002). *Herodotus in Context: Ethnography, Science and the Art of Persuasion*. Cambridge/ New York: Cambridge University Press.
- Thomas, R. (2009). Writing, Reading, Public and Private “Literacies”. In W. Johnson, & H. Parker, *Ancient Literacies: The Culture of Reading in Greece and Rome* (pp. 13-45). Oxford: Oxford University Press.
- Tigerstedt, E. N. (1965). *The Legend of Sparta in Classical Antiquity*. Stockholm : Almqvist & Wiksell.
- Tod, M. N. 1933. *A Selection of Greek Historical Inscriptions*. Oxford: Clarendon Press.
- Too, L. (2001). *Education in Greek and Roman Antiquity*. Leiden/Boston : Brill.
- Toustain, C., & Tassin, R. (1750). *Nouveau Traité de Diplomatie, par Deux Religieux Bénédictins de la Congrégation de s. Maur R.P. Tassin, C.F. Toustain et J.B. Baussonnet*. Paris: G. Desprez & P.-G. Cavelier.
- Trapp, M. (2003). *Greek and Latin Letters: An Anthology with Translation*. Cambridge: Cambridge University Press.
- Trendall, A. D. (1952) Paestan Pottery: A revision and a supplement, in: *Proceedings of the British School in Rome*, 52, 1-53.
- Trout, D. E. (1999). *Paulinus of Nola: Life, Letters, and Poems*. Berkeley: University of California Press.
- Turner, E. G. (1952). *Athenian Books in the Fifth and Fourth Centuries B.C*. London: H. K. Lewis.
- Turner, E. G. (1973). *The papyrologist at work*. Durham (North Carolina): Duke University.
- Usher, S. (1970). Review: Reviewed Work(s): Poliorcétique by Aeneas Tacticus, A. Dain and A.-M. Bon. *The Journal of Hellenic Studies*, 90, 210-211.
- Van Oldenburg Ermke, F. (1959). *Homeros: Ilias en Odyssea*. Retie: Kempische Boekhandel.
- Van Tilborg, H. C. (2006). *Fundamentals of Cryptology: A Professional Reference and Interactive Tutorial by Henk C. A. van Tilborg, Eindhoven University of Technology, The Netherlands* (2 ed.). Boston/ Dordrecht/ London: Kluwer Academic Publishers.
- Vela Tejada, J. (1991). *Estudio sobre la Lengua de la Poliorcética de Eneas el Tactico*. Zaragoza: Departamento de Ciencias de la Antigüedad de la Universidad Zaragoza.
- Vela Tejada, J. (2004). Warfare, History and Literature in the Archaic and Classical Periods: The Development of Greek Military Treatises. *Historia: Zeitschrift für Alte Geschichte*, 53 (2), 129-146.
- Vela Tejada, J., & Martín García, F. (1991). *Eneas el Táctico: Poliorcética. Polieno, Estratagemas*. Madrid: Gedros.
- Verdegem, S. (2010). *Plutarch's Life of Alcibiades: Story, Text and Moralism*. Leuven: Leuven University Press.
- Von Gutschmid, H. A. (1880). Review of Hug: A. Hug, Aeneas von Stymphalos: Ein Arkadischer Schriftsteller aus Klassischer Zeit. *Literarisches Zentralblatt* 1880, 588-590.
- Von Fritz, K. (1941). Theopompus the Historian. *The American Historical Review*, 46, 765-787.
- Waldstein, M., & Wisse, F. (1995). *The Apocryphon of John: Synopsis of Nag Hammadi Codices II, 1, III, 1, and IV, 1, with BG 8502, 2*. Leiden: Brill.
- Walker, C. H. (2008). Document security in the Ancient World. In M. Quigley, *Encyclopedia of Information Ethics and Security* (pp. 150-156). Hershey/ London: IGI Global.
- Wallace, R. E. (2015). Language, Alphabet, and Linguistic Affiliation. In S. Bell, & A. Carpino, *A Companion to the Etruscans* (pp. 203-224). Chichester: Wiley Blackwell.
- Warner, R., & Cawkwell, G. (1979). *A History of my Times (Hellenica)*. London: Penguin.

- Waters, K. H. (1972). Herodotos and Politics. *Greece & Rome*, 19 (2), 136-150.
- Waters, K. H. (1985). *Herodotus the Historian: His Problems, Methods and Originality*. London: Croom Helm.
- Watson, J. S. (1853 (Digitalised 2003)). *Marcus Junianus Justinus: Epitome of the Philippic History of Pompeius Trogus*. (D. Camden, Editor) Retrieved from Corpus Scriptorum Latinorum: A Digital Library of Latin Literature: <http://www.forumromanum.org/literature/justin/english/trans2.html#10>
- Watson, J. S. (1866 (Digitalised in 2003)). *Cornelius Nepos: Lives of Eminent Commanders, translated, with notes, by the Reverend John Selby Watson*. (R. Pearse, Editor) Retrieved from Early Church Fathers - Additional Texts: <http://www.tertullian.org/fathers/nepos.htm>
- Way, A. G. (1955). *Caesar: Alexandrian War. African War. Spanish War*. (Vol. 402 Loeb Classical Library). Cambridge (Massachusetts): Harvard University Press.
- Welskopf, E. A. (1974). *Hellenische Poleis: Krise, Wandlung, Wirkung* (Vol. 4). Darmstadt: Wissenschaftliche Buchgesellschaft.
- West, S. (1998). Archilochus' Message Stick. *Classical Quarterly*, 38, 42-48.
- White, J. W. (1914). *The Scholia on the Aves of Aristophanes with an Introduction on the Origin, Development, Transmission, and Extant Sources of the Old Greek Commentary on his Comedies*. Hildesheim/ New York: Georg Olms Verlag.
- White, P. (2010). *Cicero in Letters: Epistolary Relations of the Late Republic*. New York: Oxford University Press.
- Whitehead, D. (1990). *Aeneas the Tactician: How to Survive Under Siege*. Oxford: Clarendon Press.
- Whitiak, D. A. (2003). *The Art of Steganography* (Global Information Assurance Certification Paper, SANS Institute 2003 - Part of GIAC practical repository ed.). Retrieved from <http://www.giac.org/paper/gsec/2944/art-steganography/104>
- Whittaker, C. R. (1970). *Herodian: History of the Empire* (Vol. II: Books 5-8; Loeb Classical Library 455). Cambridge (Massachusetts): Harvard University Press.
- Williams, K., March, L., & Wassell, S. R. (2010). *The Mathematical Works of Leon Battista Alberti*. Basel: Birkhäuser.
- Williams, T. H. (1904). The Authorship of the Greek Military Manual attributed to 'Aeneas Tacticus'. *American Journal of Philology*, 25 (4), 390-405.
- Willock, M. M. (1978). *The Iliad of Homer*. London: Macmillan Education.
- Winterling, A. (1991). Polisbegriff und Stasistheorie des Aeneas Tacticus. Zur Frage der Grenzen der Griechischen Polisgesellschaften im 4. Jahrhundert vor Christus. *Historia: Zeitschrift für Alte Geschichte*, 40 (2), 193-229.
- Wisse, F. (1979). Language Mysticism in the Nag Hammadi Texts and in Early Coptic Monasticism I: Cryptography. *Enchoria: Zeitschrift für Demotistik und Koptologie*, 9, 101-120.
- Wisse, F. (1980). Textual Restorations in On The Origin of the World. *The Bulletin of the American Society of Papyrologists*, 17 (1-2), 87-91.
- Wisse, F. (1981). The Opponents in the New Testament in light of the Nag Hammadi Writing. In B. Barc (Ed.), *Colloque international sur les textes de Nag Hammadi : Québec, 22-25 août 1978* (pp. 99-120). Québec/ Louvain: Presses de l'Université Laval/ Editions Peeters.
- Wisse, F. (1982). *The Profile Method for the Classification and Evaluation of Manuscript Evidence, as applied to the continuous Greek text of the Gospel of Luke*. Grand Rapids: Eerdmans.
- Wisse, F. (1983). Prolegomena to the study of the New Testament and Gnosis. In A. Logan, & A. Weddeburn, *The New Testament and gnosis : essays in honour of Robert McL. Wilson* (pp. 138-145). Edinburgh: T. & T. Clark.

- Wisse, F. (1989). The Nature and Purpose of Redactional Changes in Early Christian Texts: The Canonical Gospels. In W. Petersen, *Gospel Traditions in the Second Century: Origins, Recensions, Text, and Transmission* (pp. 39-53). Notre Dame: University of Notre Dame Press.
- Wisse, F. (1990). Pseudo-Liberius, Oratio Consolitaria de morte Athanasii. *Le Muséon*, 103 (1-2), 43-65.
- Wolicki, A. (2018). *Spartan symmarchy in the sixth and fifth centuries BCE*. Warsaw: Wydawnictwa Uniwersytetu Warszawskiego.
- Woodard, R., & Scott, D. (2014). *The Textualization of the Greek Alphabet*. Cambridge: Cambridge University Press.
- Woolliscroft, D. I. (2001). *Roman Military Signalling*. Stroud: Tempus.
- Wouters, A. (1976). “Latijns Grieks” en “Grieks Latijn”, over Translitteraties en hun Bedoeling. *Hermeneus Tijdschrift voor Antieke Cultuur*, 48 (4), 179-191.
- Youtie, H. C. (1971). Βραδέως γράφων: Between Literacy and Illiteracy. *Greek, Roman, and Byzantine Studies*, 12 (2), 239-261.
- Zapechnikov, S., Tolstoy, A., & Nagibi, S. (2015). History of Cryptography in Syllabus on Information Security Training. *9th IFIP World Conference on Information Security Education (WISE)* (pp. 146-157). Berlin/Heidelberg: Springer-Verlag.

List of translations and commentaries

The following list provides an overview of Greek and Latin translations and commentaries used for this work – including in this appendix. Most works come from the LOEB Classical Library Series. Translations of text in the thesis come from this series unless otherwise indicated. Full bibliographical details of all consulted works can be found in the bibliography.

	<i>Dissoi Logoi</i>	Laks and Most (2016)
	<i>Sylloge Tacticorum</i>	Charzelis and Harris (2017)
Aeneas Tacticus	<i>How to Survive Under Siege</i>	Barends (1955); Hug (1877); Hunter and Handford (1927); Illinois Greek Club (1928); Whitehead (1990).
Aeschylus	<i>Agamemnon</i>	Sommerstein (2008)
Alberti	<i>De Componendis Cifris</i>	Williams, March et al. (2010)
Ammianus	<i>Roman History</i>	Rolfe (1950); Seyfarth (1970)
Apollodorus	<i>The Library</i>	Frazer (1921)
Archilochus of Paros	<i>Fragment 185</i>	Gerber (1999); Swift (2019)
Aristarchus	<i>Scholia to the Iliad</i>	Schmidt (1920); Erbse (1971)
Aristophanes	<i>Birds</i>	Henderson (2000); Sommerstein (1987)
	<i>Lysistrata</i>	Henderson (2001); Sommerstein (1990)
Athenaeus	<i>The Learned Banqueters</i>	Douglas Olson (2009)
Aulus Gellius	<i>Attic Nights</i>	Rolfe (1946); Holford-Strevens (2019-I; 2019-II)
Ausonius	<i>Epistles</i>	Evelyn-White (1921)
Cardano	<i>De Subtilitate</i>	Forrester and Henry (2013)

Caesar	<i>The Alexandrian War</i>	Way (1955)
	<i>The African War</i>	Way (1955)
	<i>The Civil War</i>	Damon (2016)
	<i>The Gallic War</i>	Edwards (1917)
	<i>The Spanish War</i>	Way (1955)
Cassius Dio	<i>Roman History</i>	Cary and Foster (1914)
Cicero	<i>Letters to Atticus</i>	Shackleton Bailey (1999; all)
Cornelius Nepos	<i>On Great Generals</i>	Rolfe (1929); Watson (1866)
Diodorus Siculus	<i>Library of History</i>	Oldfather (1950)
Frontinus	<i>Stratagems</i>	Bennett and McElwain (1925)
Herodian	<i>History of the Empire</i>	Whittaker (1970)
Herodotus	<i>Histories</i>	Godley (1920; 1922; 1925);
		Holland and Cartledge (2013)
Homer	<i>Iliad</i>	Murray and Wyatt (1924; 1925; 1999)
Isidore of Seville	<i>The Etymologies</i>	Barley, Lewis et.al (2006)
Julius Africanus	<i>Kestoi</i>	Illinois Greek Club (1928)
Justin	<i>Philippic History</i>	Watson (1853)
Nicophon	<i>The Birth of Aphrodite</i>	Edmonds (1957); Kassel and Austin
		(1989); Storey (2011: I & II)
Ovid	<i>Amores</i>	Goold (1977); Jestin and Katz (2000)
	<i>Heroides</i>	Goold (1977); Jacobson (1974)
	<i>Ars Amatoria</i>	Mozley (1929)
Philo of Byzantium	<i>Compendium of Mechanics</i>	<i>Veterum Mathematicorum Opera</i> ;
		Author's translation
Photius	<i>Lexicon</i>	Sosin (2018: I & II)
Pindar	<i>Olympian Odes</i>	Race (1997)

Plato	<i>Greater Hippias</i>	Fowler (1926)
Pliny the Elder	<i>Natural History</i>	Jones and Andrews (1980)
Plutarch	<i>Life of Agesilaus</i>	Perrin (1916)
	<i>Life of Alcibiades</i>	Perrin (1917)
	<i>Life of Artaxerxes</i>	Forster Smith (2010); Perrin (1926)
	<i>Life of Lysander</i>	Flaceliere and Chambry (1971); Perrin (1917)
	<i>Moralia: Ancient Customs of the Spartans</i>	Babbitt (1931)
Polyaenus	<i>Stratagems of War</i>	Shepherd (1793); Krentz and Wheeler (1994)
Polybius	<i>The Histories</i>	Paton, Walbank et al. (2011)
Porphry of Tyre	<i>Life of Pythagoras</i>	Guthrie (1987)
Procopius	<i>Secret History</i>	Dewing (1935)
Suetonius	<i>Lives of Julius Caesar</i>	Rolfe (1914)
	<i>Lives of Augustus</i>	Rolfe (1914)
Theophrastus	<i>Nomoi</i>	<i>Biblioteca Apostolica Vaticana</i> ; 2306;
		Aly (1943); Sbordone (1950); Keaney (1974); Szedegy-Maszak (1981)
Thucydides	<i>The Peloponnesian War</i>	Gomme, Andrewes & Dover (1981);
		Hammond (2009); Hornblower (1996; 2010); Lattimore (1998); Rhodes (2014); Smith (1919)
Xenophon	<i>Cyropaedia</i>	Miller (1914)
	<i>Hellenica</i>	Brownson (1918; 1921); Warner & Cawkwell (1979)

Appendix 1: Greco-Roman sources on cryptography and steganography

The following is an alphabetic overview of Greco-Roman sources on cryptography and steganography.

1: Aeneas Tacticus (*How to Survive under Siege*, ca. 360 BCE)

Περὶ δὲ ἐπιστολῶν κρυφαίων παντοία μὲν εἰσιν αἱ πέμψεις, προσυγκεῖσθαι δὲ δεῖ τῷ πέμψαντι καὶ δεχομένῳ ἰδίᾳ· αἱ δὲ λανθάνουσι μάλιστα τοιαῖδε ἂν εἶεν (Aeneas Tacticus, *How to Survive Under Siege*, 31.1)

In regard to secret messages, there are all sorts of ways of sending them, but a private arrangement must be previously made between the sender and the receiver.

ἐπέμφθη ἐπιστολὴ ὧδε. εἰς φορτία ἢ ἄλλα σκευὴ ἐνεβλήθη βυβλίον ἢ ἄλλο τι γράμμα τὸ τυχὸν καὶ μεγέθει καὶ παλαιότητι. ἐν τούτῳ δὲ γέγραπται ἡ ἐπιστολὴ ἐπιστιζομένων γραμμάτων τοῦ πρώτου στίχου ἢ δευτέρου ἢ τρίτου, ἐπιστιγμαῖς δὲ ἐλαχίσταις καὶ ἀδηλοτάταις πλὴν τῷ πεμπομένῳ. εἴτα ἀφικομένου τοῦ βιβλίου παρ' ὃν δεῖ, ἐξεγράφετο καὶ τὰ ἐπισεσημασμένα γράμματα τιθεὶς ἐφεξῆς τὰ ἐκ τῷ πρώτου στίχου καὶ δευτέρου καὶ τὰ ἄλλα ὡσαύτως, ἐγνώριζε τὰ ἐπισταλέντα. ὀλίγα δ' ἂν τις θέλων ἐπιστεῖλαι καὶ ὧδε ποιῆσαι, παρόμοιον τούτῳ. ἐπιστολὴν γράψαντα περὶ τινων φανερώς ἐν πλείοσιν, ἐν ταύτῃ τῇ ἐπιστολῇ τὸ αὐτὸ ποιεῖν ἐπισημαινόμενον γράμματα, δι' ὧτων ἐμφανεῖς ἅπερ ἂν βούλῃ. τὴν δὲ ἐπισημασίαν εἶναι ὡς ἀδηλοτάτην ἐπιστιγμαῖς διὰ πολλοῦ ἢ γραμμαῖς παραμήκεσιν. ἃ τοῖς μὲν ἄλλοις μηδεμίαν ὑπόνοιαν ἔξει, τῷ δὲ πεμπομένῳ γνωστὴ ἔσται ἡ ἐπιστολή (Aeneas Tacticus, *How to Survive Under Siege*, 31.1-3)

In one case a message was sent in this way: in with merchandise or other baggage there was inserted a book, or some other chance document, of any size or age, and in this the message had been written by marking the letters of the first, second, or third line with dots, very small and discernible only to the recipient. Then, when the person intended received the book, he made a transcript, and by setting down in order the marked letters from the first line and the second and the others in the same way he discovered the message. But should anyone wish to send a brief message, he might use also the following method, which is similar to the preceding. Writing in detail and undisguisedly on some subject, in this message you may reach the same result by marking letters by which you will indicate whatever you may wish. And the marking must be made as inconspicuous as possible, by dots placed far apart or by rather long dashes. These will arouse no suspicion whatsoever in others, but the letter will be clear to the recipient.

πεμπέσθω ἀνὴρ ἀγγελίαν φέρων τινὰ ἢ καὶ ἐπιστολὴν περὶ ἄλλων φανερῶν· τοῦ δὲ μέλλοντος πορεύεσθαι κρυφαίως αὐτοῦ εἰς τὸ τῶν ὑποδημάτων πέλμα ἐντεθήτω εἷς τὸ μεταξὺ βυβλίον καὶ καταρραπτέσθω, πρὸς δὲ τοὺς πηλοὺς καὶ τὰ ὕδατα εἰς κασσίτερον ἐληλασμένον λεπτὸν γραφέσθω πρὸς τὸ μὴ ἀφανίζεσθαι ὑπὸ τῶν ὑδάτων τὰ γράμματα. ἀφικομένου δὲ παρ' ὃν δεῖ, καὶ ἀναπαυομένου

ἐν τῇ νυκτί, ἀναλυέτω τὰς ῥαφὰς τῶν ὑποδημάτων, καὶ ἐξελὼν καὶ ἀναγνούς, ἄλλα γράψας λάθρᾳ ἔτι καθεύδοντος καὶ ἐγκαταρράψας ἀποστελλέτω τὸν ἄνδρα, ἀνταγγείας ἢ καὶ δούς τι φέρειν φανερώς. οὕτως οὖν οὔτε ἄλλος οὔτε ὁ φέρων εἰδήσει· χρὴ δὲ τὰς ῥαφὰς τῶν ὑποδημάτων ὡς ἀδηλοτάτας ποιεῖν (Aeneas Tacticus, *How to Survive Under Siege*, 31.4-5)

Let a man be sent bearing some message or even a letter ostensibly about general matters, not secret, and, just before he starts, without his knowledge let a letter be inserted in the sole of his sandals and be sewed in, and, to guard against mud and water, have it written on a piece of thin-beaten tin, so that the writing will not be effaced by the water. And when he reaches the one intended and goes to rest for the night, this person should pull out the stitchings of the sandals, take out and read the letter, and, writing another secretly while the man is still asleep, sew it in and send him back, having given him some message in reply or even something to carry openly. In this way, then, neither the messenger nor anyone else will know the message. It is necessary, however, to make the sewings of the sandals as inconspicuous as possible.

Εἰ Ἐφεσον [...] εἰσεκομίσθη γράμματα τῷ τρόπῳ τοιῷδε. ἄνθρωπος ἐπέμφθη ἐπιστολὴν ἔχων φύλλοις ἐγγεγραμμένην, τὰ δὲ φύλλα ἐφ' ἑλκει καταδεδεμένα ἦν ἐπὶ κνήμην (Aeneas Tacticus, *How to Survive Under Siege*, 31.6)

A letter was brought to Ephesus in some such manner as this: a man was sent with a message written on leaves which were bound to a wound on his leg.

εἰσενεχθεῖν δ' ἂν γραφὴ καὶ ἐν τοῖς τῶν γυναικῶν ὥσιν ἔχουσιν ἀντ' ἐνωτίων ἐλασμοὺς ἐνειλημένους λεπτοὺς μολιβδίνους (Aeneas Tacticus, *How to Survive Under Siege*, 31.7)

Writing could be brought in also on thin pieces of beaten lead rolled up and worn in women's ears in place of ear-rings.

ἐκομίσθη δὲ ἐπιστολὴ περὶ προδοσίας εἰς στρατόπεδον ἀντικαθημένων πολέμιων ὑπὸ τοῦ προδιδόντος ὧδε. τῶν ἐξιόντων ἱππέων ἐκ τῆς πόλεως εἰς προνομὴν τῶν πολέμιων ἐνὶ ἐγκατερράφῃ ὑπὸ τὰ πετερίγια τοῦ θώρακος βιβλίον· ᾧ ἐντέταλτο, εἴαν τις ἐπιφάνεια τῶν πολέμιων γένηται, πεσεῖν ἀπὸ τοῦ ἵππου ὡς ἄκοντα καὶ ζωγρηθῆναι. καὶ γενομένου δ' ἐν τῷ στρατοπέδῳ ἀποδοθῆναι τὸ βιβλίον ᾧ ἔδει. ὑπηρέτησεν δ' ὁ ἱππεὺς ἀδελφὸς ἀδελφῷ (Aeneas Tacticus, *How to Survive Under Siege*, 31.8)

A letter having to do with betrayal was once conveyed by the traitor to the camp of the beleaguering enemy in this way. As the horsemen were going out of the city for a raid upon the enemy one of them had a sheet of papyrus sewn under the flaps of his breastplate, and he was instructed, if the enemy should appear, to fall from his horse as though by accident, and to be captured alive; and when he was taken into camp he was to give the sheet of writing to the proper person. The horseman assisted as a brother would a brother.

ἄλλος δὲ ἰππέα ἐκπέμπων εἰς τὴν ἡνίαν τοῦ χαλινοῦ βυβλίον ἐνέρραψεν. ἐγένετο δὲ περὶ ἐπιστολὴν τοιόνδε. πόλεως γὰρ πολιορκουμένης ἐπεὶ παρήλθεν ἔσω τῆς πόλεως ὁ κομίζων τὰς ἐπιστολάς τῳ μὲν προδιδόντι καὶ τοῖς ἄλλοις οἷς ἔφερεν οὐκ ἀποδίδωσιν, πρὸς δὲ τὸν ἄρχοντα τῆς πόλεως ἦλθεν μηνύων καὶ τὰς ἐπιστολάς ἐδίδου. ὁ δ' ἀκούσας ἐκέλευεν ταύτας μὲν τὰς ἐπιστολάς οἷς ἔφερεν ἀποδοῦναι, τὰ δὲ παρ' ἐκείνων, εἰ ἀληθές τι μηνύει, παρ' αὐτὸν ἐνεγκεῖν· καὶ ὁ μηνύων ταῦτα ἔπραξεν. ὁ δὲ ἄρχων λαβὼν τὰς ἐπιστολάς καὶ ἀνακαλεσάμενος τοὺς ἀνθρώπους τὰ σημεῖα τε ἐδείκνυνεν τῶν δακτυλίων, ἅπερ ὁμολόγουν αὐτῶν εἶναι, καὶ λύων τὰ βιβλία ἐδήλου τὸ πρᾶγμα. τεχνικῶς δὲ δοκεῖ φωρᾶσαι, ὅτι τὰς πεμπομένας παρὰ τοῦ ἀνθρώπου οὐκ ἀπέλαβεν· ἦν γὰρ αὐτοῖς ἀρνηθῆναι καὶ φάσκειν ἐπιβουλεύεσθαι ὑπὸ τινος. τὰς δ' ἀνταποστελλομένας λαβὼν ἀναντιλέκτως ἤλεγξεν (Aeneas Tacticus, *How to Survive Under Siege*, 31.9-9b)

Another man, when sending out a horseman, sewed a sheet of papyrus to the bridle-rein. And the following incident happened about a letter. During the siege of a city, when the man carrying the message entered the town, he did not give the letters to the traitor and to the others to whom he was bringing it, but went to the commanding officer of the city, disclosed the matter, and handed over the letters. When the officer heard it, he ordered him to deliver these letters to those to whom he was bringing them, but to bring to him their answer as evidence that he was telling the truth. The informer did so, and the officer, taking the letters, called the men to him, showed them the marks of the seals which they admitted to be their own, and, opening the letters, exposed the matter. And he seems to have detected this skilfully in that he did not accept from the man the letters that were sent. For then it would have been possible for the men to deny it and claim that someone was plotting against them. But by taking the letters that were sent in answer he proved the case incontestably.

