View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by Repository@USM

A NEW APPROACH TO PUBLIC-KEY CRYPTOSYSTEM BASED ON MANDELBROT AND JULIA FRACTAL SETS

MOHAMMAD AHMAD A. ALIA

UNIVERSITI SAINS MALAYSIA

2008

A NEW APPROACH TO PUBLIC-KEY CRYPTOSYSTEM BASED ON MANDELBROT AND JULIA FRACTAL SETS

by

MOHAMMAD AHMAD A. ALIA

Thesis submitted in fulfillment of the
requirements for the degree
of Doctor of Philosophy

2008

ACKNOWLEDGEMENTS

This thesis is the result of three years of work whereby I have been accompanied and supported by many people. It is wonderful that I now have the opportunity to express my gratitude to all of them.

The first person I would like to express my deep and sincere gratitude to is my supervisor, Associate Professor Dr. Azman Bin Samsudin, School of Computer Sciences, Universiti Sains Malaysia (USM). His wide knowledge and his logical way of thinking have been of great value to me. His understanding, encouragement and personal guidance have provided a good basis for the present thesis.

I would like to thank the School of Computer Sciences, Universiti Sains Malaysia for supporting this study.

Also, I would like to take this opportunity to express my profound gratitude to my beloved parent and parent in law, without whom I would never have been able to achieve so much. I especially wish to express my love for my wife Reem, who did not only endure my manifold activities but also provided inspiration and support for my inclination to perfectionism. Only she knows how much I am indebted to her. I appreciate her for caring after our cute twins Raya and Razan, who were born during this study, on October 4, 2006.

Last, but certainly not least, I want to thank my brother, sisters, brother in law and sisters in law, their moral support during my study in Malaysia.

Mohammad Alia

TABLE OF CONTENTS

CHAPTER ONE: INTRODUCTION

CHAPTER TWO: CRYPTOGRAPHY BASIC

CHAPTER THREE: LITERATURE REVIEW

CHAPTER FOUR: KEY EXCHANGE PROTOCOL BASED ON MANDELBROT AND JULIA FRACTAL SETS

CHAPTER FIVE: PUBLIC-KEY ENCRYPTION BASED ON THE MANDELBROT AND JULIA FRACTAL SETS

CHAPTER SIX: DIGITAL SIGNATURE BASED ON THE MANDELBROT AND JULIA FRACTAL SETS

CHAPTER SEVEN: CONCLUSION AND FUTURE WORK

APPENDICES

APPENDIX A: GMP LIBRARY

APPENDIX B: A MATHEMATICAL BACKGROUND

APPENDIX C: CORRELATION COEFFICIENT TESTS

LIST OF TABLES

LIST OF FIGURES

SATU PENDEKATAN BARU UNTUK KRIPTOSISTEM KEKUCI AWAM BERASASKAN SET FRAKTAL MANDELBROT DAN JULIA

ABSTRAK

Kajian ini mencadangkan primitif baru kekunci-awam berasaskan kepada set Fraktal Mandelbrot dan Julia. Penciptaan kekunci-awam primitif berasas Fraktal boleh dilakukan kerana perkaitan yang kuat di antara set Fraktal Mandelbrot dan set Fraktal Julia. Dalam protokol yang dicadangkan, fungsi Fraktal Mandelbrot mengambil kekunci persendirian yang dipilih sebagai parameter input dan menjana kekunci awam penghubung. Fungsi Fraktal Julia kemudiannya digunakan menurut kepada fungsi dan algoritma seperti yang diperlukan. Dalam protokol pertukaran kekunci, fungsi Julia digunakan untuk mengira kekunci bersama berdasarkan kepada kekunci persendirian dan kekunci awam yang diterima. Dalam algoritma penyulitan kekunci-awam, fungsi Julia digunakan untuk menyulitkan teks asal dengan kekunci-awam penerima dan menyah-sulitkan teks sulit berdasarkan kepada kekunci-persendirian penerima. Akhirnya dalam skim tandatangan digital, fungsi Julia digunakan untuk menjana tandatangan pesanan dengan kekunci-awam penerima dan mengesahkan tandatangan pesanan yang diterima berdasarkan kepada kekunci-persendirian penerima. Disamping itu, kami mencadangkan variasi algoritma tandatangan di mana pengesahan dapat dilakukan oleh pihak awam. Melalui kaedah alternatif ini, penerima akan menjana kekunci-awam dan kekunci persendiriannya dengan menggunakan fungsi Mandelbrot dan kemudian fungsi Julia digunakan oleh pihak awam untuk mengesahkan pesanan berdasarkan kepada kekunci-awam pengirim.

Primitif kekunci-awam yang dicadangkan telah direka agar dapat mengelak serangan, menggunakan kekunci bersaiz kecil dan berprestasi laju (sehingga 24% lebih laju) berbanding dengan kebanyakan primitif kekunci-awam semasa seperti RSA (Rivest, Shamir dan Adleman), DH (Diffie Hellman), DSA (Digital Signature Algorithm).

Oleh itu primitif kekunci-awam Fraktal yang dicadangkan adalah satu alternatif yang menarik berbanding primitif kekunci-awam tradisional yang berdasarkan kepada teori nombor.

A NEW APPROACH TO PUBLIC-KEY CRYPTOSYSTEM BASED ON MANDELBROT AND JULIA FRACTAL SETS

ABSTRACT

This study proposes new public-key primitives based on Mandelbrot and Julia Fractal sets. The creation of the Fractal based public-key primitives is possible because of the strong connection between the Mandelbrot and Julia Fractal sets. In the proposed protocols, Mandelbrot Fractal function takes the chosen private key as the input parameter and generates the corresponding public key. Julia Fractal function is then used in accordance with the function and the required algorithm specifically. In the key exchange protocol, the Julia function is used to calculate the shared key based on the existing private key and the received public key. In the public-key encryption algorithm, the Julia function is used to encrypt the plaintext with the receiver's public key and decrypt the ciphertext based on the receiver's private key. Finally, in the digital signature scheme, the Julia function is used to sign the message with the receiver's public key and verify the received message based on the receiver's private key. In addition, another variation of the signature algorithm is proposed where the verification can be made by the general public. In this alternative method, the sender will generate his public and private keys by Mandelbrot function and then the Julia function will be used by the public to verify the message based on the sender's public keys.

