A NEW VISUAL PUBLIC-KEY CRYPTOSYSTEM BASED ON NON-EXPANSION TECHNIQUE AND BOOLEAN OPERATIONS

by

ABDULLAH MOHAMMED ABDO ALI JAAFAR

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

2011

ACKNOWLEDGEMENTS

I would like to express my deep and sincere gratitude to my supervisor, Associate Professor Dr. Azman Bin Samsudin, School of Computer Sciences, Universiti Sains Malaysia (USM) for his patience, guidance, professional suggestions and advices and encouragement during the research and preparation of this thesis. I truly appreciate the time he devoted to me and showing me the proper directions in the research and his openness, honesty and sincerity.

The roles played by all members of academic and non-academic staff of the School of Computer Sciences, Universiti Sains Malaysia (USM) are also humbly and graciously acknowledged and so also are all my colleagues, who supported and encouraged me.

I owe sincere gratitude to my university in Yemen, Taiz University, where I work as lecturer, for all the support for this study. Similarly, I thank Dr. Ahmed Alameery, the cultural attaché to Saudi Arabia, and later, to Morocco, and I am also grateful to Dr. Mahyoub Al-Buhairi, the vice president of Taiz University for student affairs, for their encouragement and moral support.

I also take this opportunity to express my profound gratitude to my beloved parents for their care, encouragement and prayers. I would like to thank my brothers and sisters for their moral support during my stay in Malaysia for this study.

Last but not least, my special love and appreciation goes to my wife, my daughters Huda, Nada and Rana, my sons Osama and Emad, for their patience, sacrifice, understanding and support which they showed to me especially when I most needed. I especially appreciate the effort of my wife for take good care of our lovely son Emad, before and after he was born during the course of this study, on December 26, 2008.

Abdullah M. Jaafar

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATION AND TERMINOLOGIES

Alice	: The name traditionally used for the first user of cryptography in a system; Bob's friend
AES	: Advanced Encryption Standard
Bob	: The name traditionally used for the second user of cryptography in a system; Alice's friend
BWI	: Black-and-White Image
Card ID	: Card Identification
DES	: Data Encryption Standard
DH	: Diffie-Hellman
DLP	: Discrete Logarithm Problem
DS	: Digital Signature
DSA	: Digital Signature Algorithm
DSS	: Digital Signature Standard
EC	: Elliptic Curve
ECC	: Elliptic Curve Cryptography
E-Business	: Electronic Business
E-Commerce	: Electronic Commerce
E-Payment	: Electronic Payment
FIPS	: Federal Information Processing Standards
GQ	: Guillou-Quisquater
GCD	: Greater Common Divisor
H(V)	: Hamming weight of the vector V (the number of 1's in V)
IFP	: Integer Factorization Problem
M or m	: Message
NIST	: National Institute of Standards and Technology

NP	: Non-Deterministic Polynomial
P	: Polynomial
Peggy	: The name traditionally used for the first party of zero-knowledge proof in a system; Victor's friend
PR	: Private Key
ProbVC	: Probabilistic Visual Cryptography
ProbVSS	: Probabilistic Visual Secret Sharing
PU	: Public key
RAM	: Random Access Memory
RC4	: Rivest Cipher 4
RSA	: Rivest, Shamir and Adleman
SHA	: Secure Hash Algorithm
SI	: Secret Image
SM	: Secret Message
US	: United States
USM	: Universiti Sains Malaysia
VC	: Visual Cryptography
Victor	: The name traditionally used for the second party of zero-knowledge proof in a system; Peggy's friend
VSS	: Visual Secret Sharing
XOR	: Exclusive OR; Logical Operation
ZN	: Zero-Knowledge
ZNP	: Zero-Knowledge Proof