Κομίζεται δὲ καὶ ὧδε. κύστιν ἰσομεγέθη ληκύθῳ ὁπόσῃ ἂν βούλῃ πρὸς τὸ πλῆθος τῶν γραφησομένων φυσήσαντα καὶ ἀποδήσαντα σφόδρα ξηρᾶναι, ἔπειτα ἐπ' αὐτῆς γράψαι ὅ τι ἂν βούλῃ μέλανι κατακόλλῳ. ξηρανθέντων δὲ τῶν γραμμάτων ἐξελεῖν τὴν πνοὴν τῆς κύστιδος καὶ συμπίεσαντα εἰς τὴν λήκυθον ἐνθεῖναι· τὸ δὲ στόμα τῆς κύστιδος ὑπερέχτω τοῦ στόματος τῆς ληκύθου. ἔπειτα φυσήσαντα τὴν κύστιν ἐν τῇ ληκύθῳ ἐνοῦσαν, ἵνα διευρυνθῇ ὡς μάλιστα, καὶ ἐλαίου ἐμπλήσαντα περιτεμεῖν τῆς κύστιδος τὸ ὑπερέχον τῆς ληκύθου καὶ προσαρμόσαι τῷ στόματι ὡς ἀδηλότατα, καὶ βύσαντα τὴν λήκυθον κομίζειν φανερώς. διαφανές τε οὖν τὸ ἔλαιον ἔσται ἐν τῇ ληκύθῳ καὶ οὐδὲν ἄλλο φανεῖται ἐνόν. ὅταν δὲ ἔλθῃ παρ' ὃν δεῖ, ἐξεράσας τὸ ἔλαιον ἀναγνώσεται φυσήσας τὴν κύστιν· καὶ ἐκπογγίσας καὶ κατὰ ταῦτα εἰς τὴν αὐτὴν γράψας ἀποστελλέτω (Aeneas Tacticus, *How to Survive Under Siege*, 31.10-13)

Messages are sent also in this way. Take a bladder in size equal to a flask large enough for your purpose; inflate it, tie it tightly, and let it dry; then write on it whatever you wish, in ink mixed with glue. When the writing is dry, let the air out of the bladder, and press it into the flask, letting the mouth of the bladder protrude from the mouth of the flask. Then inflate the bladder inside the flask in order to expand it as much as possible, and filling it with oil, cut off the part of the bladder that comes over the top of the flask, fitting it in the mouth as inconspicuously as you can, and, corking the bottle, carry it openly. Hence the oil will be visible in the flask, but nothing else. When it comes to the appropriate person, he will pour

out the oil, inflate the bladder, and read the writing. And washing it off with a sponge, let him write on it in the same manner and send it back.

ἤδη δέ τις ἐν δέλτου ξύλῳ γράψας κηρὸν ἐπέτηξεν καὶ ἄλλα εἰς τὸν κηρὸν ἐνέγραψεν. εἶτα ὅταν ἔλθῃ παρ' ὃν ἔδει, ἐκκνήσας τὸν κηρὸν καὶ ἀναγνοὺς γράψας πάλιν ὡσαύτως ἐπέστειλεν. ἐνδέχεται δὲ καὶ εἰς πυξίον γράψαντα μέλανι ὡς βελτίστῳ ἔαν ξηρανθῆναι, ἔπειτα λευκώσαντα ἀφανίζειν τὰ γράμματα. ὅταν οὖν ἀφίκηται παρὰ τὸν πεμπόμενον, λαβόντα εἰς ὕδωρ θεῖναι τὸ πυξίον· φανεῖται οὖν ἐν τῷ ὕδατι ἀκριβῶς ἅπαντα τὰ γεγραμμένα. (Aeneas Tacticus, *How to Survive Under Siege*, 31.14)

It has actually happened that someone has written on the wooden part of a tablet, poured wax over it, and written something else on the wax. Then when it came to the appointed person, he, scraping off the wax and reading the writing, again in this way has sent back a message.

φανεῖται οὖν ἐν τῷ ὕδατι ἀκριβῶς ἅπαντα τὰ γεγραμμένα. γράφοιτο δ' ἂν καὶ εἰς πινάκιον ἡρωϊκὸν^δ ἅπερ ἂν βούλῃ. ἔπειτα καταλευκῶσαι καὶ ξηράναντα γράψαι ἱππέα φωσφόρον ἢ ὅ τι ἂν βούλῃ, ἔχοντα ἱματισμὸν λευκὸν καὶ τὸν ἵππον λευκόν· εἰ δὲ μή, καὶ ἄλλῳ χρώματι, πλὴν μέλανος. ἔπειτα δοῦναι τινὶ ἀναθεῖναι ἐγγὺς τῆς πόλεως εἰς ὃ ἂν τύχῃ ἱερὸν ὡς εὐξάμενος. ὃν δὲ δεῖ ἀναγνῶναι τὰ γεγραμμένα, χρὴ ἐλθόντα εἰς τὸ ἱερὸν καὶ γνόντα τὸ πινάκιον συσσήμῳ τινὶ προσυγκειμένῳ, ἀπενέγκαντα εἰς οἶκον θεῖναι εἰς ἔλαιον· πάντα οὖν τὰ γεγραμμένα φανεῖται (Aeneas Tacticus, *How to Survive Under Siege*, 31.14-16)

It would be possible, also, to write on a boxwood tablet with the best quality of ink, let it dry, and then by whitening the tablet to make the letters invisible. When, then, the tablet comes to the recipient, he should take it and put it into water; and so in the water there will clearly appear all that was written. You might also write on a tablet for a hero's chapel whatever you desire. Then it should be whitened and dried, and a light-bringing horseman painted on it, or anything else you please, with white apparel and his horse white; or if not white, any colour except black. Then it should be given to somebody, to be hung up near the city in whatever shrine he may chance upon, as though it were a votive offering. And he whose part it is to read the message must go to the shrine, and recognizing the tablet by some prearranged sign, must take it back home and put it into oil. And so everything written on it will become visible.

Πασῶν δὲ ἀδηλοτάτῃ πέμψις, πραγματωδεστάτῃ δὲ νῦν μοι ἢ δι' ἀγραμμάτων ἐμφανισθήσεται· ἔστι δὲ τοιαύδε. ἀστράγαλον εὐμεγέθη τρυπῆσαι τρυπήματα εἴκοσι καὶ τέτταρα, ἕξ εἰς ἐκάστην πλευρὰν τοῦ ἀστραγάλου· ἔστω δὲ τὰ τρυπήματα τοῦ ἀστραγάλου στοιχεῖα. διαμνημόνευε δ' ἀφ' ἧς ἂν πλευρᾶς ἄρξῃ τὸ ἄλφα καὶ τὰ ἐχόμενα ἅπερ ἐν ἐκάστῃ πλευρᾷ γέγραπται. μετὰ δὲ ταῦτα, ὅταν τινὰ θέλῃς ἐν αὐτοῖς τίθεσθαι λόγον, λίνον διείρειν, οἶον, ἐὰν θέλῃς Αἰνεῖαν δηλοῦν ἐν τῇ διέρσει τοῦ λίνου ἀρξάμενος ἐκ τῆς πλευρᾶς τοῦ ἀστραγάλου ἐν ἧ τὸ ἄλφα ἐστίν, δειρον, καὶ παρελθὼν τὰ ἐχόμενα τούτου παραγράμματα, ὅταν ἔλθῃς εἰς πλευρὰν οὗ τὸ ἰωτά ἐστίν, δειρον πάλιν, παρὲς δὲ τούτου τὰ ἐχόμενα, ὅπου συμβαίνει τὸ νῦ εἶναι, δειρον καὶ πάλιν παρὲς τὰ ἐχόμενα τούτου, ὅπου τὸ εἰ ἐστίν, δειρον τὸ λίνον, καὶ οὕτω τὰ ἐπίλοιπα τοῦ λόγου ἀντιγράφων ἔναιρε εἰς τὰ τρυπήματα, ὥσπερ ὁ ἄρτι ἐθέμεθα ὄνομα. ἔσται οὖν περὶ

τὸν ἀστράγαλον ἀγαθὶς λίνου τετολοπευμένη, δέησει δὲ τὸν ἀναγιγνώσκοντα ἀναγράφεσθαι εἰς δέλτον τὰ δηλούμενα γράμματα ἐκ τῶν τρυπημάτων. ἀνάπαλιν δὲ γίγνεται ἢ ἔξερσις τῇ ἐνέρσει. διαφέρει δὲ οὐδὲν τὰ γράμματα ἀνάπαλιν γραφῆναι εἰς τὴν δέλτον· οὐδὲν γὰρ ἦττον γνωσθήσεται. καταμαθεῖν δὲ πλεῖον ἔργον ἐστὶν τὰ γεγραμμένα ἢ τὸ ἔργον αὐτὸ γενέσθαι. δ' [...] ἂν τοῦτο γίγνοιτο ξύλου ὡς σπιθαμιαίου τρυπηθέντος ὅσα γε τὰ στοιχεῖα τῶν γραμμάτων· ἔπειτα ὡσαύτως ἐνείρειν τὸ λίνον εἰς τὰ τρυπήματα. ὅπου δ' ἂν εἰς τὸ αὐτὸ τρύπημα συμβῇ δις ἐνείρεσθαι, ὥσπερ τὸ αὐτὸ γράμμα δις ἐφεξῆς γράφεσθαι, προπεριελίζαντα τὸ λίνον περὶ τὸ ξύλον ἐνείρειν. γίγνοιτο δ' ἂν καὶ ὧδε. ἀντὶ τοῦ ἀστραγάλου καὶ ξύλου ποιήσαντα κύκλον ξύλινον λεᾶναι, καὶ τρῆσαι ἐφεξῆς κύκλῳ τὰ στοιχεῖα τῶν γραμμάτων τέτταρα καὶ εἴκοσι· ὑποψίας δ' ἔνεκεν καὶ ἄλλα ἐν μέσῳ τοῦ κύκλου τρυπῆσαι, ἔπειτα οὕτω εἰς τὰ στοιχεῖα ἐφεξῆς ὄντα τὸ λίνον ἐνείρειν. ὅταν δὲ δις τὸ αὐτὸ γράμμα συμβαίῃ γράφειν, ἐκ τῶν ἐν μέσῳ τρυπημάτων προενείραντα εἰς τὸ αὐτὸ γράμμα ἐνείρειν· γράμμα δὲ λέγω τὸ τρύπημα (Aeneas Tacticus, *How to Survive Under Siege*, 31.16-22)

The most secret method of all for sending messages, but the most difficult, namely, that without writing, I shall now make clear. It is this: In a sufficiently large astragal bore twenty-four holes, six on each side. Let the holes stand for letters, and note clearly on which side begins Alpha and the following letters that have been written on each particular side. Then, whenever you wish to communicate any word by them, draw a thread through them, as, for instance, if you wish to express Αἰνεῖαν by the drawing through of a thread, begin from the side of the astragal on which Alpha is found, pass the thread through, and omitting the characters placed next to Alpha, draw through again when you come to the side where Iota belongs; and disregarding the characters following this, again pass the thread through where Nu happens to be. And again passing by the succeeding letters draw the thread through where Epsilon is found. Now continuing in this way to write the rest of the communication, pass the thread into the holes in such a manner as that in which we just now wrote the name. Accordingly, there will be a ball of thread wound around the astragal, and it will be necessary for the one who is to read the information to write down upon a tablet the characters revealed by the holes. The unthreading takes place in the reverse order to that of the thread. But it makes no difference that the letters are written upon the tablet in reverse order, for none the less will the message be read, although to understand what has been written is a greater task than to prepare it. But this would be accomplished more easily if a piece of wood about a span long were perforated just as many times as there are letters in the alphabet, and the thread were then in the same way drawn into the holes. Wherever two insertions occur, the same character being written twice in succession, you should wind the thread around the wood before inserting it. Or it could even be done as follows. Instead of the astragal or the piece of wood, make a disc of wood, polish it, and bore successively on the disc the twenty-four characters of the alphabet; but to avoid suspicion you should bore other holes also in the centre of the disc, and then in this way run the thread through the characters, which are in their regular order. But whenever the writing of the same letter occurs twice in succession, you must insert the thread in the holes bored in the centre of the disc before running it into the same letter; and by letter I mean the hole.

Ποτίδαιαν γὰρ θέλων προδοῦναι Τιμόξενος Ἀρταβάζω προσυνέθεντο ἀλλήλοις ὁ μὲν τῆς πόλεώς τι χωρίον, ὁ δὲ τοῦ στρατοπέδου, εἰς ὅπερ ἐτόξευον πᾶν ὃ τι ἤθελον ἀλλήλοις ἐμφανίσαι. ἐτεχνάζετο δὲ ὧδε⁶ τοῦ τοξεύματος περὶ τὰς γλυφίδας ἐλίζαντες τὸ βιβλίον καὶ πτερώσαντες ἐτόξευον εἰς τὰ προσυγκείμενα χωρία. ἐγένετο δὲ καταφανὴς ὁ Τιμόξενος προδιδούς τὴν Ποτίδαιαν· τοξεύων γὰρ ὁ Ἀρτάβαζος εἰς τὸ προσυγκείμενον, ἀμαρτῶν τοῦ χωρίου διὰ πνεῦμα καὶ φαύλην πτέρωσιν, βάλλει ἄνδρὸς Ποτιδαίου τὸν ὦμον, τὸν δὲ βληθέντα περιέδραμεν ὄχλος, οἷα φιλεῖ γίνεσθαι ἐν τῷ πολέμῳ· αὐτίκα δὲ τὸ τόξευμα λαβόντες ἔφερον ἐπὶ τοὺς στρατηγούς, καὶ οὕτως καταφανὴς ἐγένετο ἡ πρᾶξις (Aeneas Tacticus, *How to Survive Under Siege*, 31.25-27; see also Herodotus, *Histories*, 8.128.2-129.1)

among the ancients the following scheme was once contrived. When Timoxenus wished to hand over Potidaea to Artabazus, they prearranged, the one a certain spot in the city, the other one in the camp, to which they used to shoot whatever they wished to communicate with each other. They adopted the device of winding a sheet of writing around the notched end of the arrow, and, after feathering it, they shot it into the places previously determined. But Timoxenus was discovered in the attempt to betray Potidaea. For Artabazus, shooting toward the designated area, missed the spot because of the wind and because the arrow was badly feathered, and hit a man of Potidaea on the shoulder, and a crowd gathered around the wounded man, as often happens in war. And immediately picking up the arrow, they brought it to the generals, and thus the plot was revealed.

Ἰστιαῖος δὲ βουλόμενος τῷ Ἀρισταγόρᾳ σημῆναι ἀποστῆναι, ἄλλως μὲν οὐδαμῶς εἶχεν ἀσφαλῶς δηλῶσαι, ἅτε φυλασσομένων τῶν ὁδῶν καὶ οὐκ εὐπορον ὄν γράμματα λαθεῖν φέροντα, τῶν δὲ⁵ δούλων τὸν πιστότατον ἀποξυρήσας ἔστιξεν καὶ ἐπέσχεν ἕως ἀνέφυσαν αἱ τρίχες. ὥς δὲ ἀνέφυσαν τάχιστα, ἔπεμπεν εἰς Μίλητον, ἐπιστείλας τῷ ἐπεστιγμένῳ ἄλλο μὲν οὐδέν, ἐπειδὴ δ' ἀφίκηται εἰς Μίλητον πρὸς Ἀρισταγόραν, κελεύειν ξυρήσαντα κατιδεῖν εἰς τὴν κεφαλὴν. τὰ δὲ στίγματα ἐσήμαινεν ἃ ἔδει ποιεῖν (Aeneas Tacticus, *How to Survive Under Siege*, 31.28-29; see also Aulus Gellius, *Attic Nights*, 17.9.18-27; Herodotus, *Histories*, 5.35; Polyaeus, *Stratagems of War*, 1.24)

Again, Histiaeus, wishing to tell Aristagoras to revolt, had no other safe means of communicating, since the roads were guarded and it was not easy for a letter-carrier to escape notice, but shaving the head of his most faithful slave, he tattooed it and detained him until the hair had grown again. And as soon as it had grown, he dispatched him to Miletus and gave the tattooed man no other orders except that when he had come to Miletus, into the presence of Aristagoras, he should request him to shave his head and examine it, whereupon the marks indicated what was to be done.

Γράφειν [...] ὧδε. προσυνθέμενον τὰ φωνήεντα γράμματα ἐν κεντήμασι τίθεσθαι, ὁπόστων δ' ἂν τύχη ἕκαστον ὄν, ἐν τοῖς γραφομένοις τοσαύτας στιγμὰς εἶναι. οἷον τόδε·

Διονύσιος κόλος - Δ :: :: N :: :: C :: :: :: C K :: :: Λ :: :: C

Ἡρακλείδας ἡκέτω - :: P · ΚΛ :: :: Δ · C :: K · T :: ::

καὶ τόδε ἄλλο· ἀντὶ τῶν φωνηέντων γραμμάτων τίθεσθαι ὅ τι δὴ (Aeneas Tacticus, *How to Survive Under Siege*, 31.30-31)

It is [...] possible to write as follows. It should be arranged in advance to express the vowels by dots, and whatever the number of each vowel happens to be, so many dots are to be placed in the writing. As for example the following:

“Dionysius docked” - d::: n::: s: .: :: s d:: ck: d
“let Heracleidas come” - l: t h: r. c l:: . d: s c:: m:

And here is another way: Instead of the vowels, put in anything whatever.

πολλοὶ δὲ κατ’ Ἑπειρον κυσὶν ἐχρήσαντο ὧδε. ἀπαγαγόντες δέσμιον περιέθηκαν περὶ τὸν αὐχένα ἱμάντα, ἐν ᾧ ἐπιστολὴ ἐνέρραπτο. εἶτα ἀφῆκαν νυκτὸς ἢ μέθ’ ἡμέραν πρὸς ὃν ἐξ ἀνάγκης ἐμελλεν ἥξειν ὅθεν ἀπήχθη. ἔστι δὲ τοῦτο καὶ Θεσσαλόν (Aeneas Tacticus, *How to Survive Under Siege*, 31.32; see also Julius Africanus, *Kestoi*, 53)

Many in Epirus used to employ dogs in the following manner. After leading the dog away in leash they placed around his neck a strap, inside of which was sewed a letter. Then at night or during the daytime, they dispatched the dog to the person to whom he was sure to go, that is, to the one from whom he had been taken away. And this is also a Thessalian custom.

2: Aeschylus (Agamemnon, 458 BCE)

Ἥφαιστος Ἰδῆς λαμπρὸν ἐκπέμπων σέλας.

φρυκτὸς δὲ φρυκτὸν δεῦρ’ ἀπ’ ἀγγάρου πυρὸς

ἔπεμπεν: Ἰδὴ μὲν πρὸς Ἑρμαῖον λέπας

Λήμνου: μέγαν δὲ πανὸν ἐκ νήσου τρίτον

Ἀθῶν αἶπος Ζηνὸς ἐξεδέξατο,

ὑπερτελής τε, πόντον ὥστε νωτίσαι,

ἰσχὺς πορευτοῦ λαμπάδος πρὸς ἡδονήν

†πεύκη τὸ χρυσοφεγγές, ὥς τις ἥλιος,

σέλας παραγγεῖλασα Μακίστου σκοπαῖς:

ὁ δ’ οὔτι μέλλων οὐδ’ ἀφρασμόνως ὕπνω

νικώμενος παρῆκεν ἀγγέλου μέρος:

ἐκὰς δὲ φρυκτοῦ φῶς ἐπ’ Εὐρίπου ῥοὰς

Μεσσαπίου φύλαξι σημαίνει μολόν.
 οἱ δ' ἀντέλαμψαν καὶ παρήγγειλαν πρόσω
 γραΐας ἐρείκης θωμὸν ἄψαντες πυρί.
 σθένουσα λαμπὰς δ' οὐδέπω μαυρουμένη,
 ὑπερθοροῦσα πεδῖον Ἀσωποῦ, δίκην
 φαιδρᾶς σελήνης, πρὸς Κιθαιρῶνος λέπας
 ἤγειρεν ἄλλην ἐκδοχὴν πομποῦ πυρός.
 φάος δὲ τηλέπομπον οὐκ ἠναίνετο
 φρουρὰ πλέον καίουσα τῶν εἰρημένων:
 λίμνην δ' ὑπὲρ Γοργῶπιν ἔσκηψεν φάος:
 ὄρος τ' ἐπ' Αἰγίπλαγκτον ἐξικνούμενον
 ὠτρυνε θεσμὸν μὴ χρονίζεσθαι πυρός.
 πέμπουσι δ' ἀνδαίοντες ἀφθόνῳ μένει
 φλογὸς μέγαν πώγωνα, καὶ Σαρωνικοῦ
 πορθμοῦ κάτοπτον πρῶν' ὑπερβάλλειν πρόσω
 φλέγουσαν: ἔστ' ἔσκηψεν εὖτ' ἀφίκετο
 Ἀραχναῖον αἶπος, ἀστυγείτονας σκοπᾶς:
 κᾶπειτ' Ἀτρειδῶν ἐς τόδε σκίπτει στέγος
 φάος τόδ' οὐκ ἄπαππον Ἰδαίου πυρός.
 τοιοῖδε τοί μοι λαμπαδηφόρων νόμοι,
 ἄλλος παρ' ἄλλου διαδοχαῖς πληρούμενοι:
 νικᾷ δ' ὁ πρῶτος καὶ τελευταῖος δραμῶν.
 τέκμαρ τοιοῦτον σύμβολόν τέ σοι λέγω
 ἀνδρὸς παραγγείλαντος ἐκ Τροίας ἐμοί (Aeschylus, *Agamemnon*, 281-316).

[Clytaemnestra speaking:] Hephaestus, sending a bright blaze on its way from Mount Ida; and then from that courier-fire beacon sent on beacon all the way here. Ida sent it to Hermes' crag on Lemnos, and from the island the great flambeau was received, thirdly, by the steep height of Zeus at Athos. Then the mighty travelling torch <shot up> aloft to arch over the sea, to the delight <of the god>, bringing its message-flame close to the sky, <and landed on Peparethos, where again much> pinewood <was burned,> which,

like another sun, conveyed the message in light of golden brilliance to the watch-heights of Macistus. Nor did Macistus neglect its part in transmitting the message, either by dilatoriness or through being heedlessly vanquished by sleep: far over the waters of the Euripus the beacon-light announced its coming to the watchmen of Messapium. They lit up in response and passed the message further on, kindling with fire a heap of old heather; and the torch, powerful and still not weakened, leaped over the plain of the Asopus like the shining moon, came to the crags of Cithaeron, and there set in motion its successor stage of the messenger-fire. The watch did not refuse the bidding of the light sent from afar, but kindled more than they had been ordered; and the light swooped over Gorgopis bay and came to the mountain where goats roam, where it stimulated the men not to <be slow in fulfilling> the ordinance about the fire. They kindled and sent on, in abundant strength, a great beard of flame, so that it would go on its blazing way right beyond the headland that looks over the Saronic narrows; then it swooped down and arrived at the steep heights of Arachnaeum, the watch-point nearest our city. And then it fell upon this house of the Atreidae, this light directly descended from the fire kindled on Ida. Such, I tell you, were my dispositions for this torch-relay, one after another of them fulfilled in succession: the first and the last runner were alike victorious! Such, I tell you, is the evidence and the token that my husband has transmitted to me from Troy.