The proposed public-key primitives were designed to be resistant against attacks, utilize small key size and perform comparatively faster (up to 24% faster) than most of the existing public-key primitives such as RSA (Rivest, Shamir and Adleman), DH (Diffie Hellman), DSA (Digital Signature Algorithm), etc. The proposed Fractal public-key primitives are, therefore, an attractive alternative to the traditional number theory based public-key primitives.

LIST OF ABBREVIATIONS AND TERMINOLOGIES

AES	: Advanced Encryption Standard
Alice	: The name traditionally used for the first user of cryptography in a system; Bob's friend
ANSI	: American National Standards Institute
ATM	: Automated Teller Machine
BC	: Before Christ
Bob	: The name traditionally used for the second user of cryptography in a system; Alice's friend
CS	: Computer Science
DES	: Data Encryption Standard
DH	: Diffie Hellman
DLP	: Discrete Logarithm Problem
DSA	: Digital Signature Algorithm
DSS	: Digital Signature Standard
EC	: Elliptic Curve
ECC	: Elliptic Curve Cryptosystem
ECDLP	: Elliptic Curve Discrete Logarithm Problem
ECDSA	: Elliptic Curve Digital Signature Algorithm
E-Business	: Electronic Business
E-Commerce	: Electronic Commerce
E-Payment	: Electronic Payment
FIPS	: Federal Information Processing Standards
GCD	: Greater Common Divisor
GF	: Galois Field
GMP	: GNU Multiple Precision

IBM	: International Business Machines Corporation
IEEE	: Institute of Electrical and Electronics Engineers
IFP	: Integer Factorization Problem
IP	: Internet Protocol
IPSec	: IP security
ISO	: International Standards Organization
Juliafn	: Julia Function
LCM	: Least Common Multiple
LFSR	: Linear Feedback Shift Register
Mandelfn	: Mandelbrot Function
MD5	: Message-Digest algorithm 5
NP	: Non-Deterministic Polynomial
NIST	: National Institute of Standards and Technology
NSA	: National Security Agency
P	: Polynomial
PFDS	: Public Fractal Digital Signature
PGP	: Pretty Good Privacy
PKI	: Public Key Infrastructure
QAP	: Quadratic Assignment Problems
RAM	: Random Access Memory
RSA	: Revist, Shamir and Adleman
SHA	: Secure Hash Algorithm
SSH	: Secure Shell
SSL	: Secure Sockets Layer
S/MIME	: Secure / Multipurpose Internet Mail Extensions
TLS	: Transport Layer Security
TSP	: Traveling Salesman Problem

US	: United States
USM	: Universiti Sains Malaysia

CHAPTER 1

INTRODUCTION

Cryptography is one of the most important fields in computer security. It is a method of transferring private information and data through open network communication, so only the receiver who has the secret key can read the encrypted messages which might be documents, phone conversations, images or other form of data (refer to Figure 1.1). To implement privacy simply by encrypting the information intended to remain secret can be achieved by using methods of Cryptography. The information must be scrambled, so that other users will not be able to access the actual information. For example, in a multi-users system, each user may keep his privacy intact via her/his own password. On internet, a large number of internet users use internet application, such as business, research, learning, etc. These activities are very important for the users' application; hence, the importance of using Cryptography has been highlighted to help them keep the privacy.

Cryptography services in general help to ensure the following (Menezes et al., 1996; Mouratidis et al., 2003):

- Confidentiality: Confidentiality is a service used to guarantee information it is accessible only to authorized entities and is inaccessible to others.
- Authentication: Authentication is a service used to provide the identity of an entity.
- Integrity: Integrity is a service used to guarantee that the information remains unchanged from the source entity to the destination entity.

- Non-repudiation: Non-repudiation is a service used to confirm the involvement of an entity in a certain form communication, and prevents any party from denying the sent message.
- Accessibility: Accessibility is a service put in place to allow the use of information resources by authorized entities.

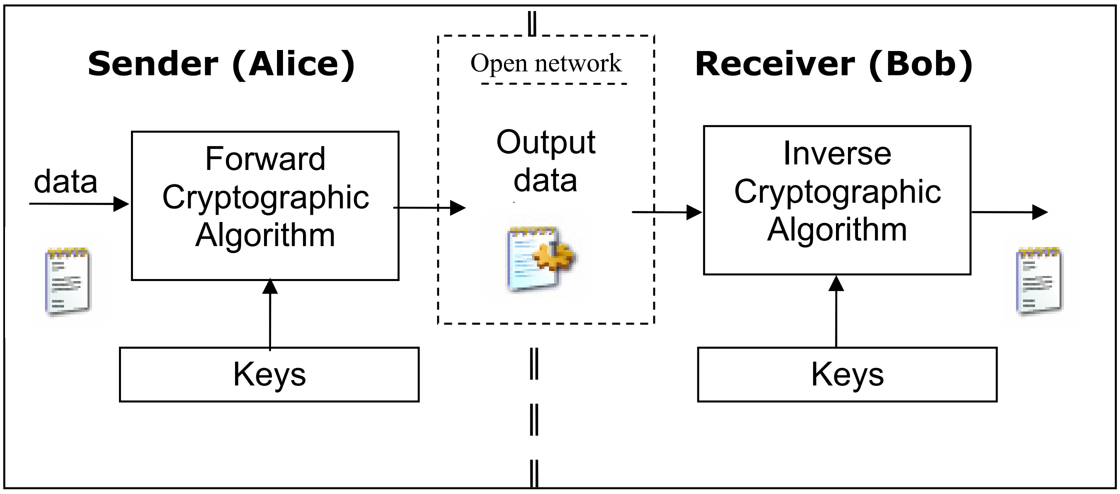


Figure 1.1: Cryptography system

1.0 Information Security and Cryptography

Information security is the process which describes all measures taken to prevent unauthorized use of electronic data, whether this unauthorized use takes the form of destruction, use, disclosure, modification, or disruption. Information security and Cryptography are interconnected and share the common services of protecting the confidentiality, integrity and availability of the information ignoring data form (electronic document, printed document). In the encryption process, information security uses Cryptograph to shift the information into the cipher form which does not allow it to be used by unauthorized personnel.

Cryptography provides the information security for other useful applications such as in encryption, message digests, and digital signatures. The length and strength of the Cryptography keys are considered an important mechanism. The keys used for encryption and decryption must be strong enough to produce strong encryption. They must be protected from unauthorized users and must be available when they are needed.