SATU KRIPTOSISTEM KEKUNCI-AWAM VISUAL BARU YANG BERASASKAN TEKNIK TAK BERKEMBANG DAN OPERASI BOOLEAN

ABSTRAK

Banyak kriptosistem kunci-awam digunakan dalam kehidupan seharian kita, contohnya untuk kegunaan privasi, autentik, dan integriti. Namun demikian, kebanyakan algoritma kunci-awam yang sedia ada adalah berdasarkan kepada komputan matematik kompleks. Sehingga kini, binaan kriptosistem kunci-awam dengan ciri-ciri keselamatan yang tinggi tanpa menggunakan komputan kompleks merupakan suatu cabaran yang serius, yang memerlukan suatu kaedah kriptografi baru dibangunkan. Kriptografi visual adalah istimewa kerana skemanya yang memerlukan pemeriksaan visual, yang mana setara dengan komputan Boolean yang ringkas; seterusnya menyebabkan komputan kompleks tidak diperlukan. Reka bentuk asas kriptografi visual menggunakan sistem visual manusia, untuk memulihkan imej-rahsia. Di samping itu, proses pemeriksaan visual boleh dilakukan dengan lebih mudah oleh manusia, tetapi sukar untuk komputer menirunya. Keadaan ini secara tidak langsung memberikan perlindungan tambahan pada skema visual terhadap serangan "brute-force" pada kunci-rahsia visual. Walau bagaimanapun, kriptografi visual semasa hanyalah tertumpu kepada kriptografi kunci-rahsia. Oleh itu, dalam kajian ini, primitif kunci-awam alternatif dicadangkan, berdasarkan kriptografi visual tak-berkembang dan operasi Boolean. Kriptosistem visual yang dicadangkan termasuklah: protokol pertukaran kunci visual, protokol tandatangan digital visual, dan bukti identiti protokol tanpa-pengetahuan visual. Keselamatan protokol kunci-awam visual yang dicadangkan, dijamin oleh masalah *K-SAT NP-hard* dan masalah matriks tidak songsang (non-invertible matrix) yang tiada penyelesaiannya. Analisis

keselamatan menunjukkan bahawa kriptosistem kunci-awam visual adalah selamat, terutamanya apabila digunakan dengan saiz imej-bayang (kongsi tampak) yang besar. Masa diperlukan untuk "brute-force" nilai-rahsia (kunci-rahsia visual) bertambah secara eksponen dengan bertambahnya saiz imej-bayang. Potensi kegunaan yang luas, pengkhususan pada aplikasi visual, pelaksanaan imej-bayang yang mudah, membuatkan kriptosistem kunci-awam visual yang dicadangkan merupakan suatu alternatif yang sesuai kepada kriptosistem kunci-awam klasik yang sedia ada pada hari ini.

A NEW VISUAL PUBLIC-KEY CRYPTOSYSTEM BASED ON NON-EXPANSION TECHNIQUE AND BOOLEAN OPERATIONS

ABSTRACT

Many public-key cryptosystems are used in our daily lives to attain privacy, authenticity, integrity and non-repudiation. However, most of the existing public-key algorithms are based on complex mathematical computations. Until recently, building a highly secured public-key cryptosystem without utilizing complex computations has been a serious challenge, making it necessary for investigations to develop new cryptography methods. Visual cryptography is special because the scheme requires visual inspection or the equivalence of simple Boolean computation and therefore, does not require complex computations. The basic design of visual cryptography exploits the human visual system, to recover secret images. Moreover, the visual inspection process could be carried out very easily by humans, but hard for the computer to imitate. Indirectly, such scheme adds extra protection to the visual scheme against brute-force search on the visual secret key. However, visual cryptography currently exists only for secret-key cryptography. Therefore, in the current study, alternative public-key primitives are proposed, based on non-expansion visual cryptography and Boolean operations. The proposed visual cryptosystem include: visual key exchange protocol, visual digital signature protocol and visual zero-knowledge proof of identity protocol. The security of the proposed visual public-key protocols is assured by the *K-SAT NP*-hard problem and non-solvable of the non-invertible matrix problem. Security analyses showed that the proposed visual public-key cryptosystem is secure, especially when used with large sizes of shadow images (visual shares). The time required to brute-force the secret

values (visual secret keys) increased exponentially with the increase in the size of shadow images. The wide potential use, specific niche on visual applications, simplicity and ease of implementation of shadow images, therefore makes the proposed visual public-key cryptosystem a suitable alternative to the classical public-key cryptosystems that are currently in use today.