3: Ammianus Marcellinus (*Roman History*, 4th century CE)

Proinde curarum crescente sollicitudine inde passibus citis Amidam pro temporis copia venimus civitatem postea secutis cladibus inclytam. Quo reversis exploratoribus nostris in vaginae internis notarum figuris membranam repperimus scriptam a Procopio ad nos perferri mandatam, quem legatum ad Persas antea missum cum comite Lucilliano praedixi, haec consulto obscurius indicantem, ne captis baiulis sensuque intellecto scriptorum excitaretur materia funestissima : "Amendatis procul Graiorum legatis, forsitan et necandis rex longaevis non contentus Hellesponto, iunctis Granici et Rhyndaci pontibus Asiam cum numerosis populis pervasurus adveniet, suoapte ingenio inritabilis et asperrimus, auctore et incensore Hadriani quondam Romani Principis successore; actum et conclamatum est ni caverit Graecia." Qui textus significabat Persarum regem transitis fluminibus Anzaba et Tigride, Antonino hortante dominium orientis adfectare totius. His ob perplexitatem nimiam aegerrime lectis consilium suscipitur prudens (Ammianus Marcellinus, *Roman History*, 18.6.17-19; see also Frontinus, *Stratagems*, 3.13.5)

Then with our [Ammianus and his troops] anxious cares increasing we went from there as quickly as circumstances allowed to Amida, a city afterwards notorious for the calamities which it suffered. And when our scouts had returned there, we found in the scabbard of a sword a parchment written in cipher, which had been brought to us by order of Procopius, who, as I said before, had previously been sent as an envoy to the Persians with Count Lucillianus. In this, with intentional obscurity, for fear that, if the bearers were taken and the meaning of the message known, most disastrous consequences would follow, he gave the following message: "Now that the envoys of the Greeks have been sent far away and perhaps are to be killed, that aged king, not content with Hellespontus, will bridge the Granicus and the

Rhyndacus and come to invade Asia with many nations. He is naturally passionate and very cruel, and he has as an instigator and abetter the successor of the former Roman emperor Hadrian; unless Greece takes heed, it is all over with her and her dirge chanted." This writing meant that the king of the Persians had crossed the rivers Anzaba and Tigris, and, urged on by Antoninus, aspired to the rule of the entire Orient. When it had been read, with the greatest difficulty because of its excessive ambiguity, a sagacious plan was formed.

4: Aristophanes (late 5th/early 4th century BCE)

4.1: *Birds* (ca. 414 BCE)

πρὶν μὲν γὰρ οἰκίσαι σε τήνδε τὴν πόλιν,
ἐλακωνομάνουν ἅπαντες ἄνθρωποι τότε,
ἐκόμων ἐπείνων ἐρρύπων ἐσωκράτουν
σκυτάλι' ἐφόρουν, νυνὶ δ' ὑποστρέψαντες αὖ
ὀρνιθομανοῦσι, πάντα δ' ὑπὸ τῆς ἡδονῆς
ποιοῦσιν ἅπερ ὀρνιθες ἐκμιμούμενοι (Aristophanes, *Birds*, 1280-1285)

Before you built this city all men were crazy about the Spartans:
they wore their hair long, went hungry,
never bathed, acted like Socrates,
brandished batons [*scytalae*].
But now they've about-faced and gone bird-crazy,
and they're having a wonderful time imitating birds in everything they do.

4.2: *Lysistrata* (ca. 411 BCE)

ΚΙΝΗΣΙΑΣ

κάπειτα δόρυ δῆθ' ὑπὸ μάλης ἤκεις ἔχων;

ΚΗΡΥΞ

οὐ τὸν Δί' οὐκ ἐγώνγα.

ΚΙΝΗΣΙΑΣ

ποῖ μεταστρέφεις;

τί δὴ προβάλλει τὴν χλαμύδ'; ἢ βουβωνιᾶς

ὑπὸ τῆς ὁδοῦ;

ΚΗΡΥΞ

ἀλεός γα ναὶ τὸν Κάστορα

ὄνθρωπος.

ΚΙΝΗΣΙΑΣ

ἀλλ' ἔστukas, ὦ μιαρώτατε.

ΚΗΡΥΞ

οὐ τὸν Δί' οὐκ ἐγώνγα· μηδ' αὖ πλαδδίη,

ΚΙΝΗΣΙΑΣ

τί δ' ἐστὶ σοι τοδί;

ΚΗΡΥΞ

σκυτάλα Λακωνικά. (Aristophanes, *Lysistrata*, 985-991).

Cinesias

And that's why you've come hiding a spear in your clothes?

Herald

I'm not, I swear!

Cinesias

Why are you twisting away from me? And why hold your coat out in front of you? Got a swollen groin from the long ride, maybe?

Herald

By Castor, the man's crazy!

Cinesias

Why, you've got a hard-on, you dirty rascal!

Herald

I certainly do not! Don't be talking twaddle.

Cinesias

Then what do you call that?

Herald

A Spartan walking stick.

5: Athenaeus of Naucratis (*The Learned Banqueters*, early 3rd century CE)

Ἀχαιοὺς δ' ὁ Ἑρετρίεὺς γλαφυρὸς ὢν ποιητὴς περὶ τὴν σύνθεσιν ἔσθ' ὅτε καὶ μελαίνει τὴν φράσιν καὶ πολλὰ αἰνιγματωδῶς ἐκφέρει, ὥσπερ ἐν Ἰριδι σατυρικῇ. λέγει γάρ·

λιθάργυρος

δόλπη παρηωρεῖτο χρίματος πλέα

τὸν Σπαρτιάτην γραπτὸν ἐν διπλῷ ξύλῳ

κύρβιν.

τὸν γὰρ λευκὸν ἱμάντα βουληθεὶς εἰπεῖν, ἐξ οὗ ἡ ἀργυρᾶ λήκυθος ἐξήρτητο, Σπαρτιάτην γραπτὸν ἔφη ἀντὶ τοῦ Σπαρτιάτην σκυτάλην. ὅτι δὲ λευκῷ ἱμάντι περιειλοῦντες τὴν σκυτάλην οἱ Λάκωνες ἔγραφον ἃ ἠβούλοντο, εἴρηκεν ἱκανῶς Ἀπολλώνιος ὁ Ῥόδιος ἐν τῷ Περὶ Ἀρχιλόχου (Athenaeus of Naucratis, *The Learned Banqueters*, 451c-d)

Although Achaeus of Eretria is a poet who composes elegantly, he occasionally uses obscure language and expresses himself in a confusing fashion, as for example in the satyr play *Iris*, where he says: A flask made of litharge⁴³¹ and full of oil was suspended alongside the inscribed Spartiate tablet on a double peg. Because when he [Achaeus] wanted to refer to the white thong from which [a] silver oil-flask was hanging, he referred to it as an “inscribed Spartiate” rather than as a “Spartan message-staff”. As for the fact that the Spartans wrapped their message-staffs in white thongs and wrote what they wanted on them, Apollonius of Rhodes discusses this at length in his *On Archilochus*.

6: Aulus Gellius (*Attic Nights*, ca. 177 CE)⁴³²

In his epistulis quibusdam in locis inveniuntur litterae singulares sine coagmentis syllabarum, quas tu putes positas incondite; nam verba ex his litteris confici nulla possunt. Erat autem conventum inter eos clandestinum de commutando situ litterarum, ut in scripto quidem alia aliae locum et nomen teneret, sed in legendo locus cuique suus et potestas restitueretur; quatenam vero littera pro qua scriberetur, ante is, sicuti dixi, conplacebat qui hanc scribendi latebram parabant (Aulus Gellius, *Attic Nights*, 17.9.2-4)

In certain parts of [...] letters [sent from Caesar to Oppius and Balbus] there are found individual characters which are not connected to form syllables, but apparently are written at random; for no word can be formed from those letters. [...] a secret agreement had been made between the correspondents about a change in the position of the letters, so that, in writing, one name and position was given to one letter and another to another, but in reading its own place and force was restored to each of them. But

⁴³¹ Eastaugh, Walsh et. al. 2004, 241. Litharge is one of the natural mineral forms of lead (II) oxide with a yellowish colour. Since Antiquity litharge has been used for dying purposes.

⁴³² The latest textual edition from Holford-Strevens (2019) largely preserves the standard text for this section. Any changes are highlighted in bold. The minor changes to the text introduced in his edition (based on the *Gryphius* 1537 and Salmasius manuscripts), prefer ‘tornati’ to ‘ornati’ at 17.9.7. However, this slight modification does not suggest any change to the standard translation here. In the translation offered below, Aulus Gellius describes the *scytale* as ‘smoothed and prepared’ (*derasi atque ornati*); the recommendation from Holford-Strevens would give us ‘smoothed and turned [as upon a lathe]’ (*derasi atque tornati*).

which letter was written for which was, as I have already said, agreed upon by those who devised this secret code.

Lacedaemonii autem veteres, cum dissimulare et occultare litteras publice ad imperatores suos missas volebant, ne, si ab hostibus eae captae forent, consilia sua noscerentur, epistulas id genus factas mittebant. Surculi duo erant teretes, oblonguli, pari crassamento eiusdemque longitudinis, derasi atque tornati consimiliter; unus imperatori in bellum proficiscenti dabatur, alterum domi magistratus cum iure atque cum signo habebant. Quando usus venerat litterarum secretiorum, circum eum surculum lorum modicae tenuitatis, longum autem quantum rei satis erat, complicabant, volumine rotundo et simplici, ita uti orae adiunctae undique et cohaerentes lori, quod plicabatur, coirent. Litteras deinde in eo loro per transversas iuncturarum oras versibus a summo (surculo) ad imum proficiscentibus inscribebant. Id lorum litteris ita perscriptis revolutum ex surculo imperatori commenti istius conscio mittebant; resolutio autem lori litteras truncas atque mutilas reddebat membraque earum et apices in partis diversissimas spargebat. Propterea, si id lorum in manus hostium inciderat, nihil quicquam coniectari ex eo scripto quibat; sed ubi ille ad quem erat missum acceperat, surculo conpari quem habebat (a) capite ad finem, proinde ut debere fieri sciebat, circumplicabat, atque ita litterae per eundem ambitum surculi coalescentes rursum coibant integramque et incorruptam epistulam et facilem legi praestabant. Hoc genus epistulae Lacedaemonii σκυτάλην appellant (Aulus Gellius, *Attic Nights*, 17.9.6-16)

The ancient Lacedaemonians, when they wanted to conceal and disguise the public dispatches sent to their generals, in order that, in case they were intercepted by the enemy, their plans might not be known, used to send letters written in the following manner. There were two thin, cylindrical wands of the same thickness and length, smoothed and prepared so as to be exactly alike. One of these was given to the general when he went to war, the other the magistrates kept at home under their control and seal. When the need of more secret communication arose, they bound about the staff a thong of moderate thickness, but long enough for the purpose, in a simple spiral, in such a way that the edges of the thong which was twined around the stick met and were joined throughout. Then they wrote the dispatch on that thong across the connected edges of the joints, with the lines running from the top to the bottom. When the letter had been written in this way, the thong was unrolled from the wand and sent to the general, who was familiar with the device. But the unrolling of the thong made the letters imperfect and broken, and their parts and strokes were divided and separated. Therefore, if the thong fell into the hands of the enemy, nothing at all could be made out from the writing; but when the one to whom the letter was sent had received it, he wound it around the corresponding staff, which he had, from the top to the bottom, just as he knew that it ought to be done, and thus the letters, united by encircling a similar staff, came together again, rendering the dispatch entire and undamaged, and easy to read. This kind of letter the Lacedaemonians called σκυτάλη.

Legebamus id quoque in vetere historia rerum Poenicarum, virum indidem quempiam inlustrem—sive ille Hasdrubal sive quis alius est non retineo—epistulam scriptam super rebus arcanis hoc modo

abscondisse: pugillaria nova, nondum etiam cera inlita, accepisse, litteras in lignum incidisse, postea tabulas, uti solitum est, cera conlevissime easque tabulas, tamquam non scriptas, cui facturum id praedixerat misisse; eum deinde ceram derasisse litterasque incolumes ligno incisas legisse (Aulus Gellius, *Attic Nights*, 17.9.16-17; see also Justin, *Epitome of the Philippic History of Pompeius Trogus*, 21.6)

[Aulus Gellius speaking:] I [...] read this in an ancient history of Carthage, that a certain famous man of that country—whether it was Hasdrubal or another I do not recall—disguised a letter written about secret matters in the following way: he took new tablets, not yet provided with wax, and cut the letters into the wood. Afterwards he covered the tablet with wax in the usual way and sent it, apparently without writing, to one to whom he had previously told his plan. The recipient then scraped off the wax, found the letters safe and sound inscribed upon the wood, and read them.

Est [...] in monumentis rerum Graecarum profunda quaedam et inopinabilis latebra, barbarico astu excogitata. Histiaeus nomine fuit, loco natus in terra Asia non ignobili. Asiam tunc tenebat imperio rex Darius. Is Histiaeus, cum in Persis apud Darium esset, Aristagorae cuiusdam res quasdam occultas nuntiare furtivo scripto volebat. Comminiscitur opertum hoc litterarum admirandum. Servo suo diu oculos aegros habenti capillum ex capite omni tamquam medendi gratia deradit caputque eius leve in litterarum formas compungit. His litteris quae voluerat perscripsit, hominem postea quoad capillus adolesceret domo continuit. Ubi id factum est, ire ad Aristagoran iubet et “Cum ad eum,” inquit, “veneris, mandasse me dicito ut caput tuum, sicut nuper egomet feci, deradat.” Servus, ut imperatum erat, ad Aristagoran venit mandatumque domini adfert. Atque ille id non esse frustra ratus, quod erat mandatum fecit. Ita litterae perlatae sunt (Aulus Gellius, *Attic Nights*, 17.9.18-27; see also Aeneas Tacticus, *How to Survive Under Siege*, 31.28-39; Herodotus, *Histories*, 5.35; Polyaeus, *Stratagems of War*, 1.24)

There is [...] in the records of Grecian history another profound and difficult method of concealment, devised by a barbarian's cunning. He was called Histiaeus and was born in the land of Asia in no mean station. At that time king Darius held sway in Asia. This Histiaeus, being in Persia with Darius, wished to send a confidential message to a certain Aristagoras in a secret manner. He devised this remarkable method of concealing a letter. He shaved all the hair from the head of a slave of his who had long suffered from weak eyes, as if for the purpose of treatment. Then he tattooed the forms of the letters on his smooth head. When in this way he had written what he wished, he kept the man at home for a time, until his hair grew out. When this happened, he ordered him to go to Aristagoras, adding: “When you come to him, say that I told him to shave your head, as I did a little while ago.” The slave, as he was bidden, came to Aristagoras and delivered his master's order. Aristagoras, thinking that the command must have some reason, did as he was directed. And thus the letter reached its destination.

7: Ausonius (*Epistles*, 4th century CE)

Vel si tibi proditor instat
aut quaesitoris gravior censura timetur,
occurre ingenio, quo saepe occulta teguntur.
Thraecicii quondam quam saeva licentia regis
fecerat elinguem, per licia texta querellas
edidit et tacitis mandavit crimina telis.
et pudibunda suos malo commisit amores
virgo nec erubuit tacituro conscia pomo.
depressis scrobibus vitium regale minister
credidit idque diu texit fidissima tellus:
inspirata dehinc vento cantavit harundo.
lacte incide notas: arescens charta tenebit
semper inaspicuas; prodentur scripta favillis.
vel Lacedaemoniam *scytalen* imitare, libelli
segmina Pergamei tereti circumdata ligno
perpetuo inscribens versu, qui deinde solutus,
non respondentes sparso dabit ordine formas,
donec consimilis ligni replicetur in orbem.
Innumeras possum celandi ostendere formas
et clandestinas veterum reserare loquellas:
si prodi, Pauline, times nostraeque vereris
crimen amicitiae [...] (Ausonius, *Epistles*, 28.10-31)

If an informer is beside thee,
and if 'tis an inquisitor's too stern rebuke is feared,
baffle it with a device whereby secrets are oft concealed.
She whom the brutal outrage of the Thracian king
had robbed of her tongue, revealed her sorrows
by means of woven threads
and committed the story of her wrongs to the silent loom.
Also a shamefast maid entrusted the tale of her love to an apple,
and blushed not to share her secret with fruit which could never speak.
To deep-dug pits a servant revealed his royal lord's deformity,
and long the earth hid the secret most faithfully:
hereafter the reed, breathed on by the wind, sang the story.
Trace letters with milk:
the paper as it dries will keep them ever invisible;
yet with ashes the writing is brought to light.
Or imitate the Spartan *scytale*,

writing on strips of parchment
wound about a rounded stick in continuous lines,
which, afterwards unrolled,
will show characters incoherent because sequence is lost,
until they are rolled again about just such another stick.
I can show thee countless codes of the ancients
for concealing and unlocking secret messages;
if thou, Paulinus, fearest to be betrayed
and dread'st the charge of my friendship.

8: Cassius Dio (*Roman History*, 3rd century CE)

εἰώθει δὲ καὶ ἄλλως, ὁπότε τι δι' ἀπορρήτων τινὶ ἐπέστελλε, τὸ τέταρτον ἀεὶ στοιχεῖον ἀντὶ τοῦ καθήκοντος ἀντεγγράφειν, ὅπως ἂν (Cassius Dio, *Roman History*, 40.9.3)

It was his [Caesar's] usual practice, whenever he was sending a secret message to any one, to substitute in every case for the proper letter of the alphabet the fourth letter beyond, so that the writing might be unintelligible to most persons.

ὅπως γε μὴδ' αὐτός τι μήτ' οὖν ἐθελοντῆς μήτ' ἄκων ἐξείπη, οὔτε τι αὐτῷ ἐξελάλησε, καὶ τῷ Κικέρωνι πάνθ' ὅσα ἡβουλήθη ἑλληνιστὶ ἐπέστειλεν, ἵνα ἂν καὶ τὰ γράμματα ἀλφ, ἀλλ' ἀσύνετά γε καὶ τότε τοῖς βαρβάροις ὄντα μὴδὲν σφας ἐκδιδάξη (Cassius Dio, *Roman History*, 40.9.3; see also Caesar, *The Gallic War*, 5.48)

In order that even he [the messenger] might not reveal anything, voluntarily or involuntarily, he gave him no verbal message and wrote to [Quintus] Cicero in Greek all that he wished to say, in order that even if the letter were captured, it should even so be meaningless to the barbarians and afford them no information.

9: Cicero (*Letters to Atticus*, 68-44 BCE)

Habes σκυτάλην Λακωνικήν. omnino excipiam hominem. erat autem v Non. venturus vesperi, id est hodie; cras igitur ad me fortasse veniet. temptabo, audiam: nihil properare, missurum ad Caesarem. clam agam, cum paucissimis alicubi occultabor; certe hinc istis invitissimis evolabo, atque utinam ad Curionem! σύνες ὃ τοι λέγω. magnus dolor accessit. efficietur aliquid dignum nobis (Cicero, *Letters to Atticus*, 10.10 (Letter 201)).

There's a Laconian dispatch [σκυτάλην Λακωνικήν] for you! To be sure I shall lie in wait for him—he is coming on the evening of the 3rd, i.e. today, so perhaps he will call on me tomorrow. I shall sound him, listen to him. I shall say that I am in no hurry, that I shall send to Caesar. I shall act by stealth and conceal

myself somewhere with a very few companions. At all events I shall escape from here, however much they want to stop me, and I only hope it will be to Curio. Mark my words. Intense vexation has been added to my other motives. I shall bring off something worthy of myself.⁴³³

10: Cornelius Nepos (*The Book on the Great Generals of Foreign Nations*. Pausanias, 1st century BCE)

Spartam redire nolebat; Colonas, qui locus in agro Troade est, se contulerat; ibi consilia cum patriae tum sibi inimica capiebat. Id postquam Lacedaemonii rescierunt, legatos cum clava ad eum miserunt, in qua more illorum erat scriptum: nisi domum reverteretur, se capitis eum damnaturos. Hoc nuntio commotus, sperans se etiam tum pecunia et potentia instans periculum posse depellere, domum rediit. Huc ut venit, ab ephoris in vincla publica est coniectus; licet enim legibus eorum cuivis ephoro hoc facere regi. Hinc tamen se expedivit, neque eo magis carebat suspicione; nam opinio manebat eum cum rege habere societatem (Cornelius Nepos, *The Book on the Great Generals of Foreign Nations*, 4.3.4; see also Thucydides, *History of the Peloponnesian War*, 1.131.1)

To Sparta he [Pausanias] would not return, but withdrew to Colonaë, a place in the country of Troas, where he formed designs pernicious both to his country and himself. When the Lacedaemonians knew of his proceedings, they sent deputies to him with a scytale [clava], on which it was written, after their fashion, that "if he did not return home, they would condemn him to death." Being alarmed at this communication, but hoping that he should be able, by his money and his influence, to ward off the danger that threatened him, he returned home. As soon as he arrived there, he was thrown into the public prison by the *Ephori*, for it is allowable, by their laws, for any one of the *Ephori* to do this to a king. He however got himself freed from confinement, but was not cleared from suspicion, for the belief still prevailed, that he had made a compact with the king of Persia.

11: Diodorus Siculus (*Library of History*, 1st century BCE)

Ἐπὶ δὲ τοὺς εἰς Σηστὸν καταφυγόντας Ἀθηναίους στρατεύσας τὴν μὲν πόλιν εἴλε, τοὺς δ' Ἀθηναίους ὑποσπόνδους ἀφῆκεν. Εὐθὺς δὲ τῇ δυνάμει πλεύσας ἐπὶ Σάμον αὐτὸς μὲν ταύτην ἐπολιόρκει, Γύλιππον δὲ τὸν εἰς Σικελίαν τοῖς Συρακοσίοις τῷ ναυτικῷ συμπολεμήσαντα ἀπέστειλεν εἰς Σπάρτην τά τε λάφυρα κομίζοντα καὶ μετὰ τούτων ἀργυρίου τάλαντα χίλια καὶ πεντακόσια. Ὅντος δὲ τοῦ χρήματος ἐν σακίοις, καὶ ταῦτ' ἔχοντος ἐκάστου σκυτάλην ἔχουσιν τὴν ἐπιγραφὴν τὸ πλῆθος τοῦ χρήματος δηλοῦσαν, ταύτην ἀγνοήσας ὁ Γύλιππος τὰ μὲν σακία παρέλυσεν, ἐξελόμενος δὲ τάλαντα τριακόσια,

⁴³³ Significantly, the words 'Laconian dispatch' (σκυτάλην Λακωνικήν) are written in Greek instead of Latin, something that Cicero often did in his letters. In this letter (*Letters to Atticus*, 10.10) one can find five more instances in which Cicero changed Latin words for Greek ones.

καὶ διὰ τῆς ἐπιγραφῆς γνωσθεὶς ὑπὸ τῶν ἐφόρων, ἔφυγε καὶ κατεδικάσθη θανάτῳ (Diodorus Siculus, *Library of History*, 13.106.8-9)

After this, advancing against the Athenians who had found refuge in Sestus, he [Lysander] took the city but let the Athenians depart under a truce. Then he sailed at once to Samos with his troops and himself began the siege of the city, but Gylippus, who with a flotilla had fought in aid of the Syracusans in Sicily, he dispatched to Sparta to take there both the booty and with it fifteen hundred talents of silver. The money was in small bags, each of which contained a scytale which carried the notation of the amount of the money. Gylippus, not knowing of the *scytale*, secretly undid the bags and took out three hundred talents, and when, by means of the notation, Gylippus was detected by the *ephors*, he fled the country and was condemned to death.

12: Frontinus (*Stratagems*, late 1st century CE)

Romani, obsessi in Capitolio, ad Camillum auxilio implorandum miserunt Pontium Cominium, qui, ut stationes Gallorum falleret, per saxa Tarpeia demissus tranato Tiberi Veios pervenit et perpetrata legatione similiter ad suos rediit. Campani, diligenter Romanis a quibus obsessi erant custodias agentibus, quendam pro transfuga subornatum miserunt, qui occultatam balteo epistulam inventa effugiendi occasione ad Poenos pertulit.

Venationi quoque et pecoribus quidam insuerunt litteras membranis mandatas.

Aliqui et iumento in aversam partem infulserunt, dum stationes transeunt.

Nonnulli interiora vaginarum inscripserunt.

L. Lucullus, Cyzicenos obsessos a Mithridate ut certiores adventus sui faceret, cum praesidiis hostium teneretur introitus urbis, qui unus et angustus ponte modico insulam continenti iungit, militem e suis nandi et nauticae artis peritum iussit insidentem duobus inflatis utribus litteras insutas habentibus, quos ab inferiore parte duabus regulis inter se distantibus commiserat, ire septem milia passuum traiecit. Quod ita perite gregalis fecit, ut cruribus velut gubernaculis dimissis cursum dirigeret et procul visentis, qui in statione erant, marinae specie beluae deciperet.