Cryptography also contributes to Computer Science, particularly, in the techniques used in computer and network security for access control and information confidentiality. Cryptography is also used in many applications encountered in everyday life such as: computer passwords, ATM cards, and electronic commerce (refer to Figure 1.2). The request for Cryptography system has increased recently for the public especially after the fast development of the Internet in the last 10 years ago.

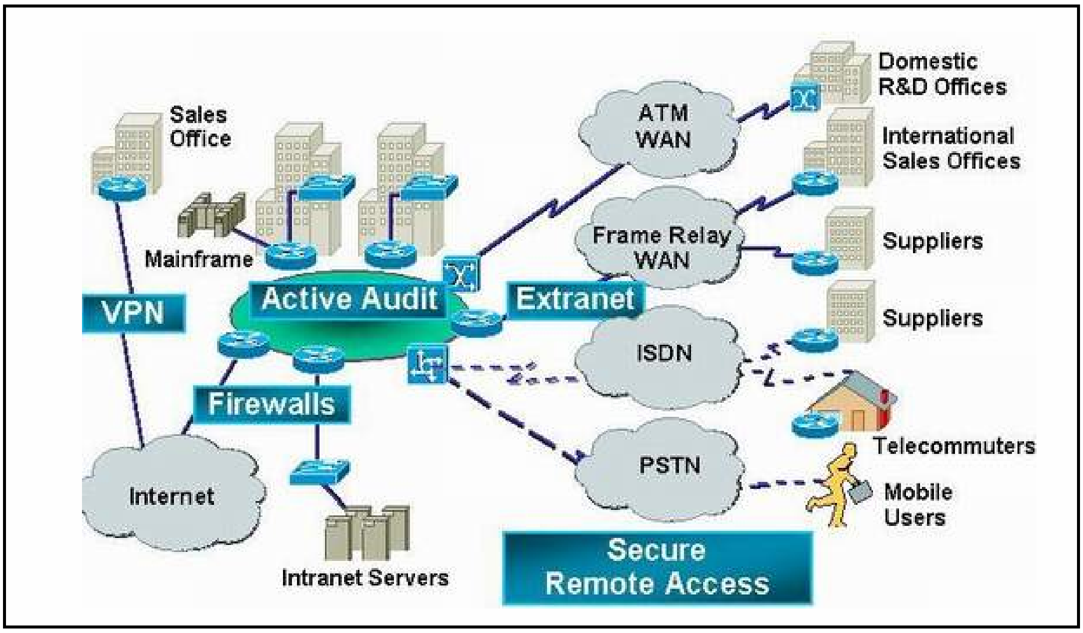


Figure 1.2: Network security system (Macroview Telecom Group, 2006)

1.1 Motivation

A large number of internet users and the power have reacted in contrasting to the researchers in developing protection algorithms of public-key Cryptography to ensure the highest degree of protection to users against the brute force attacks with lowest cost. Therefore, the major motivation of this research is to reduce the computation cost and increase the security for the public-key Cryptography protocols (key exchange, encryption, and digital signature). This motivation leads us to propose new public-key cryptosystem based on Fractal (NP-hard problem). Since, there are many previous works in Fractal Cryptography. Most of these protocols were design in the symmetric approaches. Note that, there is only one work that has been done on public-key cryptography which is based on Newton Raphsone gravitation law (Whitehead et al., 2003).

1.2 Research Questions

The importance of this study can be summarized by three fundamental questions as follows:

- Why it is important to find new alternative for the public-key cryptosystem?
- Why Fractal public-key cryptosystem is an attractive alternative to number theory based public-key cryptosystems?
- What is the method used in this study?

These questions will be answered in the following Sections (Section 1.3 to 1.9).

1.3 Problem Definition

Most of the currently used public-key primitives are computationally expensive with relatively lengthy key requirement due to dependency on the number theory, which the primitives were derived from. Therefore, it's important to develop (investigate) new cryptography primitives from other mathematical hard problem (NP hard) which is not based number theory.

In this thesis, we propose new public-key primitives based on Mandelbrot and Julia Fractal sets. However, this study attempts to deal with the following problems which are related to Cryptographer requirements:

- Cryptanalysis and Attacking: the attacks were so strong and the speed of the activities of the cryptanalyst to break the security of the cryptosystem protocols exceeded the cryptographers' expectations.
- Key size: most of public-key Cryptography protocols depend on a large prime key that to ensure the security of these protocols and prevent a brute force attack.
- Algorithm speed: a lot of the public-key Cryptography protocols perform at a low speed depending on key size.
- Performance evaluation: some of the public-key protocols provide high level of security at a much higher cost.

These arguments lead to other problems which are related to the security in the user's applications through the open network. These problems are represented by the wide internet access and its applications such as e-payment, e-business, etc.

1.4 Research Scope

To overcome these problems, we introduce alternative public-key primitives based on Mandelbrot and Julia Fractal sets. The problems of attacks which are faced by cryptanalysts have made us look for the new system that can be applied to the cryptosystem. Our study in this thesis focuses on the Fractal which is a NP-hard problem (hard to cryptanalyze).

1.5 Research Purpose

The objective of this thesis is to study the aspects of Fractal systems in the treatment of public-key Cryptography systems, with focus on Mandelbrot Fractal set and Julia fractal set. Hence, the objectives of the case studies are:

- To find an alternative public-key cryptography primitives based on Fractal.
- In this thesis the security assessments of Fractal public-key cryptosystem are based on:
  1. The strength of the proposed algorithms
     - Mathematical hard problem
     - Randomize result
     - Adequate key size
  2. The performance of the proposed algorithm.

1.6 Research Methodology

This research was conducted in order to find new public-key primitives based on Mandelbrot and Julia Fractal sets. The security and the Performance of these proposed primitives were also part of the thesis objectives. Therefore, to answer these research goals, this study employs the following research methodology as to:

- Shows literature survey on public-key Cryptography.
- Shows literature survey on Fractal.
- Propose new public-key primitives based on Mandelbrot and Julia Fractal sets.
    1. Propose a new key exchange protocol based on Mandelbrot and Julia Fractal sets.
    2. Propose a new public-key encryption algorithm based on Mandelbrot and Julia Fractal sets.
    3. Propose a new digital signature scheme based on Mandelbrot and Julia Fractal sets.
- Compare our proposed Fractal public-key cryptosystems with the others traditional public-key cryptosystems.
- Highlight the security results for the proposed public-key cryptosystem.