Hirtius consul ad Decimum Brutum, qui Mutinae ab Antonio obsidebatur, litteras subinde misit plumbo scriptas, quibus ad brachium religatis milites Scultennam amnem tranabant.

Idem columbis, quas inclusas ante tenebris et fame adfecerat, epistulas saeta ad collum religabat easque a propinquo, in quantum poterat, moenibus loco mittebat. Illae lucis cibique avidae altissima aedificiorum petentes excipiebantur a Bruto, qui eo modo de omnibus rebus certior fiebat, utique postquam disposito quibusdam locis cibo columbas illuc devolare instituerat (Frontinus, *Stratagems*, 13; see also Ammianus Marcellinus, *Roman History*, 18.6.17-19)

When the Romans were besieged in the Capitol, they sent Pontius Cominius to implore Camillus to come to their aid. Pontius, to elude the pickets of the Gauls, let himself down over the Tarpeian Rock, swam the Tiber, and reached Veii. Having accomplished his errand, he returned by the same route to

his friends.

When the Romans were maintaining careful guard against the inhabitants of Capua, whom they were besieging, the latter sent a certain fellow in the guise of a deserter, and he, finding an opportunity to escape, conveyed to the Carthaginians a letter which he had secreted in his belt.

Some have written messages on skins and then sewed these to the carcasses of game or sheep.

Some have stuffed the message under the tail of a mule while passing the picket-posts.

Some have written on the linings of scabbards.

When the Cyzicenes were besieged by Mithridates, Lucius Lucullus wished to inform them of his approach. There was a single narrow entrance to the city, connecting the island with the mainland by a small bridge. Since this was held by forces of the enemy, he sewed some letters up inside two inflated skins and then ordered one of his soldiers, an adept in swimming and boating, to mount the skins, which he had fastened together at the bottom by two strips some distance apart, and to make the trip of seven miles across. So skilfully did the soldier do this that, by spreading his legs, he steered his course as though by rudder, and deceived those watching from a distance by appearing to be some marine creature.

The consul Hirtius often sent letters inscribed on lead plates to Decimus Brutus, who was besieged by Antonius at Mutina. The letters were fastened to the arms of soldiers, who then swam across the Scultenna River.

Hirtius also shut up pigeons in the dark, starved them, fastened letters to their necks by a hair, and then released them as near to the city walls as he could. The birds, eager for light and food, sought the highest buildings and were received by Brutus, who in that way was informed of everything, especially after he set food in certain spots and taught the pigeons to alight there.

13: Herodian (*History of the Empire from the Death of Marcus*, late 2nd/early 3rd century CE)

παραδούς αὐτῷ ἑκατοντάρχας καὶ στρατιώτας τινάς, οἷς ἔδωκε κατασεσημασμένα γράμματα ἐν πτυκτοῖς πίναξι, δι' ὧν τὰ ἀπόρρητα καὶ κρυπτὰ ἀγγέλματα τοῖς βασιλεῦσιν ἐπιστέλλεται (Herodian, *History of the Empire from the Death of Marcus*, 7.6.5)

Gordian transferred to his [a provincial quaestor's] command some centurions and soldiers, to whom he gave a letter sealed in folding tablets, the normal method used by the emperor to send private, secret messages.

14: Herodotus (*Histories*, ca. 440 BCE)

λαγὸν μηχανησάμενος, καὶ ἀνασχίσας τοῦτου τὴν γαστέρα καὶ οὐδὲν ἀποτίλας, ὥς δὲ εἶχε οὕτω ἐσέθηκε βυβλίον, γράψας τὰ οἱ ἔδοκε: ἀπορράψας δὲ τοῦ λαγοῦ τὴν γαστέρα, καὶ δίκτυα δούς ἅτε θηρευτῇ τῶν οἰκετέων τῷ πιστοτάτῳ, ἀπέστειλε ἐς τοὺς Πέρσας, ἐντειλάμενός οἱ ἀπὸ γλώσσης διδόντα τὸν λαγὸν Κύρῳ ἐπειπεῖν αὐτοχειρὶ μιν διελεῖν καὶ μηδένα οἱ ταῦτα ποιεῦντι παρεῖναι. ταῦτά τε δὴ ὧν ἐπιτελέα ἐγίνετο καὶ ὁ Κῦρος παραλαβὼν τὸν λαγὸν ἀνέσχισε: εὐρὼν δὲ ἐν αὐτῷ τὸ βυβλίον ἐνεὸν λαβὼν ἐπελέγετο, τὰ δὲ γράμματα ἔλεγε τάδε. ὦ παῖ Καμβύσει, σὲ γὰρ θεοὶ ἐπορώσι: οὐ γὰρ ἂν κοτὲ ἐς

τοσοῦτο τύχης ἀπίκευ: σύ νυν Ἀστυάγεα τὸν σεωυτοῦ φονέα τῖσαι. κατὰ μὲν γὰρ τὴν τούτου προθυμίην τέθνηκας, τὸ δὲ κατὰ θεοῦς τε καὶ ἐμὲ περίεις: τά σε καὶ πάλαι δοκέω πάντα ἐκμεμαθηκέναι, σέο τε αὐτοῦ περὶ ὡς ἐπρήχθη, καὶ οἷα ἐγὼ ὑπὸ Ἀστυάγεος πέπονθα, ὅτι σε οὐκ ἀπέκτεινα ἀλλὰ ἔδωκα τῷ βουκόλῳ. σύ νυν, ἣν βούλῃ ἐμοὶ πείθεσθαι, τῆς περ Ἀστυάγης ἄρχει χώρας, ταύτης ἀπάσης ἄρξεις. Πέρσας γὰρ ἀναπείσας ἀπίστασθαι στρατηλάτεις ἐπὶ Μήδους: καὶ ἦν τε ἐγὼ ὑπὸ Ἀστυάγεος ἀποδεχθέω στρατηγὸς ἀντὶα σεῦ, ἔστι τοι τὰ σὺ βούλει, ἦν τε τῶν τις δοκίμων ἄλλος Μήδων: πρῶτοι γὰρ οὗτοι ἀποστάντες ἀπ' ἐκείνου καὶ γενόμενοι πρὸς σέο Ἀστυάγεα καταίρουν πειρήσονται. ὡς ὧν ἐτοίμου τοῦ γε ἐνθάδε ἐόντος, ποίειε ταῦτα καὶ ποίειε κατὰ τάχος (Herodotus, *Histories*, 1.123.4-1.124).

He [Harpagus] artfully slit the belly of a hare, and then leaving it as it was without further harm he put into it a paper on which he wrote what he thought fit. Then he sewed up the hare's belly, and sent it to Persia by the trustiest of his servants, giving him nets to carry as if he were a huntsman. The messenger was charged to give Cyrus the hare and bid him by word of mouth to cut it open with his own hands, none other being present. All this was done. Cyrus took the hare and slit it and read the paper which was in it; the writing was as follows: "Son of Cambyses, seeing that the gods watch over you (for else you had not so prospered) do you now avenge yourself on Astyages, your murderer; for according to his intent you are dead; it is by the gods' doing, and mine, that you live. Methinks you have long ago heard the story of what was done concerning yourself and how Astyages entreated me because I slew you not but gave you to the cowherd. If then you will be counselled by me, you shall rule all the country which is now ruled by Astyages. Persuade the Persians to rebel, and lead their army against the Medes; then you have your desire, whether I be appointed to command the army against you or some other notable man among the Medians; for they will of themselves revolt from Astyages and join you and endeavour to pull him down. Seeing then that all here is ready, do as I say and do it quickly"

ἄρρωδέων [...] τούτων ἕκαστα ἐβουλευέτο ἀπόστασιν: συνέπιπτε γὰρ καὶ τὸν ἐστιγμένον τὴν κεφαλὴν ἀπῖχθαι ἐκ Σούσων παρὰ Ἰστιαίου, σημαίνοντα ἀπίστασθαι Ἀρισταγόρην ἀπὸ βασιλέως. ὁ γὰρ Ἰστιαῖος βουλόμενος τῷ Ἀρισταγόρῃ σημῆναι ἀποστῆναι ἄλλως μὲν οὐδαμῶς εἶχε ἀσφαλέως σημῆναι ὥστε φυλασσομενέων τῶν ὁδῶν, ὁ δὲ τῶν δούλων τὸν πιστότατον ἀποξυρήσας τὴν κεφαλὴν ἔστιξε καὶ ἀνέμεινε ἀναφῶναι τὰς τρίχας, ὡς δὲ ἀνέφυσαν τάχιστα, ἀπέπεμπε ἐς Μίλητον ἐντειλάμενος αὐτῷ ἄλλο μὲν οὐδέν, ἐπεὰν δὲ ἀπικηται ἐς Μίλητον, κελεύειν Ἀρισταγόρην ξυρήσαντά μιν τὰς τρίχας κατιδέσθαι ἐς τὴν κεφαλὴν. τὰ δὲ στίγματα ἐσήμαινε, ὡς καὶ πρότερόν μοι εἴρηται, ἀπόστασιν. ταῦτα δὲ ὁ Ἰστιαῖος ἐποίηε συμφορὴν ποιούμενος μεγάλην τὴν ἐωυτοῦ κατοχὴν τὴν ἐν Σούσοισι: ἀποστάσιος ὧν γινομένης πολλὰς εἶχε ἐλπίδας μετήσεσθαι ἐπὶ θάλασσαν, μὴ δὲ νεώτερόν τι ποιεύσης τῆς Μιλήτου οὐδαμὰ ἐς αὐτὴν ἥξειν ἔτι ἐλογίζετο (Herodotus, *Histories*, 5.35.2-4).

With [...] fears in his mind, he [Histiaeus] began to plan revolt, for it chanced that at that very time there came from Susa Histiaeus' messenger, the man with the marked head, signifying that Aristagoras should revolt from the king. Since Histiaeus desired to give word to Aristagoras that he should revolt and had no other safe way of doing so because the roads were guarded, he shaved and branded the head of his most trustworthy slave. He waited till the hair had grown again, and as soon as it was grown, he sent the

man to Miletus with no other message except that when he came to Miletus he must bid Aristagoras shave his hair and examine his head. The writing branded on it signified revolt, as I have already said. This Histiaeus did because he greatly disliked his detention at Susa and fully expected to be sent away to the coast in the case that there should be a revolt. If, however, Miletus remained at peace, he calculated that he would never return there.

ἄναιμι δὲ ἐκεῖσε τοῦ λόγου τῇ μοι τὸ πρότερον ἐξέλιπε. ἐπύθοντο Λακεδαιμόνιοι ὅτι βασιλεὺς στέλλοιτο ἐπὶ τὴν Ἑλλάδα πρῶτοι, καὶ οὕτω δὴ ἐς τὸ χρηστήριον τὸ ἐς Δελφοὺς ἀπέπεμψαν, ἔνθα δὴ σφί ἐχρήσθη τὰ ὀλίγα πρότερον εἶπον: ἐπύθοντο δὲ τρόπῳ θωμασίῳ. Δημάρητος γὰρ ὁ Ἀρίστωνος φυγὼν ἐς Μήδους, ὥς μὲν ἐγὼ δοκέω καὶ τὸ οἶκός ἐμοὶ συμμάχεται, οὐκ ἦν εὖνοος Λακεδαιμονίοισι, πάρεστι δὲ εἰκάζειν εἴτε εὐνοίῃ ταῦτα ἐποίησε εἴτε καὶ καταχαίρων. ἐπεῖτε γὰρ Ξέρξης ἔδοξε στρατηλατέειν ἐπὶ τὴν Ἑλλάδα, ἔὼν ἐν Σούσοισι ὁ Δημάρητος καὶ πυθόμενος ταῦτα ἠθέλησε Λακεδαιμονίοισι ἐξαγγεῖλαι. ἄλλως μὲν δὴ οὐκ εἶχε σημῆναι: ἐπικίνδυνον γὰρ ἦν μὴ λαμφθεῖν: ὁ δὲ μηχανᾶται τοιάδε: δελτίον δίπτυχον λαβὼν τὸν κηρὸν αὐτοῦ ἐξέκνησε, καὶ ἔπειτα ἐν τῷ ξύλῳ τοῦ δελτίου ἔγραψε τὴν βασιλέως γνώμην, ποιήσας δὲ ταῦτα ὀπίσω ἐπέτηξε τὸν κηρὸν ἐπὶ τὰ γράμματα, ἵνα φερόμενον κεινὸν τὸ δελτίον μηδὲν πρῆγμα παρέχοι πρὸς τῶν ὁδοφυλάκων. ἐπεὶ δὲ καὶ ἀπῆκετο ἐς τὴν Λακεδαίμονα, οὐκ εἶχον συμβαλέσθαι οἱ Λακεδαιμόνιοι, πρὶν γε δὴ σφί, ὥς ἐγὼ πυνθάνομαι, Κλεομένεος μὲν θυγάτηρ Λεωνίδεω δὲ γυνὴ Γοργῷ ὑπέθετο ἐπιφρασθεῖσα αὐτῇ, τὸν κηρὸν κνᾶν κελεύουσα, καὶ εὐρήσειν σφέας γράμματα ἐν τῷ ξύλῳ. πειθόμενοι δὲ εὗρον καὶ ἐπελέξαντο, ἔπειτα δὲ τοῖσι ἄλλοις Ἑλλήσι ἐπέστειλαν (Herodotus, *Histories*, 7.239)

The Lacedaemonians were the first to be informed that the king [Xerxes] was equipping himself to attack Hellas; with this knowledge it was that they sent to the oracle at Delphi, where they received the answer about which I [Herodotus] spoke a little while ago. Now the way in which they were informed of this was strange. Demaratus son of Ariston, an exile among the Medes, was, as I suppose (reason being also my ally), no friend to the Lacedaemonians, and I leave it to be imagined whether what he did was done out of goodwill or spiteful triumph. When Xerxes was resolved to march against Hellas, Demaratus, who was then at Susa and had knowledge of this, desired to send word of it to the Lacedaemonians. He, however, feared detection and had no other way of informing them than this trick:—taking a double tablet, he scraped away the wax from it, and then wrote the king's plan on the wood. Next he melted the wax back again over the writing, so that the bearer of this seemingly blank tablet might not be troubled by the way-wardens. When the tablet came to Lacedaemon, the Lacedaemonians could not guess its meaning, until at last (as I have been told) Gorgo, Cleomenes' daughter and Leonidas' wife, discovered the trick herself and advised them to scrape the wax away so that they would find writing on the wood. When they did so, they found and read the message, and presently sent it to the rest of the Greeks.

ὅπως βυβλίον γράψει ἡ Τιμόξεινος ἐθέλων παρὰ Ἀρτάβαζον πέμψαι ἢ Ἀρτάβαζος παρὰ Τιμόξεινον, τοξεύματος παρὰ τὰς γλυφίδας περιελίξαντες καὶ πετρώσαντες τὸ βυβλίον ἐτόξευον ἐς συγκείμενον χωρίον. ἐπῆιστος δὲ ἐγένετο ὁ Τιμόξεινος προδιδούς τὴν Ποτίδαιαν· τοξεύων γὰρ ὁ Ἀρτάβαζος ἐς τὸ

συγκείμενον, ἀμαρτῶν τοῦ χωρίου τούτου βάλλει ἀνδρὸς Ποτιδαίητεω τὸν ὄμον, τὸν δὲ βληθέντα περιέδραμε ὄμιλος, οἷα φιλέει γίνεσθαι ἐν πολέμῳ, οἱ αὐτίκα τὸ τόξευμα λαβόντες ὡς ἔμαθον τὸ βυβλίον, ἔφερον ἐπὶ τοὺς στρατηγούς· παρὴν δὲ καὶ τῶν ἄλλων Παλληναίων συμμαχίῃ. τοῖσι δὲ στρατηγοῖσι ἐπιλεξαμένοισι τὸ βυβλίον καὶ μαθοῦσι τὸν αἴτιον τῆς προδοσίης ἔδοξε μὴ καταπλῆξαι Τιμόξεινον προδοσίῃ τῆς Σκιωναίων πόλιος εἵνεκα, μὴ νομιζοίατο εἶναι Σκιωναῖοι ἐς τὸν μετέπειτα χρόνον αἰεὶ προδῶται. Ὁ μὲν δὴ τοιούτῳ τρόπῳ ἐπάιστος ἐγγέγονε (Herodotus, *Histories*, 8.128.2-129.1; see also Aeneas Tacticus, *How to Survive Under Siege*, 31.25-27)

Whenever Timoxenus wrote a letter for sending to Artabazus, or Artabazus to Timoxenus, they would wrap it round the shaft of an arrow at the notches and put feathers to the letter, and shoot it to a place whereon they had agreed. But Timoxenus' plot to betray Potidaea was discovered; for Artabazus in shooting an arrow to the place agreed upon, missed it and hit the shoulder of a man of Potidaea; and a throng gathering quickly round the man when he was struck (which is a thing that ever happens in war), they straightway took the arrow and found the letter and carried it to their generals, the rest of their allies of Pallene being also there present. The generals read the letter and perceived who was the traitor, but they resolved for Scione's sake that they would not smite Timoxenus to the earth with a charge of treason, lest so the people of Scione should ever after being called traitors. Thus was Timoxenus' treachery brought to light.

15: Homer (*Iliad*, 8th/7th century BCE)

ὥς φάτο, τὸν δὲ ἄνακτα χόλος λάβεν οἷον ἄκουσε:

κτεῖναι μὲν ῥ' ἄλέεινε, σεβάσσατο γὰρ τό γε θυμῷ,

πέμπε δέ μιν Λυκίην δέ, πόρεν δ' ὃ γε σήματα λυγρὰ

γράψας ἐν πίνακι πτυκτῷ θυμοφθόρα πολλά,

δεῖξαι δ' ἠνώγειν ᾧ πενθερῷ ὄφρ' ἀπόλοιτο

δὴ σῆμα κακὸν παρεδέξατο γαμβροῦ (Homer, *Iliad*, 6.166-170).

[Proetus] shunned killing him [Bellerophon], for his heart shrank from that; but he sent him to Lycia, and gave him fatal tokens, scratching in a folded tablet signs many and deadly, and ordered him to show these to his father-in-law [Iobates], so that he might perish.

δὴ σῆμα κακὸν παρεδέξατο γαμβροῦ (Homer, *Iliad*, 6.178).

he [Iobates] had received from him [Bellerophon] the evil token from his son-in-law [Proetus].

ἦ [...] ἄρ' ὥς εἰποῦσ' ἀπέβη πόδας ὠκέα Ἴρις,
αὐτὰρ Ἀχιλλεὺς ὦρτο Διὶ φίλος· ἀμφὶ δ' Ἀθήνη
ὤμοις ἰφθίμοισι βάλλ' αἰγίδα θυσσανόεσσαν,
ἀμφὶ δέ οἱ κεφαλῇ νέφος ἔστεφε δῖα θεάων
χρύσειον, ἐκ δ' αὐτοῦ δαΐε φλόγα παμφανόωσαν.
ὥς δ' ὅτε καπνὸς ἰὼν ἐξ ἄστεος αἰθέρ' ἵκηται
τηλόθεν ἐκ νήσου, τὴν δῆϊοι ἀμφιμάχωνται,
οἳ τε πανημέριοι στυγερῷ κρίνονται Ἄρηϊ
ἄστεος ἐκ σφετέρου· ἅμα δ' ἡελίῳ καταδύντι
πυρσοὶ τε φλεγέθουσιν ἐπήτριμοι, ὑψόσε δ' αὐγὴ
γίγνεται αἴσσουσα περικτιόνεσσιν ἰδέσθαι,
αἳ κέν πῶς σὺν νηυσὶν ἄρεω ἀλκτῆρες ἵκωνται·
ὥς ἂπ' Ἀχιλλῆος κεφαλῆς σέλας αἰθέρ' ἵκανε (Homer, *Iliad*, 18.203-214)

So spoke swift-footed Iris and went away; but Achilles, dear to Zeus, rose up, and around his mighty shoulders Athene flung her tasselled aegis, and around his head the fair goddess set thick a golden cloud, and from the man made blaze a gleaming flame. And as smoke goes up from a city and reaches to heaven from afar, from an island that foes beleaguer, and its men contend all day long in hateful war from their city's walls, and then at sunset flame out the beacon fires one after another, and high aloft darts their glare for dwellers round about to look on, in the hope that they may come in their ships to be warders off of ruin, so from the head of Achilles went up the gleam toward heaven.

16: Julius Africanus (*Kestoi*, late 2nd/early 3rd century CE)

Τοῖς κεκρημένοις προδόταις ἀναγκαῖον εἰδέναι πῶς ἐπιστολὰς δεῖ αὐτοὺς εἰσπέμπειν. ἀπόστελλε γοῦν οὕτως. πεμπέσθω ἀνὴρ ἐν τῷ φανερωῷ φέρων ἐπιστολὴν τινα περὶ ἄλλων πραγμάτων. τοῦ δὲ πορευέσθαι μέλλοντος κρυφαίως αὐτοῦ εἰς τὸ τῶν ὑποδημάτων πέλμα ἐντεθῆτω εἰς τὸ μεταξὺ βιβλίον καὶ καταραπτέσθω· πρὸς δὲ τοὺς πηλοὺς καὶ τὰ ὕδατα εἰς κασσίτερον ἐληλασμένον γραφέσθω πρὸς τὸ μὴ ἀφανίζεσθαι ὑπὸ τῶν ὑδάτων τὰ γράμματα. ἀφικομένου δὲ πρὸς ὃν δεῖ καὶ ἀναπαυομένου νυκτὸς ἀναλῦτω τὰς ῥαφὰς τῶν ὑποδημάτων καὶ ἐξελὼν ἀναγνοὺς τε καὶ ἄλλα γράμματα λάθρα ἀποστελλέτω τὸν ἄνδρα, ἀνταποστείλας καὶ δοὺς τι φέρειν φανερωῶς· οὕτως γὰρ οὔτε ἄλλος οὔτε ὁ φέρων εἰδήσει.

Ἀστράγαλον εὐμεγέθη δεῖ σε τρυπῆσαι τρυπήματα κδ', ἐξ εἰς ἐκάστην πλευρὰν τοῦ ἀστραγάλου· ἔστω δὲ τὰ τρυπήματα στοιχεῖα. διαμνημόνευε δὲ ἀφ' ἧς ἂν πλευρᾷς ἄρξηται τὸ ἄλφα καὶ τὰ ἐχόμενα ἅπερ ἐν ἐκάστη πλευρᾷ γέγραπται. μετὰ δὲ ταῦτα ὅταν τινὰ θέλῃς ἐν αὐτῷ τίθεσθαι, λίνῳ δῆσαι. διαιροῦντα δὲ δηλοῦν ἐν τῇ τοῦ λίνου διέρσει, ἀρξάμενος ἐκ τῆς πλευρᾷς τοῦ ἀστραγάλου, ἐν ᾗ τὸ ἄλφα ἐστί, παρελθὼν

τὰ ἐχόμενα τούτου γράμματα, ὅταν ἔλθῃς εἰς πλευρὰν οὗ τὸ ἰῶτα γράμμα ἐστί, δίειρον καὶ πάλιν παρῆς τὰ ἐχόμενα, ὅπου τὸ νῦ εἶναι συμβαίνει δίειρον, καὶ οὕτως τὰ τοῦ λόγου ἀντιγραφεῖν ἂν εἰς τὰ τρυπήματα. δεῖσεται δὲ τὸν ἀναγινώσκοντα ἀναγράφεσθαι εἰς δέλτον τὰ δηλούμενα γράμματα ἐκ τῶν τρυπημάτων, ἀνάπαλιν γινομένης τῆς ἐξέρσεως τῇ ἐνέρσει. Ἐπέμφθη γράμματά ποτε πολλάκις κατ' Ἡπειρον οὕτως χρησαμένων αὐτῶν. κυνὶ δεσμὸν τεθεικότες περὶ τὸν αὐχένα ἐνέβαλον τοῦ ἱμάντος ἔσωθεν ἐπιστολὴν, εἴτα νυκτὸς τοῦτον ἀφῆκαν ἢ μεθ' ἡμέραν πρὸς ὃν ἐξ ἀνάγκης ἤμελλεν ἦξειν, ὅθεν ἀπηνέχθη. ἔστι δὲ τοῦτο Θετταλόν. Ἄλλοι τινὲς εἰς βιβλίον γράψαντες ὡς λεπτότατον μακροὺς στίχους καὶ λεπτὰ γράμματα, ἵνα εὐογκότατα γένηται, εἴτα ἐπὶ τοῦ ὤμου τοῦ χιτωνίσκου ὑποθέντες καὶ ἀποπτύξαντες, ἀνύποπτον ἐποιοῦν τὴν κομιδὴν τῆς ἐπιστολῆς. Ἄλλοι πάλιν ἐν τῷ τῆς δέλτου ξύλῳ γράψαντες κηρὸν ἐπέτηξαν καὶ ἄλλα εἰς τὸν κηρὸν ἔγραψαν. εἴτα ὅταν ἔλθῃ παρ' ὃν δεῖ τὸν κηρὸν ἐκκνήσας καὶ ἀναγνοὺς ὁμοιοτρόπως ἀνταπέστειλεν. ἐγὼ δὲ τὰς παραγινομένας δέλτους εὐθὺς ἀνοίγειν παραινῶ, διότι τὰ εἰσπεμπόμενα μετὰ ἐπιβουλῆς πάννυ χαλεπὸν φυλάξαι (Julius Africanus, *Kestoi*, 51-53)

Those who employ traitors must know how they should send in messages. Dispatch them, then, like this. Let a man be sent openly bearing some message about other matters. Let the letter be inserted without the knowledge of the bearer in the sole of his sandals and be sewed in, and, to guard against mud and water, have it written on beaten tin so that the writing will not be effaced by the water. And when he reaches the one intended and goes to rest for the night, this person should pull out the stitches of the sandals, take out and read the letter, and, writing another secretly, let him send the man back, having dispatched some reply and having given him something to carry openly. For in this way no one else, not even the messenger, will know the message. In a sufficiently large astragal you must bore twenty-four holes, six on each side. Let the holes stand for letters, and note clearly on which side begins Alpha and which of the following letters have been written on each particular side. Then whenever you wish to make some communication by means of it, tie a thread to it. And you are to make clear your differentiation between the letters by the drawing through of the thread, beginning from the side of the astragal on which Alpha is found, omitting the characters placed next to Alpha when you come to the side where the letter Iota is marked, pass the thread through, and again, disregarding the characters following this, pass the thread through where Nu happens to be, and thus the elements of the word would be indicated in the holes. And it will be necessary for the one who is to read the information to write down upon a tablet the characters revealed by the holes, the unthreading taking place in the reverse order to that of the threading. Letters were often sent in Epirus by the employment of the following method. After getting a collar around a dog's neck, they placed inside the strap a letter; then at night or during the daytime they dispatched the dog to the person to whom he was sure to go, that is, to the one from whom he had been brought. And this is a Thessalian custom. Certain others, by writing long lines with fine characters upon some very thin papyrus, so that they may be as compact as possible, then by placing it on the shoulder under the over-tunic and spreading that out, have caused the letter to be transmitted without suspicion. Others, again, after writing on the wooden part of the tablet, have poured wax over it and written something else on the wax. Then when it came to the appointed person, he, scraping off the wax and reading the writing, sent back a reply in a similar manner. And I advise that letters be opened as soon as received, because it is very difficult to guard against anything sent in by artifice.

17: Justin (*Epitome of the Philippic History of Pompeius Trogus*, 2nd century CE)

Xerxes bellum a patre coeptum aduersus Graeciam per quinquennium instruxit. Quod ubi primum didicit Demaratus, rex Lacedaemoniorum, qui apud Xerxen exulabat, amicior patriae post fugam, quam regi post beneficia, ne inopinato bello opprimerentur omnia in tabellis ligneis magistratibus perscribit easdemque cera superinducta delet, ne aut scriptura sine tegmine iudicium daret aut recens cera dolum proderet, fido deinde seruo perferendas tradit iusso magistratibus Spartanorum tradere. Quibus perlatis, Lacedaemone quaestioni res diu fuit, quod neque scriptum aliquid uiderent nec frustra missas suspicarentur, tantoque rem maiorem, quanto esset occultior putabant. Haerentibus in coniectura uiris, soror regis Leonidae consilium scribentis inuenit. Erasa igitur cera, belli consilia deteguntur (Justin, *Epitome of the Philippic History of Pompeius Trogus*, 2.10.12-17; see also Aeneas Tacticus, *How to Survive Under Siege*, 31.14)

Xerxes [...] proceeded, during five years, with his preparations for the war against Greece, which his father had commenced. As soon as Demaratus, king of the Lacedaemonians, who was then an exile at the court of Xerxes, understood his intentions, he, feeling more regard for his country, notwithstanding his banishment, than for the king in return for his favours, sent full intelligence of the matter to the magistrates of the Lacedaemonians, that they might not be surprised by an unexpected attack; writing the account on wooden tablets, and hiding the writing with wax spread over it; taking care, however, not merely that writing without a cover might not give proof against him, but that too fresh wax might not betray the contrivance. These tablets he committed to a trusty slave, who was ordered to deliver them into the hands of the authorities at Sparta. When they were received, the object of them was long a matter of inquiry, because the magistrates could see nothing written on them, and yet could not imagine that they were sent to no purpose; and they thought the matter must be momentous in proportion to its mysteriousness. While the men were still engaged in conjecture, the sister of king Leonidas surmised the writer's intention. The wax being accordingly scraped off, the account of the warlike preparations appeared.

Inter haec Karthaginienses tanto successu rerum Alexandri Magni exterriti, verentes, ne Persico regno et Africum vellet adiungere, mittunt ad speculandos eius animos Hamilcarem cognomento Rodanum, virum sollertia facundiaque ceteros insignem. Augebant enim metum et Tyros, urbs auctorum originis suae, capta et Alexandria aemula Karthaginis in terminis Africae et Aegypti condita et felicitas regis, apud quem nec cupiditas nec fortuna ullo modo terminabantur. Igitur Hamilcar per Parmeniona aditu regis obtento profugisse se ad regem expulsum patria fingit militemque se expeditionis offert. Atque ita consiliis eius exploratis in tabellis ligneis vacua desuper cera inducta civibus suis omnia perscribebat. Sed Karthaginienses post mortem regis reversum in patriam, quasi urbem regi venditasset, non ingrato tantum, verum etiam crudeli animo necaverunt (Justin, *Epitome of the Philippic History of Pompeius Trogus*, 21.6; see also Aulus Gellius, *Attic Nights*, 17.9.16-17)

During these proceedings, the Carthaginians, alarmed at the rapid successes of Alexander the Great, and fearing that he might resolve to annex Africa to his Persian empire, sent Hamilcar, surnamed Rhodanus, a man remarkable for wit and eloquence beyond others, to sound his intentions; for, indeed, the capture of Tyre, their own parent city, and the founding of Alexandria, as a rival to Carthage, on the confines of Africa and Egypt, as well as the good fortune of the king, whose ambition and success seemed to know no limit, raised their apprehensions to an extreme height. Hamilcar, obtaining access to the king through the favour of Parmenio, represented himself to Alexander as having been banished from his country, and as having fled to him for refuge, offering, at the same time, to serve as a soldier in the expedition against Carthage. Having thus ascertained his views, he sent a full account of them to his countrymen, inscribed on wooden tablets, with blank wax spread over the writing. The Carthaginians, however, when he returned home after the death of Alexander, put him to death, not only ungratefully but cruelly, on pretence that he had offered to sell their city to the king.

18: Ovid (43 BCE-17/18 CE)

18.1: *Amores*

Cum premet ille torum, vultu comes ipsa modesto

Ibis, ut accumbas – clam mihi tange pedem!

Me specta nutusque meos vultumque loquacem;

Excipe furtivas et refer ipsa notas.

Verba superciliis sine voce loquentia dicam;

Verba leges digitis, verba notata mero.⁴³⁴

Cum tibi succurret Veneris lascivia nostrae,⁴³⁵

Purpureas tenero pollice tange genas.

Siquid erit, de me tacita quod mente queraris,

Pendeat extrema mollis ab aure manus.⁴³⁶

Cum tibi, quae faciam, mea lux, dicamve, placebunt,⁴³⁷

Versetur digitis anulus usque tuis.

Tange manu mensam, tangunt quo more precantes,

Optabis merito cum mala multa viro (Ovid, *Amores*, 1.4.15-28)

When he shall press the couch,

You will come yourself with modest mien to recline beside him –

In secret give my foot a touch.

⁴³⁴ See also Pliny, *Natural History*, 11.45.

⁴³⁵ Ovid could have been influenced by Sappho here (Fragments, 31.9f). As Ovid will be, Sappho was suffering the pain of seeing a beloved in the company of someone else, and Ovid mentions blushing in the pentameter.

⁴³⁶ See also Macrobius, *Saturnalia*, 3.11.5.

⁴³⁷ See also Petronius, *Satyricon*, 64.

Keep your eyes on me, to get my nods and the language of my eyes;
And catch my stealthy signs, and yourself return them.

With my brows I shall say to you words that speak without sound;
You will read words from my fingers you will read words traced in wine.

When you think of the wanton delights of our love,
Touch you rosy cheeks with tender finger.

If you have in mind some silent grievance against me,
Let your hand gently hold to the lowest part of your ear.

When what I do or what I say shall please you, light of mine,
Keep turning the ring about your finger.

Lay your hand upon the table as those who place their hands in prayer,
When you wish your husband as many ills as he deserves.

Cum surges abitura domum, surgemus et omnes,
In medium turbae fac memor agmen eas.

Agmine me invenies aut invenieris in illo:

Quidquid ibi poteris tangere, tange, mei (Ovid, *Amores*, 1.4.55-58)

When you rise to go home, and all the rest of us rise,
Remember to lose yourself in the midst of the crowd.
You will find me there in that crowd, or will be found by me.
Lay hand on whatever of me you can touch there.

Multa supercilio vidi vibrante loquentes;
Nutibus in vestris pars bona vocis erat.

Non oculi tacuere tui, conscriptaque vino

Mensa, nec in digits littera nulla fuit.

Sermonem agnovi, quod non videatur, agentem

Verbaque pro certis iussa valere notis (Ovid, *Amores*, 2.5.15-20)

I saw you both say many things with quiverings of the brow;
In your nods was much of speech.
Your eyes, too, girl, were not dumb, and the table was written o'er with wine,
Nor did any letter fail your fingers.
Your speech too, I recognised was busied with hidden message
And your words charged to stand for certain meanings.

Candida seu tacito vidit me femina vultu,

In vultu tacitas arguis esse notas (Ovid, *Amores*, 2.7.5-6)

Or if a fair beauty has looked on me with unspeaking face,
You charge that in her face were unspoken signals.

ego, ut arcanas possim signare tabellas,
Neve tenax ceram siccaque gemma trahat,
Umida formosae tangam prius ora puellae –
Tantum ne signem scripta dolenda mihi (Ovid, *Amores*, 2.15.15-18)

To help her seal her secret missives, and to keep the dry,
Clinging gem from drawing away the wax,
I should first touch the moist lips of my beautiful love –
Only so that I sealed no missive that would bring me pain.

Quid iuvenum tacitos inter convivia nutus
Verbaque conpositis dissimulata notis? (Ovid, *Amores*, 3.11a.23-24)

Why tell of the silent nods of young lovers at the banquet board,
And of words concealed in the signal agreed upon?

18.2: *Ars Amatoria*

Nos venerem tutam concessaque furta canemus,
Inque meo nullum carmine crimen erit (Ovid, *Ars Amatoria*, 1.33-34)

Of safe love-making do I sing, and permitted secrecy,
and in my verse shall be no wrong-doing.

Illic invenies quod ames, quod ludere possis, [...] (Ovid, *Ars Amatoria*, 1.91)

There will you find an object for passion or for deception, [...]

neque te prodet communi noxia culpa,
Factaque erunt dominae dictaque nota tibi.
Sed bene celetur: bene si celabitur index,
Notitae suberit semper amica tua (Ovid, *Ars Amatoria*, 1.395-398)

sharing a common guilt, she will not betray you,
you will know her mistress' words and deeds.
But keep her secret well; if the informer's secret be well kept,
she will always gladly foster your intimacy.

eat et blandis peraretur littera verbis,

Exploretque animos, primaque temptet iter.

Littera Cydippen pomo perlata fefellit,

Insciaque est verbis capta puella suis (Ovid, *Ars Amatoria*, 1.455-458).

Let a letter speed, traced with persuasive words,

And explore her feelings, and be the first to try the path.

A letter carried in an apple betrayed Cydippe,

And the maid was deceived unawares by her own words.

sive illa toro resupina feretur.

Lecticam dominae dissimulanter adi,

Neve aliquis verbis odiosas offerat auris,

Qua potes ambiguus callidus abde notis (Ovid, *Ars Amatoria*, 1.487-490)

Whether she be borne reclining on her cushions,

Approach your mistress' litter in dissembling fashion,

And lest someone intrude hateful ears to your words, hide them,

So far as you may, in cunning ambiguities.

Hic tibi multa licet sermone latentia tecto

Dicere quae dici sentiat illa sibi:

Blanditiasque leves tenui perscribere vino,

Ut dominam in mensa se legat illa tuam:

Atque oculos oculis spectare fatentibus ignem:

Saepe tacens vocem verbaque vultus habet.

Fac primus rapias illius tacta labellis

Pocula quaque bibet parte puella bibas:

Et quemcumque cibum digitis libaverit illa,

Tu pete dumque petis sit tibi tacta manus.

Sint etiam tua vota, viro placuisse puellae:

Utilior vobis factus amicus erit (Ovid, *Ars Amatoria*, 1.569-580)

Here may you say many things lurking in covered speech,

So that she may feel they are said to her,

And you may trace light flatteries in thin characters of wine,

That on the table she may read herself your mistress;

You may gaze at her eyes with eyes that confess their flame:

There are often voice and words in a silent look.

See that you are the first to seize the cup her lips have touched,
And drink at that part where she has drunk;
And whatever food she has touched with her fingers see that you ask for,
And while you ask contrive to touch her hand.
Let it also be your aim to please your lady's husband;
He will be more useful to you, if made a friend.

Ebrietas ut vera nocet sic ficta iuvabit:

Fac titubet blaeso subdola lingua sono,
Ut quicquid facias dicasve portarius aequo,
Credatur nimum causa fuisse merum (Ovid, *Ars Amatoria*, 1.597-600)

As real drunkenness does harm, so will feigned bring profit:
make your crafty tongue stumble in stammering talk,
So that, whatever you do or say more freely than you should,
May be put down to too much wine.

Ille levi virga (virgam nam forte tenebat)

Quod rogat in spisso litore pingit opus.
"Haec" inquit "Troia est" (muros in litore fecit):
"Hic tibi sit Simios; haec mea castra puta.
Campus erat" (campumque facit), "quem caede Dolonis
Sparsimus, Haemonios dum vigil optat equos.

Illic Sithonii fuerant tentoria Rhesi:

Hac ego sum captis nocte revectus equis"
Pluraque pingebat subitus cum Pergama fluctus
Abstulit et Rhesi cum duce castra suo (Ovid, *Ars Amatoria*, 2.131-140)

He with a light staff (for by chance he carried a staff)
Draws in the deep sand the tale of which she asks.
'Here', says he 'is Troy' (he made walls upon the beach),
'And here, suppose, is Simios; imagine this to be my camp.
There was a plain' (and he draws a plain) 'which we sprinkled with
Dolon's blood, while he watched and yearned for the Haemonian steeds.
There were the tents of Sithonian Rhesus;
On that night I rode back on the captured horses.'
More was he portraying, when a sudden wave washed Pergamus away,
And the camp of Rhesus with its chief.

Si tibi per tutum planumque negabitur ire,
Atque erit opposita ianua fulta sera,
At tu per praeceps tecto delabere aperto:
Det quoque furtivas alta fenestra vias (Ovid, *Ars Amatoria*, 2.243-246)

If it is denied you to go by a safe and easy road,
And if the door be held by a fastened bolt,
Yet slip down headlong through an opening in the roof;
Or let a high window afford a secret path.

Si latet ars prodest adfert deprensna pudorem,
Atque adimit merito tempus in omne fidem (Ovid, *Ars Amatoria*, 2.313-314)
Art, if hidden, avails; if detected, it brings shame,
And deservedly discredits you for ever.

quotiens scribes totas prius ipse tabellas
Inspice: plus multae quam sibi missa legunt (Ovid, *Ars Amatoria*, 2.394-396)
whenever you write, examine the whole letter first yourself;
Many read more than the message sent to them.

Quae bene celaris, siqua tamen acta patebunt,
Illa, licet pateant, tu tamen usque nega (Ovid, *Ars Amatoria*, 2.409-410)
Should what you have well concealed be yet somehow made manifest,
Manifest though it be yet deny it ever.

Qui modo celabas monitu tua criminal nostro,
Flecte iter, et monitu detege furta meo (Ovid, *Ars Amatoria*, 2.427-428)
You who were but now concealing your fault by my advice,
turn your path, and by my advice uncover your deceit.

Hoc vetiti; vos este vetat deprensa Dione
Insidias illas, quas tulit ipsa, dare.
Nec vos rivali laqueos disponite, nec vos
Excipite arcana verba notate manu (Ovid, *Ars Amatoria*, 2.593-596)

Be warned of this; Dione's detection warns you not
To set those snares that she endured.
Devise no toils for your rival,
Nor lie in wait for letters written in a secret hand.

Nos etiam verso parce profitemur amores,
Tectaque sunt solida mystica furta fide (Ovid, *Ars Amatoria*, 2.639-640)

As for me I recount even true amours but sparely
And a solid secrecy hides my dark intrigues.

quamvis vittae careatis honore,
Est vobis vestros fallere cura viros,
Ancillae puerique manu perarate tabellas,
Pignora nec iuveni credite vestra novo.
Perfidius ille quidem, qui talia pignora servat,
Sed tamen Aetnaei fulminis instar habent.
Vidi ego pallentes isto terrore puellas
Servitium miseras tempus in omne pati.
Iudice me fraus est concessa repellere fraudem,
Armaque in armatos sumere iura sinunt.
Ducere consuescat multas manus una figuras,
(A! pereant per quos ista monenda mihi)
Nec nisi deletis tutum rescribere ceris,
Ne teneat geminas una tabella manus (Ovid, *Ars Amatoria*, 3.483-498)

though you lack the honour of the fillet,
You too have your lords you are eager to deceive,
Write your messages by the hand of slave or handmaid,
And entrust not your pledges to a youth you now not.
Perfidious indeed is he who keeps such pledges,
But they hold what is like a thunderbolt of Aetna.
I have seen women pale with terror on that account,
Suffering in their misery unending servitude.
In my judgment fraud may be repelled by fraud
And the laws allow arms to be taken against an armed foe.
Let one hand be accustomed to tracing many figures,
(Ah perish they who make this counsel needful)
Nor is it safe to write an answer unless the wax is quite smoothed over,
Lest one tablet hold two hands.

Scilicet obstabit custos, ne scribere possis,
 Sumendae detur cum tibi tempus aquae?
 Conscia cum possit scriptas portare tabellas,
 Quas tegat in tepido fascia lata sinu?
 Cum possit sura chartas celare ligatas,
 Et vincto blandas sub pede ferre notas?
 Caverit haec custos, pro charta conscia tergum
 Praebeat, inque suo corpore verba ferat.
 Tuta quoque est fallitque oculos e lacte recenti
 Littera: carbonis pulvere tange, leges
 Fallet et umiduli quae fiet acumine lini,
 Un ferat occultas pura tabella notas (Ovid, *Ars Amatoria*, 3.619-630)

Will a guardian forsooth prevent your writing,
 When time is allowed you for taking a bath?
 When a confidant can carry a written tablet,
 Concealed by a broad band on her warm bosom?
 When she can hide a paper packet in her stocking
 And bear your coaxing message 'twixt foot and sandal?
 Should the guardian beware of this,
 Let the confidant offer her back for our note,
 And bear your words upon her body.
 A letter too is safe and escapes the eye, when written in new milk:
 Touch it with coal-dust and you will read.
 That too will deceive which is written with a stalk of moistened flax,
 So that a pure sheet may bear hidden marks.

18.3: *Heroides*

Atque aliquis posita monstrat fera proelia mensa,
 Pingit et exiguo Pergama tota mero:
 'Hac ibat Simois; haec est Sigeia tellus;
 Hic steterat Priami regia celsa senis.
 illic Aeacides, illic tendebat Ulixes
 hic lacer admissos terruit Hector equos (Ovid, *Heroides*, 1.31-36)

And someone about the board shows thereon the fierce combat,
 And with scant tracing of wine pictures forth all Pergamum:
 'Here flowed the Simois; this is the Sigeian land;
 here stood the lofty palace of Priam the ancient.

Yonder tented the son of Aeacus yonder, Ulysses

Here, in wild course went the frightened steeds with Hector's mutilated corpse'

quid epistula lecta nocebit?

Te quoque in hac aliquid quod iuvet esse potest;

His arcana notis terra pelagoque feruntur (Ovid, *Heroides*, 4.3-5)

What shall reading of a letter harm?

In this one, too, there may be something to pleasure you;

In these characters of mine, secrets are borne over land and sea.

19: Philo of Byzantium (*Compendium of Mechanics* (Μεγανίκε συνταχίς)), 3rd century BCE)

chalcantho[...], spongia in illo madefacta, postquam ea deteras fuerint litterae apparebunt. (Philo of Byzantium, *Compendium of Mechanics*, D.80 (102.40–44))

[Use gallnuts] dissolved in water to write [...], and then use a sponge soaked in vitriol rubbed gently over the writing to reveal the letters.

20: Pliny the Elder (*Natural History*, 77-79 CE)

Tithymallum nostri herbam lactariam vocant, alii lactucam caprinam, narrantque lacte eius inscripto corpore, cum inaruerit, si cinis inspargatur, apparere litteras, et ita quidam adulteras adloqui maluerunt quam codicillis (Pliny the Elder, *Natural History*, 26.39 (62)).

Tithymalus is called “milky plant” by us Romans, sometimes “goat lettuce.” It is said that, if letters are traced on the body with its milk and then allowed to dry, on being sprinkled with ash the letters become visible. And it is by this means, rather than by a letter, that some lovers have preferred to address unfaithful wives.

21: Plutarch (late 1st/early 2nd century CE)

21.1: *Life of Agesilaus*

καθ' ὁδὸν ὦν σκυτάλην δέχεται παρὰ τῶν οἴκοι τελεῶν κελεύουσιν αὐτὸν ἄρχειν ἅμα καὶ τοῦ ναυτικοῦ. τοῦτο μόνον πάντων ὑπῆρξεν Ἀγησιλάῳ (Plutarch, *Life of Agesilaus*, 10.5)

On the road he [Agesilaus] received a dispatch-roll [*scytale*] from the magistrates at home, which bade him assume control of the navy as well as of the army. This was an honour which no one ever received but Agesilaus.

Ἀλέξανδρος δὲ καὶ προσεπέσκωψε πυθόμενος τὴν πρὸς Ἄγιν Ἀντιπάτρου μάχην, εἰπὼν· “Ἔοικεν, ὦ ἄνδρες, ὅτε Δαρεῖον ἡμεῖς ἐνικῶμεν ἐνταῦθα, ἐκεῖ τις ἐν Ἀρκαδίᾳ γεγὼς Ἀλέξανδρος δὲ καὶ ονέναι μυομαχία.” πῶς οὐκ ἦν ἄξιον τὴν Σπάρτην μακαρίσαι τῆς Ἀγησιλάου τιμῆς πρὸς ταύτην καὶ πρὸς τοὺς νόμους τῆς εὐλαβείας; ὅς ἅμα τῷ τὴν σκυτάλην ἐλθεῖν εὐτυχίαν τοσαύτην καὶ δύναμιν παροῦσαν καὶ τηλικαύτας ἐλπίδας ὑφηγουμένας ἀφείς καὶ προέμενος εὐθὺς ἀπέπλευσεν “ἀτελευτήτῳ ἐπὶ ἔργῳ,” πολλὸν ἑαυτοῦ πόθον τοῖς συμμάχοις ἀπολιπὼν, καὶ μάλιστα δὴ τὸν Ἑρασιστράτου τοῦ Φαίακος ἐλέγξας λόγον, εἰπόντος ὥς εἰσὶ δημοσίᾳ μὲν Λακεδαιμόνιοι βελτίονες, ἰδίᾳ δὲ Ἀθηναῖοι (Plutarch, *Life of Agesilaus*, 15.4-6)

Alexander [the Great] actually went so far as to jest when he heard of Antipater's battle with Agis, saying: "It would seem, my men, that while we were conquering Darius here, there has been a battle of mice there in Arcadia." Why, then, should we not call Sparta happy in the honour paid to her by Agesilaus, and in his deference to her laws? No sooner had the dispatch-roll [*scytale*] come to him than he renounced and abandoned the great good fortune and power already in his grasp, and the great hopes which beckoned him on, and at once sailed off, "with task all unfulfilled," leaving behind a great yearning for him among his allies, and giving the strongest confutation to the saying of Erasistratus the son of Phaeax, who declared that the Lacedaemonians were better men in public life, but the Athenians in private.