1.7 Thesis Contributions

This study has produced new public-key primitives based on Mandelbrot and Julia Fractal sets. Chapters 4, 5, and 6 in this thesis contain comparisons and explanations for the proposed public-key primitives based on Fractal and other traditional techniques. The proposed public-key primitives in this study are new key exchange, a new public-key encryption and a new digital signature based on

Mandelbrot and Julia Fractal sets. The proposed public-key cryptosystem protocols in this study require small key size and perform faster when compared to the alternative traditional number theory based on public-key encryption protocols, with a higher level of security at a much lower cost.

The main innovations in this thesis will be described in detailed in each of the following Chapters, as outlined in the next Subsection.

1.8 Importance of the Study

This study shows the possibility of establishing Fractal based cryptosystem algorithm including key exchange protocol, public key encryption algorithm and digital signature scheme, derived from the logical connection between the Mandelbrot and Julia Fractal sets. The security protection of the proposed Fractal cryptosystem depends on the number of iterations and the added variation constants during the iteration of Mandelbrot and Julia functions. This makes Mandelbrot and Julia values jump path chaotically and also it will establish the needed complexity of the proposed schemes. However, we can identify that the proposed Fractal public-key cryptosystem is based on chaotic hard problem. The chaotic nature of the Fractal functions ensures the security of the proposed public-key cryptosystem schemes, and this will prevent a brute force attack.

1.9 Outline of the Thesis

The work conducted in this thesis is shown in seven Chapters with appendices. This Chapter provides an introduction to the work by giving a brief overview of the related concepts, including a brief summary on the work conducted here (Chapter 1). The following Chapters of the thesis are presented as follows.

In Chapter 2, we discuss some related concepts used in this thesis. The Cryptography algorithms are classified into two categories, secret-key (symmetric) algorithms and public-key (asymmetric) algorithms; and the discussion is based on the mathematical problems.

In Chapter 3, we discuss another related concept used in this thesis. The history of the Fractal is explained. The characteristic of Mandelbrot and Julia Fractal sets are discussed in detail with their connection and functions.

Chapter 4 shows the idea behind Fractal Cryptography systems, and we explain our first new algorithm as a new key exchange protocol based on Mandelbrot and Julia Fractal sets. In addition the comparisons between our key exchange protocol based on Fractal with the Diffie-Hellman key exchange protocol are discussed.

Chapter 5 presents the idea of our second new algorithm as a new public-key encryption system based on Mandelbrot and Julia Fractal sets. The comparisons between our encryption system based on Fractal with the RSA public-key encryption system are also being discussed.

In Chapter 6 we explain the idea of the Fractal digital signature as a third new scheme based on Mandelbrot and Julia Fractal sets. The comparisons between our digital signature scheme based Fractal with traditional number theory based Cryptography protocols like the RSA and the DSA digital signature scheme are also being explained. Also we propose another generalized scheme for Fractal based digital signature (GFDS).

Finally, in Chapter 7 we present the conclusion and the possible future work for this study. This conclusion depends on all the results which we have obtained through the implementation of the study to be clarified and summarized for the reader.

In the Appendices we have explained some related mathematical concepts which are used to help the reader to understand the work of the traditional algorithms (RSA, EC, ElGamal, etc.) and we have introduced the GMP library which is used in our implementation.

CHAPTER 2

CRYPTOGRAPHY BASIC

2.0 Introduction

In this chapter, we introduce notation and basic concepts used throughout the rest of the thesis which are related to the concepts in Cryptography. In addition, most of the following chapters have an individual preliminary section introducing concepts that are exclusively used in those specific chapters.

This Chapter gives a specific overview of the concepts which are required for understanding this thesis, but we rather assume the reader is familiar with the basic concepts for the asymmetric Cryptography algorithms such as RSA, DSA, etc. from the standard Cryptography literature.

Figure 2.1 shows the two most important branches of Cryptography which can be classified into two types, viz, symmetric and asymmetric Cryptography. Each type is fragmented into many sections based on its mathematical hard problems. This Chapter first discusses some of the non-public key algorithms that include the secret-key algorithm and the Hash functions, and then moves on to some of the most important public-key algorithms which are classified according to mathematical hard problems (integer factorization, discrete logarithm and Elliptic Curve). With this introduction, it will help us to describe our proposed Cryptography algorithms, which are based on chaotic mathematical problems.

We have organized this Chapter according to the literature survey on the Cryptography into four main sections. Since Section 2.1 gives a definition and classification for the Cryptography system. In Section 2.2, we discuss the non-public key algorithm which is classified into two types, secret-key (asymmetric) and Hash function. The Cryptography algorithms are classified into two categories, secret-key (symmetric) algorithms and public-key (asymmetric) algorithms; and the discussion is based on the mathematical problems. Section 2.3 is divided into a few subsections, and these subsections explain the public-key algorithms which include the key exchange, public-key encryption and digital signature schemes. These schemes also contain some examples which are classified depending on its mathematical hard problems. Finally, in Section 2.4 we present a summary for Chapter 2 including Table 2.5 which shows general summary for the Cryptography systems.