21.2: *Life of Alcibiades*

τέλος δὲ Κριτίας ἐδίδασκε Λύσανδρον ὥς Ἀθηναίων οὐκ ἔστι δημοκρατουμένων ἀσφαλῶς ἄρχειν Λακεδαιμονίοις τῆς Ἑλλάδος· Ἀθηναίους δέ, κἂν πρῶς πάνν καὶ καλῶς πρὸς ὀλιγαρχίαν ἔχωσιν, οὐκ ἐάσει ζῶν Ἀλκιβιάδης ἀτρεμεῖν ἐπὶ τῶν καθεστώτων. οὐ μὴν ἐπέισθη γε πρότερον τούτοις ὁ Λύσανδρος ἢ παρὰ τῶν οἴκοι τελῶν σκυτάλην ἐλθεῖν κελεύουσιν ἐκ ποδῶν ποιήσασθαι τὸν Ἀλκιβιάδην, εἴτε κἀκείνων φοβηθέντων τὴν ὀξύτητα καὶ μεγαλοπραγμοσύνην τοῦ ἀνδρός, εἴτε τῷ Ἁγίδι χαριζομένων (Plutarch, *Life of Alcibiades*, 38)

Critias tried to make it clear to Lysander that as long as Athens was a democracy the Lacedaemonians could not have safe rule over Hellas; and that Athens, even though she were very peacefully and well disposed towards oligarchy, would not be suffered, while Alcibiades was alive, to remain undisturbed in her present condition. However, Lysander was not persuaded by these arguments until a dispatch-roll [*scytale*] came from the authorities at home bidding him put Alcibiades out of the way; either because they too were alarmed at the vigour and enterprise of the man, or because they were trying to gratify Agis.

21.3: *Life of Artaxerxes*

ὕχ ἦττον οὖν τοῖς ἄνω πιστεύων ὁ Κῦρος ἢ τοῖς. περὶ αὐτόν, ἐπεχείρει τῷ πολέμῳ· καὶ Λακεδαιμονίοις ἔγραφε, παρακαλῶν βοηθεῖν καὶ συνεκπέμπειν ἄνδρας, οἷς ἔφη δώσειν, ἂν μὲν πεζοὶ παρῶσιν, ἵππους, ἂν δ' ἵππεις, συνωρίδας· ἐὰν δ' ἀγροὺς ἔχωσι, κώμας· ἐὰν δὲ κώμας, πόλεις· μισθοῦ δὲ τοῖς

στρατευομένοις οὐκ ἀριθμόν, ἀλλὰ μέτρον ἔσεσθαι. μεγαληγορῶν δὲ περὶ αὐτοῦ πολλά, καὶ καρδίαν ἔφη τοῦ ἀδελφοῦ φορεῖν βαρυτέραν, καὶ φιλοσοφεῖν μᾶλλον, καὶ μαγεύειν βέλτιον, οἶνον δὲ πλείονα πίνειν καὶ φέρειν· ἐκεῖνον δ' ὑπὸ δειλίας καὶ μαλακίας ἐν μὲν τοῖς κυνηγεσίῳις μὴδ' ἐφ' ἵππου, ἐν δὲ τοῖς κινδύνῳις μὴδ' ἐπὶ τοῦ θρόνου καθῆσθαι. Λακεδαιμόνιοι μὲν οὖν σκυτάλην πρὸς Κλέαρχον ἀπέστειλαν, ὑπηρετεῖν Κύρῳ πάντα κελεύοντες. ὁ δὲ Κύρος ἀνέβαινεν ἐπὶ βασιλέα, βαρβαρικὴν τε πολλὴν ἔχων δύναμιν καὶ μισθοφόρους Ἑλληνας ὀλίγῳ τρισχιλίων καὶ μυρίων ἀποδέοντας, ἄλλας ἐπ' ἄλλαις ποιούμενος. προφάσεις τῆς στρατείας. οὐ μὴν ἔλαθέ γ' εἰς πολὺν χρόνον, ἀλλ' ἦκε βασιλεῖ Τισσαφέρνης αὐτάγγελος, καὶ πολὺς θόρυβος εἶχε τὰ βασιλεία, τῆς τε Παρυσάτιδος τὴν πλείστην αἰτίαν τοῦ πολέμου φερομένης, καὶ τῶν φίλων. αὐτῆς ἐν ὑποψίαις ὄντων καὶ διαβολαῖς (Plutarch, *Life of Artaxerxes*, 6.2-5)

Cyrus relied quite as much upon the people of the interior as upon those of his own province and command, when he began the war. He also wrote to the Lacedaemonians, inviting them to aid him and send him men, and promising that he would give to those who came, if they were footmen, horses; if they were horsemen, chariots and pairs; if they had farms, he would give them villages; if they had villages, cities; and the pay of the soldiers should not be counted, but measured out. Moreover, along with much high-sounding talk about himself, he said he carried a sturdier heart than his brother, was more of a philosopher, better versed in the wisdom of the Magi, and could drink and carry more wine than he. His brother [Artaxerxes], he said, was too effeminate and cowardly either to sit his horse in a hunt, or his throne in a time of peril. The Lacedaemonians, accordingly, sent a dispatch-roll [*scytale*] to [their general] Clearchus ordering him to give Cyrus every assistance. So Cyrus marched up against the king with a large force of Barbarians and nearly thirteen thousand Greek mercenaries, alleging one pretext after another for his expedition. But the real object of it was not long concealed, for Tissaphernes [a Persian general and statesmen] went in person to the king and informed him of it. Then there was a great commotion at the court, Parysatis [Cyrus's mother] being most blamed for the war, and her friends undergoing suspicion and accusation.

21.4: *Life of Lysander*

ὁ δὲ Λύσανδρος [...], αὐτὸς μὲν ἐπὶ Θράκης ἐξέπλευσε, τῶν δὲ χρημάτων τὰ περιόντα καὶ ὅσας δωρεὰς αὐτὸς ἢ στεφάνους ἐδέξατο, πολλῶν, ὡς εἰκός, διδόντων ἀνδρὶ δυνατωτάτῳ καὶ τρόπον τινὰ κυρίῳ τῆς Ἑλλάδος, ἀπέστειλεν εἰς Λακεδαίμονα διὰ Γυλίππου τοῦ στρατηγήσαντος περὶ Σικελίαν. ὁ δέ, ὡς λέγεται, τὰς ῥαφὰς τῶν ἀγγείων κάτωθεν ἀναλύσας καὶ ἀφελὼν συχνὸν ἀργύριον ἐξ ἐκάστου πάλιν συνέρραπεν, ἀγνοήσας ὅτι γραμματίδιον ἐνῆν ἐκάστῳ τὸν ἀριθμὸν σημαῖνον. ἐλθὼν δὲ εἰς Σπάρτην ἃ μὲν ὑφήρητο κατέκρυπεν ὑπὸ τὸν κέραμον τῆς οἰκίας, τὰ δὲ ἀγγεῖα παρέδωκε τοῖς ἐφόροις καὶ τὰς σφραγίδας ἐπέδειξεν. ἐπεὶ δὲ ἀνοιζάντων καὶ ἀριθμούντων διεφώνει πρὸς τὰ γράμματα τὸ πλῆθος τοῦ ἀργυρίου καὶ παρεῖχε τοῖς ἐφόροις ἀπορίαν τὸ πρᾶγμα, φράζει θεράπων τοῦ Γυλίππου πρὸς αὐτοὺς αἰνιζάμενος ὑπὸ τῷ κεραμικῷ κοιτάζεσθαι πολλὰς γλαυκάς. ἦν γάρ, ὡς ἔοικε, τὸ χάραγμα τοῦ πλείστου τότε νομίσματος διὰ τοὺς Ἀθηναίους γλαυκάς. ὁ μὲν οὖν Γύλιππος αἰσχροὺς οὕτω καὶ ἀγεννὲς ἔργον ἐπὶ λαμπροῖς τοῖς ἔμπροσθεν καὶ μεγάλοις ἐργασάμενος μετέστησεν ἑαυτὸν ἐκ Λακεδαίμονος (Plutarch, *Life of Lysander*, 16-17.1)

Lysander, [...], sailed for Thrace himself, but what remained of the public moneys, together with all the gifts and crowns which he had himself received, — many people, as was natural, offering presents to a man who had the greatest power, and who was, in a manner, master of Hellas, — he sent off to Lacedaemon by Gylippus, who had held command in Sicily. But Gylippus, as it is said, ripped open the sacks at the bottom, and after taking a large amount of silver from each, sewed them up again, not knowing that there was a writing in each indicating the sum it held. And when he came to Sparta, he hid what he had stolen under the tiles of his house, but delivered the sacks to the *ephors*, and showed the seals upon them. When, however, the *ephors* opened the sacks and counted the money, its amount did not agree with the written lists, and the thing perplexed them, until a servant of Gylippus made the truth known to them by his riddle of many owls sleeping under the tiling. For most of the coinage of the time, as it seems, bore the forgery of an owl, owing to the supremacy of Athens. Gylippus, then, after adding a deed so disgraceful and ignoble as this to his previous great and brilliant achievements, removed himself from Lacedaemon.

ἐπεὶ δὲ Φαρνάβαζος ἀδικούμενος ὑπ' αὐτοῦ τὴν χώραν ἄγοντος καὶ φέροντος ἀπέστειλεν εἰς τὴν Σπάρτην κατηγοροῦς, ἀγανακτήσαντες οἱ ἔφοροι τῶν μὲν φίλων αὐτοῦ καὶ συστρατῆγων ἓνα Θώρακα λαβόντες ἀργύριον ἰδίᾳ κεκτημένον ἀπέκτειναν, ἐκεῖνῳ δὲ σκυτάλην ἔπεμψαν ἥκειν κελεύοντες (Plutarch, *Life of Lysander*, 19.4)

When Pharnabazus, who was outraged by Lysander's pillaging and wasting his territory, sent men to Sparta to denounce him, the *ephors* were incensed, and when they found Thorax, one of Lysander's friends and fellow-generals, with money in his private possession, they put him to death, and sent a dispatch-scroll [*scytale*] to Lysander, ordering him home.

ἔστι δὲ ἡ σκυτάλη τοιοῦτον. ἐπὰν ἐκπέμπωσι ναύαρχον ἢ στρατηγὸν οἱ ἔφοροι, ξύλα δύο στρογγύλα μῆκος καὶ πάχος ἀκριβῶς ἀπισώσαντες, ὥστε ταῖς τομαῖς ἐφαρμόζειν πρὸς ἄλληλα, τὸ μὲν αὐτοὶ φυλάττουσι, θάτερον δὲ τῷ πεμπομένῳ διδόασιν. ταῦτα δὲ τὰ ξύλα σκυτάλας καλοῦσιν. ὅταν οὖν ἀπόρρητόν τι καὶ μέγα φράσαι βουληθῶσι, βιβλίον ὥσπερ ἱμάντα μακρὸν καὶ στενὸν ποιοῦντες περιελίττουσι τὴν παρ' αὐτοῖς σκυτάλην, οὐδὲν διάλειμμα ποιοῦντες, ἀλλὰ πανταχόθεν κύκλῳ τὴν ἐπιφάνειαν αὐτῆς τῷ βιβλίῳ καταλαμβάνοντες. τοῦτο δὲ ποιήσαντες ἃ βούλονται καταγράφουσιν εἰς τὸ βιβλίον, ὥσπερ ἐστὶ τῇ σκυτάλῃ περικείμενον: ὅταν δὲ γράψωσιν, ἀφελόντες τὸ βιβλίον ἄνευ τοῦ ξύλου πρὸς τὸν στρατηγὸν ἀποστέλλουσι. δεξάμενος δὲ ἐκεῖνος ἄλλως μὲν οὐδὲν ἀναλέξασθαι δύναται τῶν γραμμάτων συναφὴν οὐκ ἔχοντων, ἀλλὰ διεσπασμένων, τὴν δὲ παρ' αὐτῷ σκυτάλην λαβὼν τὸ τμήμα τοῦ βιβλίου περὶ αὐτὴν περιέτεινεν, ὥστε, τῆς ἑλικος εἰς τάξιν ὁμοίως ἀποκαθισταμένης, ἐπιβάλλοντα τοῖς πρώτοις τὰ δεῦτερα, κύκλῳ τὴν ὅσιν ἐπάγειν τὸ συνεχὲς ἀνευρίσκουσιν. καλεῖται δὲ ὁμωνύμως τῷ ξύλῳ σκυτάλη τὸ βιβλίον, ὡς τῷ μετροῦντι τὸ μετρούμενον (Plutarch, *Life of Lysander*, 19.5-7)

The dispatch-scroll [the *scytale*] is of the following character. When the *ephors* send out an admiral or a general, they make two round pieces of wood exactly alike in length and thickness, so that each

corresponds to the other in its dimensions, and keep one themselves, while they give the other to their envoy. These pieces of wood they call "*scytalae*". Whenever, then, they [the *ephors* of Sparta] wish to send some secret and important message, they make a scroll [...], long and narrow, like a leathern strap, and wind it round their "*scytale*," leaving no vacant space thereon, but covering its surface all round with the parchment. After doing this, they write what they wish on the parchment, just as it lies wrapped about the "*scytale*"; and when they have written their message, they take the parchment off, and send it, without the piece of wood, to the commander. He, when he has received it, cannot otherwise get any meaning of it, — since the letters have no connection, but are disarranged, — unless he takes his own "*scytale*" and winds the strip of parchment about it, so that, when its spiral course is restored perfectly, and that which follows is joined to that which precedes, he reads around the staff, and so discovers the continuity of the message. And the parchment, like the staff, is called "*scytale*," as the thing measured bears the name of the measure

ὁ [...] Λύσανδρος, ἐλθούσης τῆς σκυτάλης πρὸς αὐτὸν εἰς τὸν Ἑλλήσποντον, διαταράχθη, καὶ μάλιστα τὰς τοῦ Φαρναβάζου δεδιὼς κατηγορίας, ἐσπούδασεν εἰς λόγους αὐτῷ συνελθεῖν, ὥς λύσων τὴν διαφοράν. καὶ συνελθὼν ἐδεῖτο γράψαι περὶ αὐτοῦ πρὸς τοὺς ἄρχοντας ἑτέραν ἐπιστολὴν ὥς οὐδὲν ἡδικημένον οὐδ' ἐγκαλοῦντα. πρὸς Κρήτα δὲ ἄρα, τὸ τοῦ λόγου, κρητίζων ἠγνόει τὸν Φαρνάβαζον. ὑποσχόμενος γὰρ ἅπαντα ποιήσῃ, φανερώς μὲν ἔγραψεν οἷαν ὁ Λύσανδρος ἤξιωσεν ἐπιστολὴν, κρύφα δὲ εἶχεν ἑτέραν αὐτόθι γεγραμμένην. ἐν δὲ τῷ τὰς σφραγίδας ἐπιβάλλειν ἐναλλάξας τὰ βιβλία μηδὲν διαφέροντα τῇ ὄψει, δίδωσιν ἐκείνην αὐτῷ τὴν κρύφα γεγραμμένην. ἀφικόμενος οὖν ὁ Λύσανδρος εἰς Λακεδαίμονα καὶ πορευθεὶς, ὥσπερ ἔθος ἐστίν, εἰς τὸ ἀρχεῖον, ἀπέδωκε τοῖς ἐφόροις τὰ γράμματα τοῦ Φαρναβάζου, πεπεισμένος ἀνηρῆσθαι τὸ μέγιστον αὐτοῦ τῶν ἐγκλημάτων: ἠγαπᾶτο γὰρ ὁ Φαρνάβαζος ὑπὸ τῶν Λακεδαιμονίων, προθυμότατος ἐν τῷ πολέμῳ τῶν βασιλέως στρατηγῶν γεγενημένος. ἐπεὶ δὲ ἀναγνόντες οἱ ἔφοροι τὴν ἐπιστολὴν ἔδειξαν αὐτῷ, καὶ συνῆκεν ὥς - οὐκ ἄρ' Ὀδυσσεύς ἐστιν αἰμύλος μόνος (Plutarch, *Life of Lysander*, 20)

Lysander, when the dispatch-scroll [*scytale*] reached him at the Hellespont, was much disturbed, and since he feared the denunciations of Pharnabazus above all others, he hastened to hold a conference with him, hoping to compose their quarrel. At this conference he begged Pharnabazus to write another letter about him to the magistrates, stating that he had not been wronged at all, and had no complaints to make. But in thus "playing the Cretan against a Cretan," as the saying is, he misjudged his opponent. For Pharnabazus, after promising to do all that he desired, openly wrote such a letter as Lysander demanded, but secretly kept another by him ready written. And when it came to putting on the seals, he exchanged the documents, which looked exactly alike, and gave him the letter which had been secretly written. Accordingly, when Lysander arrived at Sparta and went, as the custom is, into the senate-house, he gave the *ephors* the letter of Pharnabazus, convinced that the greatest of the complaints against him was thus removed; for Pharnabazus was in high favour with the Lacedaemonians, because he had been, of all the

King's generals, most ready to help them in the war. But when the *ephors*, after reading the letter, showed it to him, and he understood that: "Odysseus, then, is not the only man of guile"⁴³⁸

22: Polyaeus (*Stratagems of War*, second half 2nd century CE)

Ἰστιαῖος Μιλήσιος ἐν Πέρσαις διὰ γων παρά Δαρείῳ βασιλεῖ βουλόμενος Ἰωνίαν ἀποστήσαι γράμματα πέμπειν οὐ θαρρῶν διὰ τοὺς φύλακας τῶν ὁδῶν οἰκέτην πιστὸν ἀποξύρας τὰς τρίχας στίγματα ἐνέγραψατο τῇ κεφαλῇ ‘Ἰστιαῖος’ Ἀρισταγόρα Ἰωνίαν ἀπόστησον καὶ τοῖς στίγμασιν ἐπέθρεψε τὰς τρίχας. τοῦτον τὸν τρόπον λαθῶν τοὺς φύλακας ὁ στιγματοφόρος καταβὰς ἐπὶ θάλατταν ἀποξοθράμενος ἔδειξεν Ἀρισταγόρα τὰ στίγματα. ὁ δὲ ἀναγνοὺς ἀπέστησεν τὴν Ἰωνίαν (Polyaenus, *Stratagems of War*, 1.24; see also Herodotus, *Histories*, 5.35; Aeneas Tacticus, *How to Survive Under Siege*, 31.8-29; Aulus Gellius, *Attic Nights*, 17.9.18-27)

Whilst Histiaeus, the Miletian, resided at the court of King Darius, in Persia, he formed the design of engaging the Ionians to revolt; but was at a loss how safely to transmit a letter, the way being every where possessed by the king's guard. Shaving the head of a confidential servant, in incisions of it he thus briefly wrote: 'Histiaeus to Aristagoras, solicit the revolt of Ionia.' And as soon as his [the slave's] hair had grown again, he dispatched him to Aristagoras. By this means he passed the guards unsuspected; and, after bathing in the sea, ordered himself to be shaved, and then shewed Aristagoras the marks: which, when he had read, he prosecuted the design, and affected the revolt of Ionia.

Δημάρατος ἐπιστέλλων Σπαρτιάταις περὶ τῆς Χέρξου στρατείας ἐς πύχλα ἀκέρωτον τὴν ἐπιστολὴν γράψας ἐπεκλήρωσεν, ἵνα ὡς ἄγραφος διὰ τῶν φυλάκων κοιμισθῇ (Polyaenus, *Stratagems of War*, 2.20; see also Aeneas Tacticus, *How to Survive Under Siege*, 31.14).

The intelligence, which Demaratus communicated to the Lacedaemonians, concerning Xerxes' army, he engraved on a tablet; which he afterwards covered with wax; that if intercepted, no characters might appear.

Καρχηδόνιοι Σικελίαν πορτοῦντες ὅπως αὐτοῖς ἀπὸ λιβύης διὰ τάχους τὰ ἀναγκαῖα κομίζοιτο, κλεψύδρας δύο ποιήσαντες ἴσας τοῖς μεγέθεσι, κύκλους ἐν ἑκατέρᾳ διέγραψαν ἴσους ἔχοντας τὴν αὐτὴν ἐπιγραφὴν. Ἐπεγέγραπτο δὲ οὗ μὲν χρεῖα νεῶν οὗ δὲ στρογγύλον πλοίων, ἀλλαχοῦ δὲ χρυσίου, καὶ πάλιν σίτου καὶ πάλιν ἀλλαχοῦ μηχανεμάτων καὶ πάλιν σίτου καὶ πάλιν θηρίων καὶ πάλιν ὄπλων καὶ πεζῶν καὶ ἵππῶν. Οὗτο δὴ πάντας τοὺς κύκλους ἐπιγράψαντες, τὴν ἐτέραν τῶν κλεψυδρῶν ἐν Σικελίᾳ κατασχόντες [τὴν ἐτέραν] ἐξέπεμψαν εἰς Καρχηδόνα συντάξαντες, ἣν ἴδοσιν ἀρθέντα πυγρὸν γὰρ αὐτῶν ἀποσκοπεῖν ὅταν ὁ δεῦτερος ἀναδειχθῇ πυρσὸς, ποίου κύκλου τοῦτο συμβήσεται οὗ τὴν ἐπιγραφὴν ἀναγνόντας ὅτι τάχος

⁴³⁸ The text 'Odysseus, then, is not the only man of guile' is an iambic trimeter of some unknown poet (Perrin 1916, 288-289).

τὸ σημαινόμενον διὰ τῶν γραμμάτων ἐκπέμπειν. Τοῦτον τὸν τρόπον ὁξυτάτην εἶχον Καρχηδόνιοι τὴν κομιδὴν τῶν εἰς τὸν πόλεμον ἀναγκαίων (Polyaenus, *Stratagems of War*, 6.16.2; see also Polybius, *The Histories*, 10.43-46)

When the Carthaginians had invaded Sicily, in order to be supplied from Libya with provisions and naval stores in the most expeditious manner, they made two hour glasses exactly of the same description, and drew around each of them an equal number of circles. One of those circles they engraved "A want of ships of war", on another "A want of store-ships", on another "A want of gold", on another "Of machines", on another again "Of corn", on another "Of cattle"; "Of arms"; "Of infantry"; and "Of cavalry". The circles in this manner all filled up, one of these hour glasses the forces kept with them in Sicily; and sent the other to Carthage: directing the Carthaginians, when they saw the second torch raised, to send the particulars described in the second circle; when the third, those in the third circle; and so on. By this means they received a steady supply of whatever they wanted.

Φαρνάβαζος κατὰ Λυσάνδρου Λακεδαιμονίοις ἔγραψεν. Οἱ δὲ ἀπὸ τῆς Ἀσίας αὐτόν ἀνεκαλέσαντο σκυτάλην πέμπσαντες. Λύσανδρος ἰκετεῦει Φαρνάβαζον ἄλλην ἐπιστολὴν ὑπὲρ αὐτοῦ γράψαι φυλάνθρωπου. Φαρνάβαζος ὑποχόμενος φανερώς μὲν ἔγραψεν οἷαν ὁ Λυσάνδρος ἤξιωσε, κρύφα δὲ εἶχεν ἑτέραν γεγραμμένην, ἐν δὲ τῷ τὴν σφραγίδα ἐπιβάλλειν ὑπαλλάξας τὰ βιβλία μηδὲν διαφέροντα τῇ ὄψει δίδωσιν αὐτῷ τὴν κρύφα γεγραμμένην. Λυσάνδρος ἐπανελθὼν ἐς Λακεδαίμονα τοῖς ἐφόροις κατὰ τὸ ἔθος ἀπέδωκε τὰ γράμματα, οἱ δὲ ἀναγνόντες ἔδειξαν αὐτῷ τὴν ἐπιστολὴν προειπόντες μηδὲν ἀπολογίας δεῖσθαι αὐτὸν καθ' αὐτοῦ ἐπιστολὴν κομίσαντα (Polyaenus, *Stratagems of War*, 7.19)

Pharnabazus, having preferred charges of misdemeanor against Lysander, the Lacedaemonians sent him letters [*scytalae*] to recall from Asia. When Lysander importuned him to be less severe on his representation of his conduct; Pharnabazus promised he would; and addressed a letter to the Lacedaemonians of the purport Lysander desired. But at the same time, he privately wrote another letter, giving a very different account. In sealing the letter, he contrived to slip that which he had privately written, and which was in shape exactly the same with that Lysander had derived his letter to the *Ephori*; which as soon as they had read, they shewed him; observing at the same time that there was no room for any defence, the very letter, which he himself produced, concerning him.

23: Polybius (*The Histories*, 2nd century BCE)

Τοῦ δὲ κατὰ τὰς πυρσείας γένους, μεγίστας δὴ παρεχομένου χρείας ἐν τοῖς πολεμικοῖς, ἀνεργάστου πρότερον ὑπάρχοντος, χρήσιμον εἶναί μοι δοκεῖ τὸ μὴ παραδραμεῖν, ἀλλὰ ποιήσασθαι περὶ αὐτοῦ τὴν ἀρμόζουσαν μνήμην. ὅτι μὲν οὖν ὁ καιρὸς ἐν πᾶσι μεγάλῃν ἔχει μερίδα πρὸς τὰς ἐπιβολάς, μεγίστην δ' ἐν τοῖς πολεμικοῖς, παντὶ δῆλον· τῶν δὲ πρὸς τοῦτο συναγωνισμάτων πλείστην ἔχουσι δύναμιν οἱ πυρσοί. <δηλοῦσι γὰρ> τίνα μὲν ἄρτι γέγονε, τίνα δ' ἀκμὴν ἐνεργεῖται, καὶ δυνατόν ἐστι γινώσκειν, ᾧ μέλει, ποτὲ μὲν ἡμερῶν τριῶν ἢ τεττάρων ὁδὸν ἀπέχοντι, ποτὲ δὲ καὶ πλειόνων. ὥστ' αἰεὶ τοῖς δεομένοις πράγμασιν ἐπικουρίας παράδοξον γίνεσθαι τὴν βοήθειαν διὰ τῆς τῶν πυρσῶν ἀπαγγελίας. τὸν μὲν <οὖν> πρὸ τούτου

χρόνον ἀπλῆς γινομένης τῆς πυρσείας κατὰ τὸ πλεῖστον αὐτὴν ἀνωφελῆ συνέβαινε γίνεσθαι τοῖς χρωμένοις. διὰ γὰρ συνθημάτων ὀρισμένων ἔδει τὴν χρεῖαν συντελεῖν· τῶν δὲ πραγμάτων ἀορίστων ὑπαρχόντων τὰ πλεῖστα διέφυγε τὴν τῶν πυρσῶν χρεῖαν, οἷον ἐπ' αὐτῶν τῶν νῦν εἰρημένων. ὅτι μὲν οὖν εἰς Ὀρεὸν καὶ Πεπάρηθον ἢ Χαλκίδα πάρεστι στόλος, δυνατόν ἦν διασαφεῖν τοῖς περὶ τούτου συνθεμένοις· ὅτι δὲ μεταβάλλονται τινες τῶν πολιτῶν ἢ προδιδόασιν, ἢ φόνος ἐν τῇ πόλει γέγονεν, ἢ τι τῶν τοιούτων, ἃ δὴ συμβαίνει μὲν πολλάκις, πρόληψιν δ' ἔχειν πάντων ἀδύνατον—μάλιστα δὲ τὰ παραδόξως γινόμενα τῆς ἐκ τοῦ καιροῦ συμβουλίας καὶ ἐπικουρίας προσδεῖται—τὰ τοιαῦτα πάντα διέφυγε τὴν τῶν πυρσῶν χρεῖαν. περὶ ὧν γὰρ οὐκ ἐνεδέχετο προνοηθῆναι, περὶ τούτων οὐδὲ σύνθημα ποιήσασθαι δυνατόν (Polybius, *The Histories*, 10.43)

I think that as regards the system of signalling by fire, which is now of the greatest possible service in war but was formerly undeveloped, it will be of use not to pass it over but to give it a proper discussion. It is evident to all that in every matter, and especially in warfare, the power of acting at the right time contributes very much to the success of enterprises, and fire signals are the most efficient of all the devices which aid us to do this. For they show what has recently occurred and what is still in the course of being done, and by means of them anyone who cares to do so even if he is at a distance of three, four, or even more days' journey can be informed. So that it is always surprising how help can be brought by means of fire messages when the situation requires it. Now in former times, as fire signals were simple beacons, they were for the most part of little use to those who used them. For the service had to be performed by signals previously determined upon, and as facts are indefinite, most of them defied communication by fire signals. To take the case I just mentioned, it was possible for those who had agreed on this to convey information that a fleet had arrived at Oreus, Peparethus, or Chalcis, but when it came to some of the citizens having changed sides or having been guilty of treachery or a massacre having taken place in the town, or anything of the kind, things that often happen, but cannot all be foreseen—and it is chiefly unexpected occurrences which require instant consideration and help—all such matters defied communication by fire signal. For it was quite impossible to have a preconcerted code for things which there was no means of foretelling.

Αἰνείας [...] βουλευθεὶς διορθώσασθαι τὴν τοιαύτην ἀπορίαν, ὃ τὰ περὶ τῶν Στρατηγικῶν ὑπομνήματα συντεταγμένος, βραχὺ μὲν τι προεβίβασε, τοῦ γε μὴν δέοντος ἀκμὴν ἀμύλου τὸ κατὰ τὴν ἐπίνοιαν ἀπελείφθη. γνοίη δ' ἂν τις ἐκ τούτων. φησὶ γὰρ δεῖν τοὺς μέλλοντας ἀλλήλοις διὰ τῶν πυρσῶν δηλοῦν τὸ κατεπεῖγον ἀγγεῖα κατασκευάσαι κεραμεῖ, κατὰ τε τὸ πλάτος καὶ κατὰ τὸ βάθος ἰσομεγέθη πρὸς ἀκρίβειαν· εἶναι δὲ μάλιστα τὸ μὲν βάθος τριῶν πηχῶν, τὸ δὲ πλάτος πήχεος. εἶτα παρασκευάσαι φελλοὺς βραχὺ κατὰ πλάτος ἐνδεεῖς τῶν στομάτων, ἐν δὲ τούτοις μέσοις ἐμπεπηγένοι βακτηρίας διηρημένους εἰς ἴσα μέρη τριδᾶκτυλα, καθ' ἕκαστον δὲ μέρος εἶναι περιγραφὴν εὐσημον. ἐν ἐκάστῳ δὲ μέρει γεγράφθαι τὰ προφανέστατα καὶ καθολικώτατα τῶν ἐν τοῖς πολεμικοῖς συμβαινόντων, οἷον εὐθέως ἐν τῷ πρώτῳ, διότι "πάρεισιν ἱππεῖς εἰς τὴν χώραν," ἐν δὲ τῷ δευτέρῳ διότι "πεζοὶ βαρεῖς," ἐν δὲ τῷ τρίτῳ "ψιλοί," τούτων δ' ἐξῆς "πεζοὶ μεθ' ἱππέων," εἶτα "πλοῖα," μετὰ δὲ ταῦτα "σῖτος," καὶ κατὰ τὸ συνεχὲς οὕτω, μέχρις ἂν ἐν πάσαις γραφαῖ ταῖς χώραις τὰ μάλιστ' ἂν ἐκ τῶν εὐλόγων προνοίας τυγχάνοντα καὶ συμβαίνοντα κατὰ τοὺς ἐνεστῶτας καιροὺς ἐκ τῶν πολεμικῶν. τούτων δὲ γενομένων ἀμφοτέρα κελεύει

τρήσαι τὰ ἀγγεῖα πρὸς ἀκρίβειαν, ὥστε τοὺς αὐλίσκους εἶναι καὶ κατ' ἴσον ἀπορρεῖν: εἴτα πληρώσαντας ὕδατος ἐπιθεῖναι τοὺς φελλοὺς ἔχοντας τὰς βακτηρίας, κᾶπειτα τοὺς αὐλίσκους ἀφεῖναι ῥεῖν ἅμα. τούτου δὲ συμβαίνοντος δῆλον ὡς ἀνάγκη πάντων ἴσων καὶ ὁμοίων ὄντων, καθ' ὅσον ἂν ἀπορρέῃ τὸ ὑγρὸν, κατὰ τοσοῦτον τοὺς φελλοὺς καταβαίνειν καὶ τὰς βακτηρίας κρύπτεσθαι κατὰ τῶν ἀγγείων. ὅταν δὲ τὰ προειρημένα γένηται κατὰ τὸν χειρισμὸν ἰσοταχῇ καὶ σύμφωνα, τότε κομίσαντας ἐπὶ τοὺς τόπους, ἐν οἷς ἑκάτεροι μέλλουσι συντηρεῖν τὰς πυρσεῖας, ἑκάτερον θεῖναι τῶν ἀγγείων. εἴτ' ἐπὶ ἐμπέσῃ τι τῶν ἐν τῇ βακτηρίᾳ γεγραμμένων, πυρσὸν ἄραι κελεύει, καὶ μένειν, ἕως ἂν ἀνταίρωσιν οἱ συντεταγμένοι: γενομένων δὲ φανερῶν ἀμφοτέρων ἅμα τῶν πυρσῶν καθελεῖν. εἴτ' εὐθέως ἀφεῖναι τοὺς αὐλίσκους ῥεῖν. ὅταν δὲ καταβαίνοντος τοῦ φελλοῦ καὶ τῆς βακτηρίας ἔλθῃ τῶν γεγραμμένων ὁ βούλει δηλοῦν κατὰ τὸ χεῖλος τοῦ τεύχους, ἄραι κελεύει τὸν πυρσόν: τοὺς δ' ἑτέρους ἐπιλαβεῖν εὐθέως τὸν αὐλίσκον, καὶ σκοπεῖν τί κατὰ τὸ χεῖλός ἐστι τῶν ἐν τῇ βακτηρίᾳ γεγραμμένων: ἔσται δὲ τοῦτο τὸ δηλούμενον πάντων ἰσοταχῶς παρ' (Polybius, *The Histories*, 10.44)

Aeneas, [...] the writer of the treatise on tactics, wished to correct this defect, and did in fact make some improvement; but his invention still fell very far short of what was wanted, as the following passage from his treatise will show. "Let those who wish," he says, "to communicate any matter of pressing importance to each other by fire-signals prepare two earthenware vessels of exactly equal size both as to diameter and depth. Let the depth be three cubits, the diameter one. Then prepare corks of a little shorter diameter than that of the vessels: and in the middle of these corks fix rods divided into equal portions of three fingers' breadth, and let each of these portions be marked with a clearly distinguishable line: and in each let there be written one of the most obvious and universal of those events which occur in war; for instance in the first 'cavalry have entered the country,' in the second 'hoplites,' in the third 'light-armed,' in the next 'infantry and cavalry,' in another 'ships,' in another 'corn,' and so on, until all the portions have written on them the events which may reasonably be expected to occur in the particular war. Then carefully pierce both the vessels in such a way that the taps shall be exactly equal and carry off the same amount of water. Fill the vessels with water and lay the corks with their rods upon its surface, and set both taps running together. This being done, it is evident that if there is perfect equality in every respect between them, both corks will sink exactly in proportion as the water runs away, and both rods will disappear to the same extent into the vessels. When they have been tested, and the rate of the discharge of water has been found to be exactly equal in both, then the vessels should be taken respectively to the two places from which the two parties intend to watch for fire signals. As soon as any one of those eventualities which are inscribed upon the rods takes place, raise a lighted torch, and wait until the signal is answered by a torch from the others: this being raised, both parties are to set the taps running together. When the cork and rod on the signalling side has sunk low enough to bring the ring containing the words which give the desired information on a level with the rim of the vessel, a torch is to be raised again. Those on the receiving side are then at once to stop the tap, and to look at the words in the ring of the rod which is on a level with the rim of their vessel. This will be the same as that on the signalling side, assuming everything to be done at the same speed on both sides"

ταῦτα δὲ βραχὺ μὲν τι τῆς διὰ τῶν συνθημάτων πυρσείας ἐξήλλαχεν, ἀκμὴν δ' ἐστὶν ἀόριστα. δῆλον γὰρ [ἔσται] ὥς οὔτε προῖδέσθαι τὰ μέλλοντα πάντα δυνατὸν οὔτε προῖδόμενον εἰς τὴν βακτηρίαν γράψαι: λοιπὸν ὁπόταν ἐκ τῶν καιρῶν ἀνυπονόητά τινα συμβαίνει, φανερὸν ὥς οὐ δύναται δηλοῦσθαι κατὰ ταύτην τὴν ἐπίνοιαν. καὶ μὴν οὐδ' αὐτῶν τῶν ἐν τῇ βακτηρίᾳ γεγραμμένων οὐδέν ἐστιν ὀρισμένον. πόσοι γὰρ ἤκουσιν ἱππεῖς ἢ πόσοι πεζοὶ καὶ ποῦ τῆς χώρας καὶ πόσαι νῆες καὶ πόσος σῖτος, οὐχ οἷόν τε διασαφῆσαι: περὶ γὰρ ὧν ἀδύνατον γινῶναι πρὶν ἢ γενέσθαι, περὶ τούτων οὐδὲ συνθέσθαι πρὸ τοῦ δυνατὸν. τὸ δὲ συνέχον ἐστὶ τοῦτο: πῶς γὰρ ἂν τις βουλεύσαιτο περὶ τοῦ βοηθεῖν μὴ γινώσκων πόσοι πάρεισι τῶν πολεμίων ἢ ποῦ; πῶς δὲ θαρρήσαι πάλιν ἢ τοῦναντίον ἢ καθόλου διανοηθεῖν τι μὴ συνεῖς πόσαι νῆες ἢ πόσος σῖτος ἤκει παρὰ τῶν συμμάχων· (Polybius, *The Histories*, 10.45.1-5)

[Aeneas' method] is a slight advance on beacons with a preconcerted code, but it is still quite indefinite. For it is evident that it is neither possible to foresee all contingencies, or even if one did to write them all on the rod. So that when circumstances produce some unexpected event, it is evident that it cannot be conveyed by this plan. Again none of the things written on the rod are defined statements, for it is impossible to indicate how many infantry are coming and to what part of the country, or how many ships or how much corn. For it is impossible to agree beforehand about things of which one cannot be aware before they happen. And this is the vital matter; for how can anyone consider how to render assistance if he does not know how many of the enemy have arrived, or where? And how can anyone be of good cheer or the reverse, or in fact think of anything at all, if he does not understand how many ships or how much corn has arrived from the allies?

τὸ τῶν στοιχείων πλῆθος ἐξῆς δεῖ λαμβάνοντας διελεῖν εἰς πέντε μέρη κατὰ πέντε γράμματα. λείπει δὲ τὸ τελευταῖον ἐνὶ στοιχείῳ: τοῦτο δ' οὐ βλέπτει πρὸς τὴν χρεῖαν. μετὰ δὲ ταῦτα πλατεῖα παρεσκευάσθαι πέντε τοὺς μέλλοντας ἀποδιδόναι τὴν πυρσεῖαν ἀλλήλοις ἑκατέρους καὶ γράψαι τῶν μερῶν ἐξῆς εἰς ἕκαστον πλατεῖον, κάπειτα συνθέσθαι πρὸς αὐτοὺς διότι τοὺς μὲν πρώτους ἀρεῖ πυρσοὺς ὁ μέλλων σημαίνειν ἅμα καὶ δύο καὶ μενεῖ μέχρις ἂν ὁ ἕτερος ἀνταίρη. τοῦτο δ' ἔσται χάριν τοῦ διὰ ταύτης τῆς πυρσείας ἑαυτοῖς ἀνθομολογήσασθαι διότι πρωσοέχουσι. καθαιρεθέντων δὲ τούτων λοιπὸν ὁ σημαίνων ἀρεῖ μὲν τοὺς πρώτους ἐκ τῶν εὐωνύμων, διασαφῶν τὸ πλατεῖον ποῖον δεήσει σκοπεῖν, οἷον ἂν μὲν τὸ πρῶτον, ἔν', ἂν δὲ τὸ δεύτερον, δύο, καὶ κατὰ λόγον οὕτω: τοὺς δὲ δευτέρους ἐκ τῶν δεξιῶν κατὰ τὸν αὐτὸν λόγον, ποῖον δεήσει γράμμα τῶν ἐκ τοῦ πλατείου γράφειν αὖ τὸν ἀποδεχόμενον τὴν πυρσεῖαν. (Polybius, *The Histories*, 10.45.6-12).

We take the alphabet and divide it into five parts, each consisting of five letters. There is one letter less in the last division, but this makes no practical difference. Each of the two parties who are about to signal to each other must now get ready five tablets and write one division of the alphabet on each tablet, and then come to an agreement that the man who is going to signal is in the first place to raise two torches and wait until the other replies by doing the same. This is for the purpose of conveying to each other that they are both at attention. These torches having been lowered the dispatcher of the message will now raise the first set of torches on the left side indicating which tablet is to be consulted, *i.e.* one torch if it

is the first, two if it is the second, and so on. Next he will raise the second set on the right on the same principle to indicate what letter of the tablet the receiver should write down.

24: Porphyry of Tyre (*Life of Pythagoras*, 3rd century CE)

ἐν Αἰγύπτῳ μὲν τοῖς ἱερεῦσι συνὴν καὶ τὴν σοφίαν ἐζέμαθε καὶ τὴν Αἰγυπτίων φωνήν. γραμμάτων δὲ τρισσὰς διαφορὰς ἐπιστολογραφικῶν τε καὶ ἱερογλυφικῶν καὶ συμβολικῶν τῶν μὲν κοινολογουμένων κατὰ μίμησιν τῶν δ' ἀλληγορονμένων κατὰ τινὰς αἰνιγμοὺς καὶ περὶ θεῶν πλέον τι ἔμαθεν (Porphyry of Tyre, *Life of Pythagoras*, 11-12)

In Egypt he [Pythagoras] lived with the priests, and learned the language and wisdom of the Egyptians, and their three kinds of letters, the epistolographic, the hieroglyphic, and symbolic, whereof one [the epistolographic way] imitates the common way of speaking, while the others [the hieroglyphic and symbolic ways] express the sense of allegory and parable.

25: Suetonius (*Life of the Caesars: Lives of the Caesars* 1 and 2. *The Deified Julius* (1) and *The Deified Augustus* (2), 121 BCE)

Exstant et ad Ciceronem, item ad familiares domesticis de rebus, in quibus, si qua occultius perferenda erant, per notas scripsit, id est sic structo litterarum ordine, ut nullum verbum effici posset; quae si qui investigare et persequi velit, quartam elementorum litteram, id est D pro A et perinde reliquas commutet (Suetonius, *Life of the Caesars* 1. *The Deified Julius*, 56.6)

There are [...] letters of his [Caesar] to Cicero, as well as to his intimates on private affairs, and in the latter, if he had anything confidential to say, he wrote it in cipher, that is, by so changing the order of the letters of the alphabet that not a word could be made out. If anyone wishes to decipher these, and get at their meaning, he must substitute the fourth letter of the alphabet, namely D, for A, and so with the others.

Orthographiam, id est formulam rationemque scribendi a grammaticis institutam, non adeo custodit ac videtur eorum potius sequi opinionem, qui perinde scribendum ac loquamur existiment. Nam quod saepe non litteras modo sed syllabas aut permutat aut praeterit, communis hominum error est. Nec ego id notare, nisi mihi mirum videretur tradidisse aliquos, legato eum consulari successorem dedisse ut rudi et indocto, cuius manu “ixi” pro “ipsi” scriptum animadverterit. Quotiens autem per notas scribit, B pro A, C pro B ac deinceps eadem ratione sequentis litteras ponit; pro X autem duplex A. (Suetonius, *Lives of the Caesars* 2. *The Deified Augustus*, 88)

[Augustus] does not strictly comply with orthography, that is to say the theoretical rules of spelling laid down by the grammarians, seeming to be rather of the mind of those who believe that we should spell

exactly as we pronounce. Of course his frequent transposition or omission of syllables as well as of letters are slips common to all mankind. I should not have noted this, did it not seem to me surprising that some have written that he cashiered a consular governor, as an uncultivated and ignorant fellow, because he observed that he had written *ixi* for *ipsi*.

26: Xenophon (*Hellenica*, late 5th/early 4th century BCE)

ἀκούσαντες ταῦτα οἱ ἔφοροι ἐσκεμμένα τε λέγειν ἠγήσαντο αὐτὸν καὶ ἐξεπλάγησαν, καὶ οὐδὲ τὴν μικρὰν καλουμένην ἐκκλησίαν συλλέξαντες, ἀλλὰ συλλεγόμενοι τῶν γερόντων ἄλλος ἄλλοθι ἐβουλεύσαντο πέμψαι τὸν Κινάδωνα εἰς Αὐλῶνα σὺν ἄλλοις τῶν νεωτέρων καὶ κελεῦσαι ἥκειν ἄγοντα τῶν Αὐλωνιτῶν τέ τινας καὶ τῶν εἰλώτων τοὺς ἐν τῇ σκυτάλῃ γεγραμμένους. ἀγαγεῖν δὲ ἐκέλευον καὶ τὴν γυναῖκα, ἣ καλλίστη μὲν αὐτόθι ἐλέγετο εἶναι, λυμαίνεσθαι δ' ἐφ' ἧς τοὺς ἀφικνουμένους Λακεδαιμονίων καὶ πρεσβυτέρους καὶ νεωτέρους (Xenophon, *Hellenica*, 3.3.8)

Upon hearing [...] statements the *ephors* came to the conclusion that he [an informant] was describing a well-considered plan, and were greatly alarmed; and without even convening the Little Assembly, as it was called, but merely gathering about them—one *ephor* here and another there—some of the senators, they decided to send Cinadon to Aulon along with others of the younger men, and to order him to bring back with him certain of the Aulonians and Helots whose names were written in the official dispatch [*scytale*]. And they ordered him to bring also the woman who was said to be the most beautiful woman in Aulon and was thought to be corrupting the Lacedaemonians who came there, older and younger alike.

ἀλλὰ μὴν καὶ πρὸς Ὀλυνθίους εἰδότες ὑμᾶς πόλεμον ἐκφέροντας συμμαχίαν ἐποιοῦντο, καὶ ὑμεῖς γε τότε μὲν αἰεὶ προσείχετε τὸν νοῦν πότε ἀκούσεσθε βιαζομένους αὐτοὺς τὴν Βοιωτίαν ὑφ' αὐτοῖς εἶναι: νῦν δ' ἐπεὶ τάδε πέπρακται, οὐδὲν ὑμᾶς δεῖ Θηβαίους φοβεῖσθαι: ἀλλ' ἀρκέσει ὑμῖν μικρὰ σκυτάλη ὥστ' ἐκεῖθεν πάντα ὑπηρετεῖσθαι ὅσων ἂν δέησθε, ἐὰν ὥσπερ ἡμεῖς ὑμῶν, οὕτω καὶ ὑμεῖς ἡμῶν ἐπιμελῆσθε (Xenophon, *Hellenica*, 5.2.34-35)

[Leontiades addresses the Lacedaemonians:] Again, knowing that you [the Lacedaemonians] were making war upon the Olynthians, they [the Thebans] undertook to conclude an alliance with them, and you in those past days were always uneasily watching for the time when you should hear that they were forcing Boeotia to be under their sway; but now that this stroke has been accomplished, there is no need of your fearing the Thebans; on the contrary, a brief message [*scytale*] from you will suffice to secure from that quarter all the support that you may desire, provided only you show as much concern for us as we have shown for you.

οἱ Λακεδαιμόνιοι πολὺ προθυμότερον τὴν εἰς τὴν Ὀλυνθὸν στρατιὰν συναπέστελλον. καὶ ἐκπέμπουσι Τελευτίαν μὲν ἄρμοστήν, τὴν δ' εἰς τοὺς μυρίους σύνταξιν αὐτοὶ τε ἅπαντας συνεξέπεμπον, καὶ εἰς τὰς συμμαχίδας πόλεις σκυτάλας διέπεμπον, κελεύοντες ἀκολουθεῖν Τελευτίᾳ κατὰ τὸ δόγμα τῶν συμμάχων. καὶ οἱ τε ἄλλοι προθύμως τῷ Τελευτίᾳ ὑπηρετοῦν, καὶ γὰρ οὐκ ἀχάριστος ἐδόκει εἶναι τοῖς ὑπουργοῦσί τι, καὶ ἡ τῶν Θηβαίων δὲ πόλις, ἅτε καὶ Ἀγησιλάου ὄντος αὐτῷ ἀδελφοῦ, προθύμως συνέπεμψε καὶ ὀπλίτας καὶ ἱππέας (Xenophon, *Hellenica*, 5.2.37)

The Lacedaemonians with much more spirit set about dispatching the joint army to Olynthus [after the speech of Leontiades]. They sent out Teleutias as governor, and not only sent with him their own full contingent of the total ten thousand men, but also transmitted official dispatches [scytalae] to the various allied states, directing them to follow Teleutias in accordance with the resolution of the allies. And all the states gave their hearty support to Teleutias, — for he was regarded as a man not ungrateful to those who performed any service, — while the Theban state in particular, inasmuch as he was a brother of Agesilaus, eagerly sent with him both hoplites and horsemen.