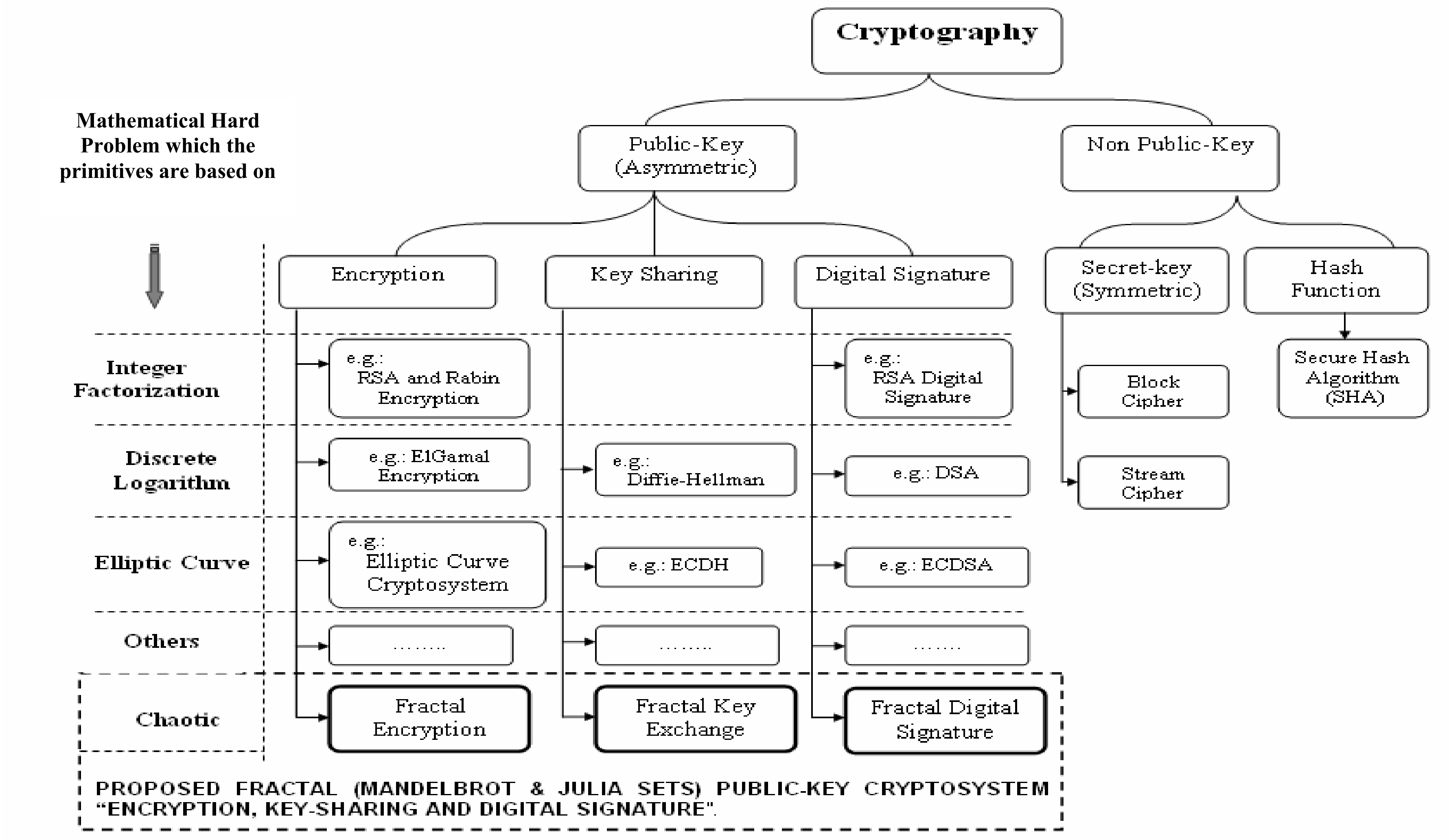


Figure 2.1: Main branches of Cryptography

2.1 Cryptography System Definition

Cryptography is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication, and data origin authentication. In addition, Cryptography is also known as the science of secret writing (Menezes et al., 1996; Branovic et al., 2003, Dent et al., 2005).

Cryptography has many repeated terms such as the plaintext, ciphertext and secret key which should be defined in proper manner. The plaintext is the original message that is considered as input data for the encryption algorithm. The ciphertext is of the secret writing and it depends on the plaintext and the secret key. Just as the ciphertext is a random stream of data, the secret key which is also input data for the encryption methods, is responsible for the transmission of the plaintext to the ciphertext through the encryption algorithm.

Cryptography may be divided into two main categories (refer to Figure 2.1):

- Asymmetric: Ciphering and deciphering using a pair of keys.
- Non asymmetric: Ciphering and deciphering using the same key (or without key – in the case of Hash function).

2.2 Non Public-Key Algorithms (Secret-Key Algorithms and Hash Functions)

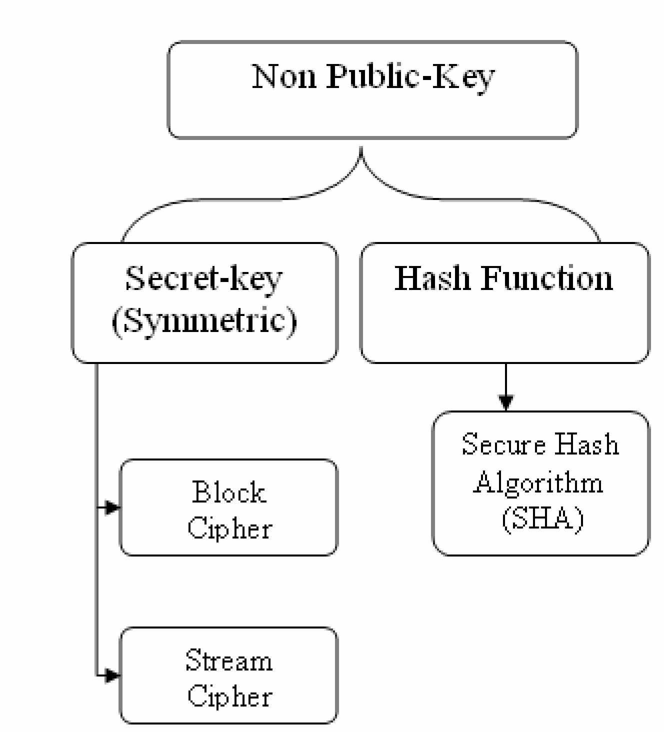


Figure 2.2: Non Public-key branches

Figure 2.2 shows the two most important branches of the non public-key Cryptography which can be classified into two types-viz, secret-key (symmetric) and Hash function. Each type is fragmented into subsections and will be represented by some examples in this Chapter. These examples will explain the security and the performance for the presented schemes.

2.2.1 Secret-Key (Symmetric) Algorithms

Secret-key is also known as single-key, or one-key algorithm. Secret-key is an encryption scheme consisting the sets of encryption and decryption algorithms. The plaintext is encrypted by key *e* and the ciphertext is decrypted by key *d,* where *e* is the encryption key and *d* is the decryption key. In secret-key scheme, key *d* must be equal to key *e.* The Data Encryption Standard (DES) (National Bureau of Standards, 1977) is an example of the secret-key scheme (refer to Figure 2.3).