Appendix 2: Medieval, Renaissance, and modern sources on cryptography and steganography referring back to Greco-Roman sources

1: Leon Battista Alberti (*De Componendis Cifris*, 1466-1467)

Prius de indice mobili. Sit verbi gratia inter nos constitutus index ex mobili tabella k. Statuam tabellam formulae uti quidem scribenti mihi libuerit, puta ut k ipsa statuta sub maiuscula B et sequens sub sequenti. Ad te igitur scribens primam omnium scribam B maiusculam sub qua indicem k in formula scripturus posuerim; id indicabit ut id quoque tu in provincia volens nostra legere, formulam quae apud te gemella est versionibus aptes usque sub B itidem sit index ipse k. Hinc demum caeterae omnes litterae minores in epistola inventae superiorum stabilium vim et sonos significabunt. Cum autem tres quattuorve dictiones exscripsero mutabo nostra in formula situm indicis versione circuli, ut sit index ipse k fortassis sub R. Ergo in epistola inscribam maiusculam R inde igitur k significabit non amplius B sed R et quae sequentur singulae superiorum stabilium novissima suscipient significata. Tu idem in provincia interlegendum admonitus inventa maiuscula eam scies nihil aliud importare ex se nisi ut moneat mobilis circuli situm atque indicis collocationem isthic esse immutatam. Ergo tu quoque sub ea indicem collocabis, eo pacto facillime cuncta perleges et perdisces. Caeterum altera illa indicis constitutio, quae fiat ex maiusculis, est ut constet inter nos ex maiuscularum ipsarum numero quatenam earum index sit; atque esto sit mihi tecum index constitutus B. Prima omnium in epistola quam ad te scribam erit littera ex minoribus quae libuerit, puta q; eam igitur conversione tabellarum in formula locabis sub ipsa indice B. Hinc fiet ut ipsa q significet sonetque B. Demum in caeteris sequemur descriptione, uti de superiori mobili diximus indice. Cum autem erit immutanda cifrae tabella et formulae habitus, tum inscribam loco in epistola unicam non plures ex litteris numeralibus, hoc est ex his quae sub numeris aderunt constitutae minoris quae significet puta 3 aut 4 et eiusmodi. Hancque ipsam inversione tabellarum substituam indici B constituto atque deinceps prout scribendi ratio postulabit, prosequar minusculis litteris maiorum significata perscribens. Hic etiam quo magis atque magis scrutatores fallas, poteris cum amico constituere ad quem scripturus sis ut maiusculae interpositae (quae alioquin nullae interponentur) nihil important et similia pleraque poteris quae longum et supervacuum est prosequi. Itaque cuiusque maiusculae sonos et vox quattuor (ut vides) et viginti formis litterarum poterit indicari et contra minuscularum quaeque litterarum viginti poterit maiorum significata et amplius quattuor numerales dicere indicis et circuli inversione et positione variata. Venio ad numeralium usum, quo nihil admirabilius. Venio ad numeralium usum, quo nihil admirabilius. Numerales litterae sunt, uti dixi, minusculae, quae supra se scriptos in tabella stabili numeros significant. Numerales quidem de se praestant ut duabus tribusve quattuorve in unum ordinem adiunctis trecentae atque sex et triginta significari possint integrae orationes ad arbitrium. Nam ex his numeralibus litteris iunctis binatim ut puta ps quae 12 fortasse significant et pf quae fortassis 13 significabunt et eiusmodi iunctionibus (quaequidem ex his quattuor numeralibus fieri binatim possunt) orationes indicabuntur usque sexdecim. Sin autem numerales eadem litterae ternatim iungentur puta psp quae fortassis 123 significant et sfp quae 231 significant, tunc quidem dabitur ut orationes possis

explicare usque sexaginta et quattuor. Si demum quaternatim uti sfkp, quae significant 2341 aut fpsk quae significant 3124 et eiusmodi iungentur litterae, dabuntur tunc ex earum adiunctionibus uti orationes explicentur integrae adusque 256. Itaque harum omnium summa habebitur orationum integrarum 336. Atqui istarum quidem usus veniet hunc in modum. Nam seorsum componemus tabulam linearum 336, in qua ordinibus explicabimus singulas quae fieri possunt numeralium istiusmodi adiunctiones, easque apponemus capitibus litterarum, sic, nam ad primam quidem lineam erit 11, ad secundam 12, ad tertiam 13, ad quartam 14, ad quintam 21, ad sextam 22, ad septimam 23, et deinceps reliqua ut in ea tabula infra subnotavimus. Hinc tabulae ex constituto singulis lineis ad suos numeros adscribemus singulas quas libuerit integras orationes, puta post numerum 12: “Naves quas polliciti sumus milite frumentoque refertas paravimus”. Similes igitur quibusque istorum numerorum in tabula adscribemus ad arbitrium animi orationes integras. Istius meae tabulae sit exemplar apud te necesse est, tu igitur in provincia cum ad te meae pervenerint litterae et in epistola offenderis litteras numerales, notabis quos indicent numeros, spectabis ex tabula isthac integrarum orationum atque inde perdisces quid sit quod scripserim; quo scribendi commento nihil brevius, nihil tutius, nihil ad cyfrarum usum excogitari aptius accommodatiusve potest, duabus tribusve aut usque quattuor litteris, at his quidem non semper eisdem sed variis trecentas et sex atque triginta explicari orationes integras et diversas posse, quis non admiretur? Et fortassis conferet duas habere tabulas numerales apud me et duas aequae tales apud te, in quarum alteris ordine positi, uti exposuimus, numeri ex principiis versuum sese legenti promptissimum exhibeant; in alteris vero tabulis ad ordinem alphabeti positae sint orationes sub litterarum titulis quo illic quidem non diffusius quaerendae ex tabula orationes sint et promptius scribenti suppeditentur. Tituli orationum erunt habendi sic: nam quae orationes ad annonam facient, ponentur sub titulo A, quae ad bellum administrandum sub <titulo> B, quae ad naves sub <titulo> N et istiusmodi reliqua. Atqui different quidem inter se tabulae isthaec numerales, quod in illis cuiusque versus principium significabitur numeris, post sequentur orationes; in his vero alteris numeri non in principio versuum sed littera titulo consona adscribetur, post sequetur oratio, in fine autem aderunt numeri prout eisdem ipsis orationibus in altera parili tabula istiusmodi orationum fuerant perscripti. Scripturus ergo ad te quam instituerim orationem eam ex tabula disquiro qua inventa sub litterarum titulo cui supposita est, specto ex fine numeros annotatos. Hos ea re ipse ex formula cyfrae nostris litteris illic eos numeros significantibus pono in epistola. Tu uti dixi ex numeris illico explicatas habebis orationes. Hoc opusculum velim apud amicos nostros observari ne in vulgus imperitorum prodeat et profanetur digna res principe et maximis rebus agendis dedito. (Alberti, *De Componendis Cifris*, 14-16)

First the mobile index. Say for example we have mutually established k as the index of the mobile circle. Writing, the formulae are positioned at will, say such k lies under the upper-case B and the next letter corresponds to the letter that comes next. In writing to you, I will first of all put the upper-case B under which lies the index k in the formula; this is a signal to you far away, wanting to read what I have written, that you should set up the twin formula in your keeping, positioning the mobile circle so that the B sits over the index k. Then all of the rest of the lower-case letters present in the coded text will take their meaning and sound from those of the fixed circle above them. After I have written three or four words I will mutate the position of the index in our formula, rotating the disk let's say, so that the index k falls below the upper-case R. Then in the missive I write an upper-case R to indicate that k no longer refers to

B, but to R, and the letters that follow will assume new meanings. You likewise, far away and receiving the message, have to look carefully in reading to find the upper-case letter, which you will know serves solely to indicate the positioning of the mobile circle and that the index has changed. Thus, you too will position the index under that upper-case letter, and be able to read and understand the entire text with ease. The four mobile letters that under the four houses on the fixed circle above that are marked with numbers, regardless of the values they themselves have, do not (if you will) receive any meaning, and can be inserted into the text as null letters. However, when combined or repeated, they are marvellously commodious, which I will describe below. Alternately, an index could be selected from among the upper-case letters and we could mutually agree on which would be the index; say we have determined the letter B as the index. The first letter that will appear in the missive that I write to you will be whatever lower-case letter you want, say q; the formula will be positioned so that this lies under the index B. It follows that q will take on the phonetic and semantic value of the B. Finally, we shall follow all the rest of the writing, as we said, with regard to the index of the highest mobile <circle>. When it is then necessary to modify the encoded alphabet and the positioning of the formula, then I will insert into the missive, in the proper place, one and only one of the numeral letters, that is, one of the letters of the small circle lying under the numbers that signify, say, the number 3 or 4, and so on. Rotating the mobile disk, I will make this letter correspond precisely to the agreed upon index B and, successively, as the logic of writing requires, I will go forward, assigning to the lower-case letters the value of the upper-case letters. In order to further disorient the investigators, I could also agree with my friend to whom I am writing that the interposing upper-case letters (of which without this convention there would be none) have no value, and similar other devices that it is not worthwhile listing. Thus, by positioning the index in a different way by rotating the mobile disk, it is possible to express the phonetic and semantic value of each of the upper-case letters, using (as you can see) twenty-four different alphabetic characters, while each of the lower-case letters can correspond to any upper-case letter whatsoever and also to the four numbers of the disk above. I now come to the use of the numeral letters, of which is nothing <more> admirable. The numeral letters are, as I said, the lower-case letters that correspond to the four numbers of the fixed circle above. The numbers, combined in groups of two, three or four, three hundred thirty-six whole phrases determined at will. These numeral letters, when paired, say that ps corresponds to 12 and pf to 13, and with other similar pairings that can for constructed with these four numerals, indicate sixteen phrases. If instead these same numbers are combined into groups of three, say psf signifies 123 and sfp 231, sixty-four phrases can be expressed. With combinations of four numerals, where sfkp is equivalent to 2341 or fpsk corresponds to 3124, and similar combinations, 256 whole phrases can be expressed. The total sum of whole phrases is 336. Now we shall show how these numeral letters are used. On one side we compose a table of 336 lines, in which we clearly arrange the numeral combinations at the beginning of the line, that is, in the first line there will be 11, in the second 12, in the third, 13, in the fourth 14, in the fifth 21, in the sixth 22, in the seventh 23, The Mathematical Works of Leon Battista Alberti 183 and so forth for all the rest, as in the table we show below. We ascribe to each individual line of the table, next to the corresponding number, say next to the number 12 'the promised ships have been equipped and provided with provisions'. In a similar way whole phrases with whatever contents we want are ascribed to each number combination in the table. It is necessary for you to have a copy of this table with you so that

when you who are far away receive my letter and you come across the numeral letters, noting that they signify numbers, you will consult the table that contains the predetermined phrases written there; for writing I will say that there is no invention that is quicker, more secure and nothing devised for cyphers could be more aptly suited, that two, three or four letters combined in different ways can express three hundred thirty-six phrases, isn't this wonderful? It is recommended that I have with me two numeral tables and for you to have two as well, arranged in different orders, one where we set out the numbers at the beginning of the line so that they are easy to read; in the other conversely in alphabetical order will be arranged the phrases according to the letter that forms the title so that the writer can find them quickly. The phrases will be arranged in the following way: those that regard administration of provisions (*annonam*) will appear under the initial A; those that refer to the carrying out of military operations (*bellum administrandum*) under B; those that regard ships (*naves*) under N, and so forth for the rest. The difference between the two numeral tables is that, in the first, at the beginning of the line, there appear the numbers followed by the phrases, conversely what appears at the beginning of the line is not the numbers but the initials followed by the phrases, and at the end will be the numbers that have been attributed to the phrases in the correlated table. Thus, in writing to you, I first look up the phrase that I want to use in the table, and having found it under the corresponding initial, I look at the numbers noted and using our encrypted formula, I insert the letters that signify those numbers into the missive. You, as I have said, will deduce the phrase from those numbers. I would have this little work of mine kept among our friends, not in the public domain, so as to not profane a subject worthy of sovereigns and rather for statesmen devoted to the most important of affairs.

2: Gerolamo Cardano (*De Subtilitate*, 1550)

Triplex haec est trasmutandi, quae in usa ut de Caesare olim Suetonius, velut si pro a, d, pro b, n, scribatur. Est autem infinitorem generum (Cardano, *De Subtilitate*, 17.1036)

The basis of substitution, which was in use, as Suetonius long ago wrote about Caesar, as if D is written instead of A, and N instead of B. It is of innumerable kinds.

translationis modus est, ut delitescant, in quibus da suspiciones, nota quada, ut in Laconica *scytala* [...] (Cardano, *De Subtilitate*, 17.1036)

[A] method of 'translation' exists, so that in some cases of suspicion, the marks may pass unnoticed; this is so with the Lacedaemonian cylinders [*scytalae*]

3: Isidore of Seville, *The Etymologies* (5th/6th century CE)

Caesar [...] Augustus ad filium, "quoniam" inquit, "innumerabilia accidunt assidue quae scribi alterutro oporteat et esse secreta, habeamus inter nos notas si vis tales ut, cum aliquid notis scribendum erit, pro unaquaque littera scribamus sequentem hoc modo, pro a b pro b c et deinceps eadem ratione ceteras; pro z autem littera redeundum erit ad duplex a" (Isidore of Seville, *The Etymologies*, 1.25.2)

Caesar Augustus [...] said to his son: Since innumerable things are constantly occurring about which we must write to each other, and which must be secret, let us have between us code-signs, if you will, such that, when something is to be written in code, we will replace each letter with the following letter in this way: B for A, C for B, and then the rest in the same way. For the letter Z, we will return to a double AA.

4: Photius (*Lexicon*, 9th century CE)

Σκυτάλη: ἐπιστολή Λακωνική. ἦν δὲ ἡ σκυτάλη ξύλον ἐξεσμένον ἐπίμηκες. Δύο δὲ παρὰ Λακεδαιμονίοις ὑπεχον σκυτάλαι. Καὶ τὴν μὲν μίαν κατεῖχον οἱ ἑφοροὶ τῶν Λακεδαιμονίων. Τὴν δὲ ἑτέραν τῷ ἐκπεπομένῳ παρ' αὐτῶν στρατηγῷ παρεῖχον. Καὶ ὁπότε ἐβούλοντο τι ἐπιστεῖλαι αὐτῷ, φέροντες ἱμάντα λευκὸν περιεῖλλον τὴν σκυτάλην. Καὶ ἐπὶ τοῦ ἱμάντος ἔγραφον. Καὶ ἀνελίστοντες παρεῖχον τὸν ἱμάντα τῷ ἀποφέροντι. Τοῦτο δὲ ἐποιοῦν, ἵνα μὴ μανθάωσιν οἱ ἀποφέροντες τὸ δηλούμενον ἐν αὐτῷ. Ὁ δὲ στρατηγὸς δεχόμενος τὸν ἱμάντα τῇ ἑαυτοῦ σκυτάλῃ περιεῖλιπεν. Καὶ ἀναγίνωσκεν οὕτως τὰ γεγραμμένα. Λέγεται οὖν καὶ ἡ ἐπιστολή. Διοσκουρίδης δὲ ἐν τοῖς περὶ νομίμων τοὺς δανεῖζοντας ἐν Σπάρτῃ διαιρεῖν σκυτάλην δύο παρόντων μαρτυρῶν καὶ γράφειν τὸ συμβόλαιον ἐν ἑκατέρῳ τμήματι. Καὶ τὸ μὲν ἐνὶ τῶν μαρτύρων διδόναι. Τὸ δὲ δι' ἑαυτοῦ ἔχειν. Ἐχρῶντο δ' αὐτῷ καὶ ἄλλοι. Ὡς Ἀριστοτέλης ἐν τῇ Ἰθακησίων πολιτείᾳ μῆβ (Photius, *Lexicon*, entry: σκυτάλη (II)).

Skytale: A Spartan letter. The '*skytale*' was a long shaved piece of wood. There used to be two '*skytalai*' among the Spartans. The Spartan's '*ephors*' would keep the one and would furnish the other to the general who was dispatched by them. And whenever they wished to send something to him, taking a white strap they would wrap it around the '*skytale*' and write on the strap. And unwrapping it they would furnish the strap to the man who carried [the message]. They used to do this so that those who carried [the message] might not know what was indicated in it. The general, on receiving the strap, used to wrap it around his own '*skytale*' and thus read what was written. Thus, both the letter is called a '*skytale*', and the wood itself, after which also the letter [is called] '*skytale*'. Dioscorides in On Customs [says] that lenders in Sparta divide a '*skytale*', with two witnesses being present, and write the contract on each piece. And that [a lender] gave the one to one of the witnesses but kept the other by himself. Others too used to use it, as Aristotle [says] in the *Constitution of the Ithacans*, 42.

5: Procopius of Caesarea (*Secret History*, 6th century CE)

τῶν κατασκόπων τοιαῦτά ἐστιν. ἄνδρες πολλοὶ ἐν δημοσίῳ τὸ ἀνέκαθεν ἐσιτίζοντο, οἱ δὲ ἐς τοὺς πολεμίους ἰόντες ἔν τε τοῖς Περσῶν βασιλείοις γινόμενοι ἢ ἐμπορίας ὀνόματι ἢ τρόπῳ ἐτέρῳ, ἔς τε τὸ ἀκριβὲς διερευνώμενοι ἕκαστα, ἐπανήκοντες ἐς Ῥωμαίων τὴν γῆν πάντα τοῖς ἄρχουσιν ἐπαγγέλλειν ἠδύναντο τὰ τῶν πολεμίων ἀπόρρητα. οἱ δὲ προὔμαθον ἐφύλασσόν τε καὶ ἀπρόοπτον οὐδὲν ξυνέπιπτε σφίσι. τοῦτο δὲ τὸ χρῆμα κὰν τοῖς Μήδοις ἐκ παλαιοῦ ἦν. Χοσρόης μὲν οὖν μείζους, ὥσπερ φασί, πεποιημένος τὰς τῶν κατασκόπων ξυντάξεις προμηθείας τῆς ἐνθένδε ἀπήλαυσεν. οὐδὲν γὰρ αὐτὸν [ἐλάνθανε τῶν ἐν Ῥωμαίοις γινόμενων. ὁ δὲ Ἰουστινιανὸς οὐδ' ὅτιοῦν ἀναλώσας καὶ αὐτὸ τὸ] τῶν κατασκόπων ὄνομα ἐξέτριψεν ἐκ Ῥωμαίων τῆς γῆς, ἐξ οὗ δὲ ἄλλα τε πολλὰ ἡμαρτήθη καὶ Λαζικὴ πρὸς τῶν πολεμίων ἑάλω, Ῥωμαίων οὐδαμῇ πεπυσμένων ὅποι ποτὲ γῆς ὁ Περσῶν βασιλεὺς ζῆν τῷ στρατῷ εἶη (Procopius of Caesarea, *Secret History*, 30.12-14)

The matter of the spies is as follows. Many men from ancient times were maintained by the State, men who would go into the enemy's country and get into the Palace of the Persians, either on the pretext of selling something or by some other device, and after making a thorough investigation of everything, they would return to the land of the Romans, where they were able to report all the secrets of the enemy to the magistrates. And they, furnished with this advance information, would be on their guard and nothing unforeseen would befall them. And this practice had existed among the Medes also from ancient times. Indeed Chosroes, as they say, increased the salaries of his spies and profited by this forethought. For nothing [that was happening among the Romans escaped] him. [Justinian, on the other hand, by refusing to spend anything at all on them] blotted out from the land of the Romans [even the very] name of spies, and in consequence of this action many mistakes were made and Lazica was captured by the enemy, the Romans having utterly failed to discover where in the world the Persian king and his army were.

6: Edgar Allan Poe (*A Few Words on Secret Writing*, 1841)

Were two individuals, totally unpractised in cryptography, desirous of holding by letter a correspondence which should be unintelligible to all but themselves, it is most probable that they would at once think of a peculiar alphabet, to which each should have a key. At first it would, perhaps, be arranged that a should stand for z, b for y, c for x, d for w, &c. &c.; that is to say, the order of the letters would be reversed. Upon second thoughts, this arrangement appearing too obvious, a more complex mode would be adopted. The first thirteen letters might be written beneath the last thirteen, thus:

n o p q r s t u v w x y z
a b c d e f g h i j k l m

and, so placed, a might stand for n and n for o, o for b and b for a, et cetera, et cetera. This, again, having an air of regularity which might be fathomed, the key alphabet might be constructed absolutely at random (Poe, *A Few Words on Secret Writing*, 1841, 33)

The *scytalae* were two wooden cylinders, precisely similar in all respects. The general of an army, in going upon any expedition, received from the *ephori* one of these cylinders, while the other remained in their possession. If either party had occasion to communicate with the other, a narrow strip of parchment was so wrapped around the *scytala* that the edges of the skin fitted accurately each to each. The writing was then inscribed longitudinally, and the epistle unrolled and dispatched. If, by mischance, the messenger was intercepted, the letter proved unintelligible to his captors. If he reached his destination safely, however, the party addressed had only to involve the second cylinder in the strip to decipher the inscription. The transmission to our own times of this obvious mode of cryptography is due, probably, to the historical uses of the *scytala*, rather than to anything else. Similar means of secret intercommunication must have existed almost contemporaneously with the invention of letters. It may be as well to remark, in passing, that in none of the treatises on the subject of this paper which have fallen under our cognizance, have we observed any suggestion of a method — other than those which apply alike to all ciphers — for the solution of the cipher by *scytala*. We read of instances, indeed, in which the intercepted parchments were deciphered; but we are not informed that this was ever done except accidentally. Yet a solution might be obtained with absolute certainty in this manner. The strip of skin being intercepted, let there be prepared a cone of great length comparatively — say six feet long — and whose circumference at base shall at least equal the length of the strip. Let this latter be rolled upon the cone near the base, edge to edge, as above described; then, still keeping edge to edge, and maintaining the parchment close upon the cone, let it be gradually slipped towards the apex. In this process, some of those words, syllables, or letters, whose connection is intended, will be sure to come together at that point of the cone where its diameter equals that of the *scytala* upon which the cipher was written. And as, in passing up the cone to its apex, all possible diameters are passed over, there is no chance of a failure. The circumference of the *scytala* being thus ascertained, a similar one can be made, and the cipher applied to it (Poe, *A Few Words on Secret Writing*, 1841, 33)

As we can scarcely imagine a time when there did not exist a necessity, or at least a desire, of transmitting information from one individual to another, in such manner as to elude general comprehension; so we may well suppose the practice of writing in cipher to be of great antiquity (Poe, *A Few Words on Secret Writing*, 1841, 33)

7: *Sylloge Tacticorum* (10th-century Byzantine military manual)

Caesar wrote a message about something he wanted on paper and rolled it up with wax like a torch. After he gave it to one of his spies, he sent it to his colleague who had previously revolted, offering to him, by means of this message, an amnesty for his transgressions. And so, he immediately won over his colleague (*Sylloge Tacticorum*, 76.1. Translation of original text: Charzelis & Harris 2017, 98)

8 : Charles François Toustain and René Prosper Tassin (*Nouveau traité de diplomatique*,
1750)

Sur un bande ou lanière fort étroite de cuir ou de parchemin, placée autour d'un cylindre ou d'un bâton, dont un correspondant avoit le semblable; les Lacédémoniens écrivoient les dépêches, concernant leur affaires d'Etat. Ces lanières confiées à des couriers ne formoient aucun sens aux yeux des ennemis, qui pouvoient les intercepter: parceque, pour les lire, il falloit avoir un cylindre de la même forme, qui celui dont on s'étoit servi en les écrivant. C'étoit par consequent un secret assez grossier de stéganographie, et non pas une sorte d'écriture d'usage ordinaire (Tassin & Toustain, *Nouveau traité de diplomatique* 1750, 605)

On a very narrow strip or thong of leather or parchment, placed around a cylinder or a stick [*scytale*], of which a correspondent had the like; the Lacedaemonians would write dispatches concerning their affairs of state. These lines they [then] entrusted to couriers. [The text] would make no sense in the eyes of the enemies, [if they] would intercept it; since to read [the text], it was necessary to have a cylinder [*scytale*] of the same shape, which was used when [a message was] written on [the strip]. It was therefore a rather crude [method] of steganography, and not an ordinary kind of writing.