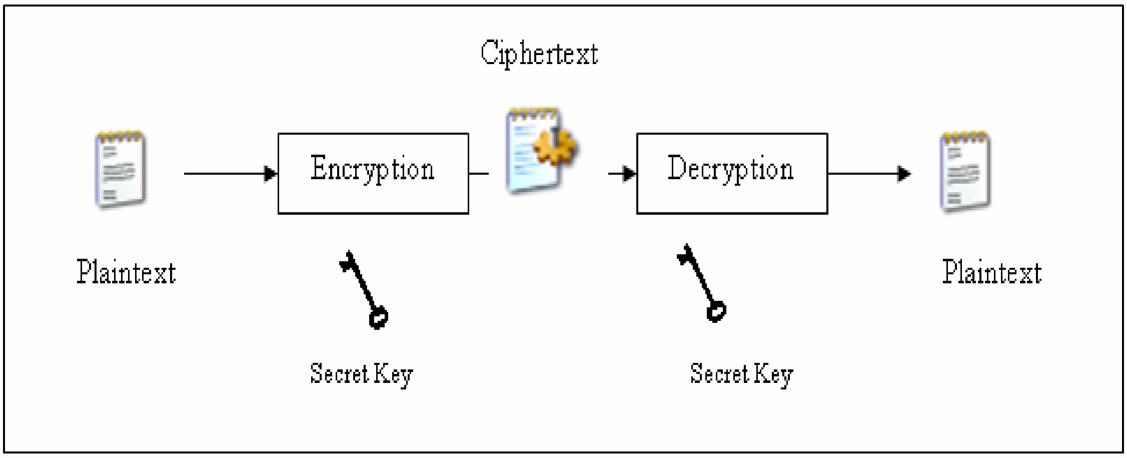


Figure 2.3: Secret-key scheme

Secret-key (symmetric) algorithms can be classified into stream ciphers and block ciphers (refer to Figure 2.2). The stream ciphers encrypt the whole message at a time. While the block ciphers split the message into blocks and then encrypt the blocks respectively. In general, the block size is normally 128 bits.

2.2.1.1 Stream Ciphers

A stream cipher is a type of secret-key encryption where the stream cipher algorithm generates key stream. The key stream bits and the plaintext bits are combined together, usually with the exclusive-or (XOR) operation, and then the result for this combination is the ciphertext. Stream ciphers are considered much faster with lower hardware cost than the block cipher algorithms (Robshaw, 1995).

In general the stream cipher can be classified (based on the key stream status) into two types as follows:

- Synchronous stream ciphers: the key stream in the synchronous stream ciphers is generated independently of the plaintext and ciphertext.
- Self-synchronising stream ciphers: in the self-synchronous stream the key stream is generated dependent on the plaintext and the ciphertext. The self-synchronising stream cipher scheme is known also as asynchronous stream ciphers or ciphertext autokey (CTAK).

There are many proposed stream cipher algorithms. Among these are RC4 (Golic, 1997), RC5 (Rivest, 1994), Helix (Ferguson et al., 2003), ISAAC (Jenkins, 1996), etc.

2.2.1.2 Block Ciphers

A block cipher is a secret-key encryption that encrypts a fixed-length block of plaintext into same length of ciphertext block. The encryption and decryption in the block cipher are performed by using the same secret key. Typically, a block cipher that takes the input 64-bit block of plaintext must produce the output 64-bit block of ciphertext.

DES is one of the secret-key schemes, and was developed in 1977 by IBM and the NSA (National Security Agency). DES processes plaintext blocks of *n* = 64 bits, producing 64-bit ciphertext blocks. The effective size for the secret key in DES is 56 bits (refer to Figure 2.4) (Menezes et al., 1996; Branovic et al., 2003; Pell, 2006).

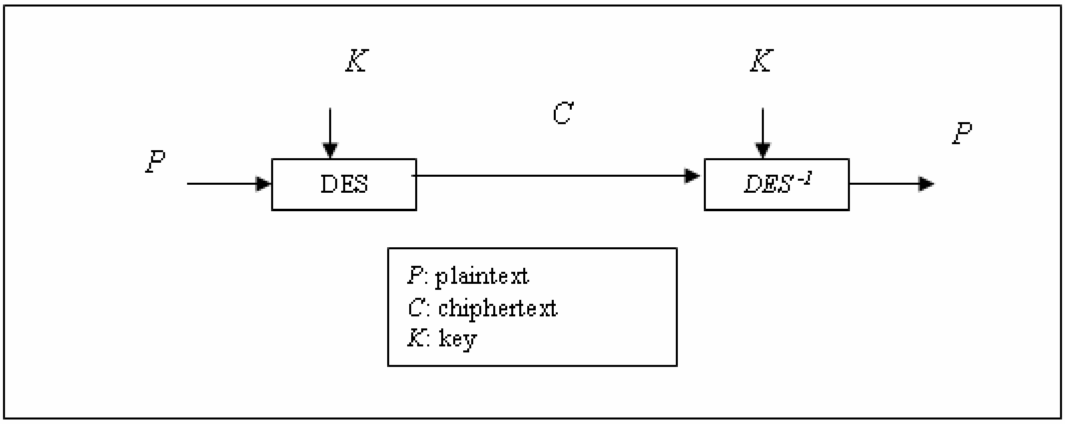


Figure 2.4: DES scheme

Recently, the National Institute of Standards and Technology (NIST) has replacing DES with AES (Advanced Encryption Standard) because the DES is considered to be not secure for many applications. Also the DES has been attacked by some of analytical theoretical operations that show the weaknesses of DES in the ciphering (FIPS PUB 81, 1996).

Other Cryptography primitives used block cipher algorithms to build Hash function and stream cipher. The Hash functions (next Subsection) might be created by the block ciphers. In addition, the stream ciphers can also be built by using the block cipher algorithms. Also, there are some block ciphers modes such as OFB-mode and CTR-mode which are used to switch the block cipher algorithm into a stream cipher algorithm (FIPS PUB 81, 1996).

2.2.2 Hashing Functions

A Hash function (refer to Figure 2.2) is a method of turning the given input message into small digests which are normally used for data integrity checking. The Hash function is used to serve algorithms such as the digital signature algorithm to produce the subsequent signature. Hash function takes a random sized input message to produce a fixed sized output which is also known as the message digests. Typically, the output of the Hash functions is connected to the Hash function techniques. There are many Hash function algorithms such as MD5 (Rivest, 1992), SHA family (National Security Agency, 2002), HAVAL (Zheng et al., 1993), etc.

For example, the SHA-512 Hash function takes input messages of lengths up to 2^{128} bits and produces as output a 512-bit message, as shown by Table 2.1. There are many Hash function techniques presented by the SHA family. Among these are SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512, which are designed by the National Security Agency (NSA) and published by the NIST as a U.S. government standard (National Security Agency, 2002).

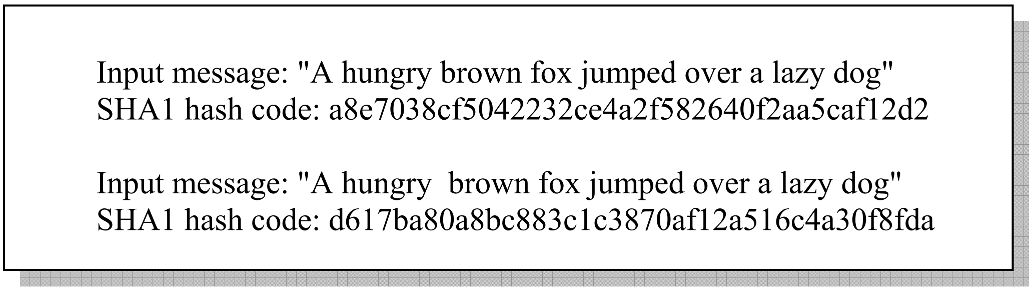
Table 2.1: SHA Hashing function family

Algorithm	Maximum Input size	Output size	Operations
SHA-1	2^{64}-1 bits	160 bits	+, and, or, xor, rotl "rotation-left"
SHA-224/256	2^{64}-1 bits	224/256 bits	+, and, or, xor, shr, rotr "rotation right"
SHA-384/512	2^{128}-1 bits	384/512 bits	+, and, or, xor, shr, rotr "rotation right"

The main properties for a good Cryptographic Hash function *h* are as follows (Avi, 2006):

- It should destroy all homomorphism structures in the underlying public key cryptosystem.
- It should be computed on the whole message value.
- It should be a one-way function.
- It should be computationally infeasible given a message and its Hash value to compute another message with the same Hash value.
- It should resist birthday attacks (not collision resistant).

SHA-1 is a one of the security Hash algorithms (SHA), and it is employed in several security applications like SSL/TLS, PGP, SSH, S/MIME, and IPSec. SHA-1 is the successor to MD5. The algorithms SHA-256, SHA-384, and SHA-512 are individually referred to as SHA-2. The following example shows the change in the Hash code by using the security Hash algorithm SHA-1 (Avi, 2006) (refer to Figure 2.5).



```
Input message: "A hungry brown fox jumped over a lazy dog"
SHA1 hash code: a8e7038cf5042232ce4a2f582640f2aa5caf12d2

Input message: "A hungry  brown fox jumped over a lazy dog"
SHA1 hash code: d617ba80a8bc883c1c3870af12a516c4a30f8fda
```

Figure 2.5: An example for Hash algorithm, SHA-1 (Avi, 2006)

As shown by Figure 2.5, the only difference between the two messages is the extra space between the words “hungry" and “brown" in the second message that gave two different values for the SHA-1 outputs.

SHA-1 was cracked recently in 2005, by Xiaoyun Wang, Yiqun Lisa Yin, and Hongbo Yu (Wang et al., 2005). This work shows that it is possible to find collisions for SHA-1 with fewer than 2^{69} operations.

Figure 2.6 shows the work of the security Hash function (SHA-512). The SHA-512 takes a random size message as an input and then divides the message to 1024-bit block to produce the Hash code after the SHA-512 operations have been executed.

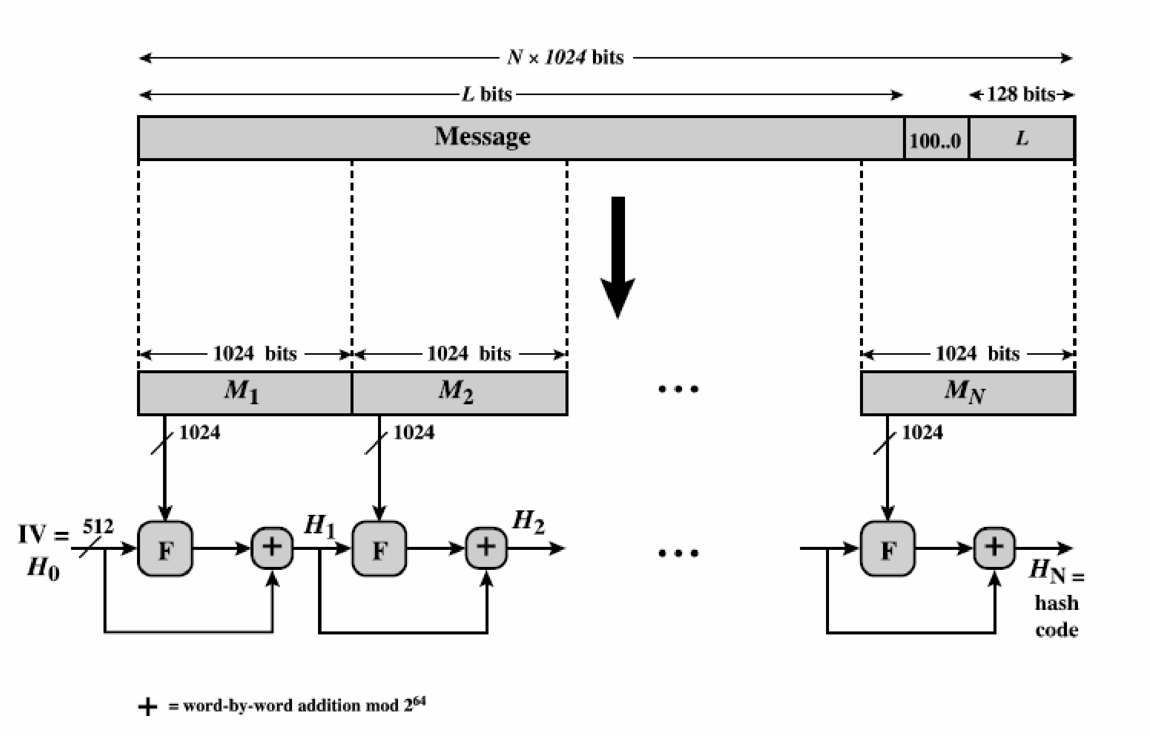


Figure 2.6: Message digests generation using SHA-512 (Avi, 2006)

2.3 Public-Key (Asymmetric) Algorithms

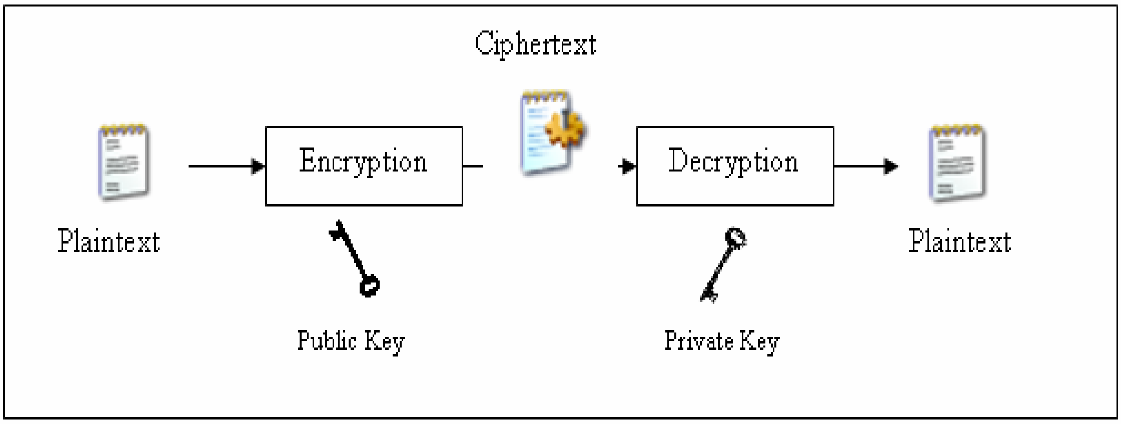


Figure 2.7: Public-key scheme

Public-key encryption protocols work in a different way. In these algorithms, there is a pair of keys, one of which is known to the public and used to encrypt the plaintext to be sent to the receiver who owns the corresponding decryption key, known as the private key (refer to Figure 2.7). In general, a security protocol uses public-key cryptosystem to exchange the secret key between communicating nodes and then uses secret-key algorithms with the agreed secret key as the password to ensure confidentiality on the data transferred.

In this Section, we present exemplified region of some public-key algorithms. Every public-key cryptosystem is based on a mathematical problem that is in some sense difficult to solve. These problems are called “hard problems” and are classified in two major categories according to the Cryptography classifications, as *P* (Polynomial) and *NP* (Non-deterministic polynomial). The problem is considered to be a *P* hard problem if the problem can be solved in polynomial time, while a problem is considered to be an *NP* hard mathematical problem if the validity of a proposed solution can be checked only in polynomial time (RSA Laboratories, 2007). Basically, the three major types of mathematical hard problem that had been successfully being used in

Cryptography are described in the following subsections of this chapter. These problems are the integer factorization problem (IFP), the discrete logarithm problem (DLP) and the Elliptic Curve discrete logarithm problem (ECDLP). This survey will help us to identify the hard mathematical problem for the proposed public-key Fractal cryptosystem which is based on the Chaos property of the Fractal (Coutinho, 1999).

As defined earlier, the pubic-key encryption and decryption transformations schemes include two different keys. One key is used to encrypt the plaintext and the other is used to decrypt the ciphertext (refer to Figure 2.7). In general, these keys are defined as follows (Menezes et al., 1996):

- *K* is a set of the key space.
- $e \in K$, where *e* is a public key, which is used to cipher the plaintext (message) *M* to the ciphertext *C*, which is transformed by the encryption transformation E_e, (E_e: *M* → *C*).
- $d \in K$, where *d* is a private key, which is used to decipher the ciphertext *C* to the plaintext (message) *M*, which is transformed by the decryption transformation D_d (D_d: *C* → *M*).

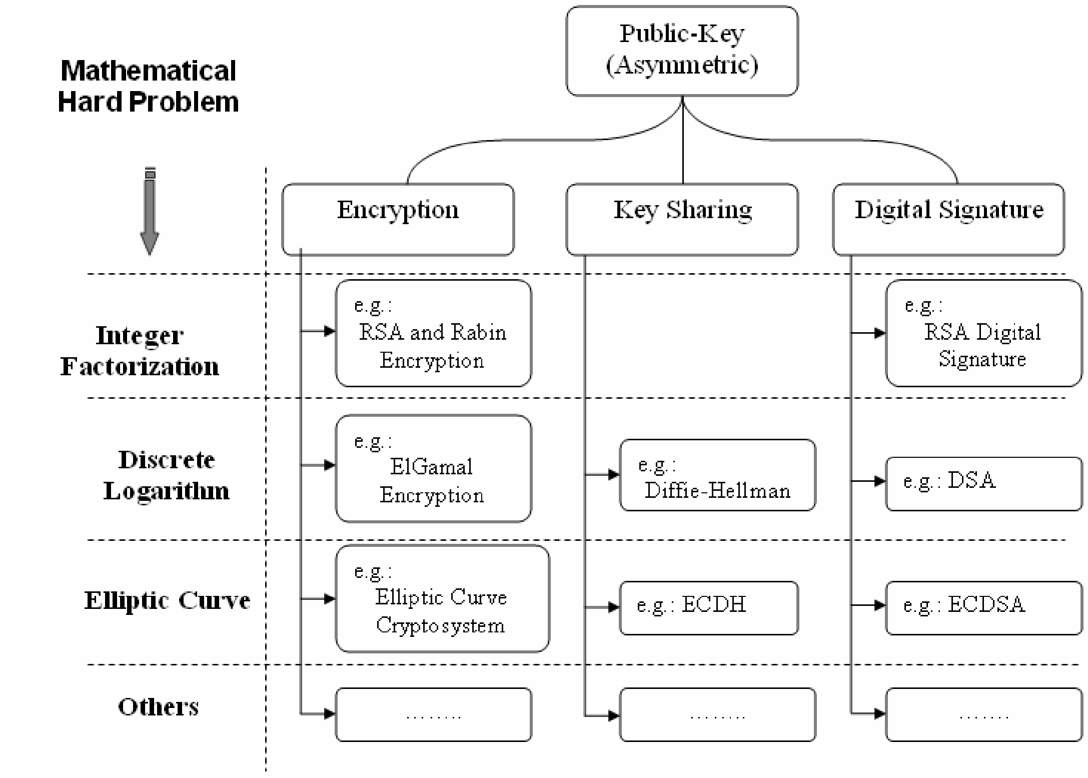


Figure 2.8: Main branches of public-key scheme

Figure 2.8 shows the most important branches of public-key cryptosystem (asymmetric) which can be classified into three types-viz, encryption, key sharing and digital signature. Each type is fragmented into many Subsections based on its mathematical hard problems (integer factorization, discrete logarithm and Elliptic Curve). This Section first discusses some of the public key algorithms that will be represented by one example for each, and we then moves on to explain the security and the performance of these algorithms.

3.1 Key Exchange

The key exchange is an important method in public-key Cryptography. Keys are exchanged between the users according to Cryptography protocols which are based on