CHAPTER 1

INTRODUCTION

1.0 General Overview

Today digital information can be distributed via the Internet to a large number of people in an easy and simple way. Information security is a field that protects and secures sensitive digital information and its systems from unauthorized access, disclosure, disruption, modification, or destruction. Information security provides many services such as data confidentiality, authentication, data integrity and non-repudiation in order to keep the distribution of sensitive digital information and its systems works reliably (Ozturk and Sogukpinar, 2005; Anoop, 2007; Chan and Wu, 2008; Information Security, 2010).

Cryptography is one of the trusted practical methods for performing information security. The main purpose of cryptography is to provide confidentiality by converting the sensitive private information (known as plaintext) into unreadable and useless form (known as ciphertext). Figure 1.1 shows different classifications of cryptography such as quantum cryptography, chaos cryptography, conventional cryptography and visual cryptography. In this study we focused only on the conventional (especially public-key) cryptography and visual cryptography.

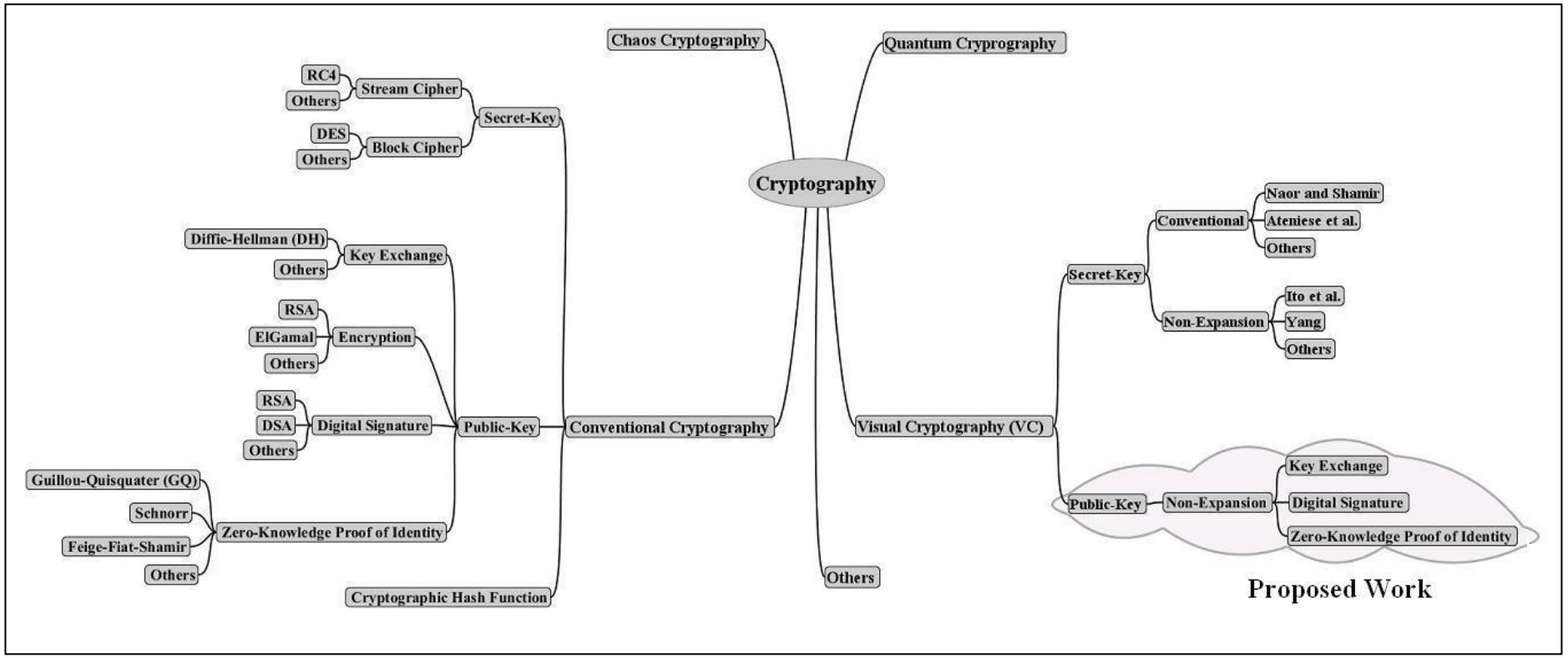

Figure 1.1: Main classifications of cryptography

There are, in general, two main types of conventional cryptography, secret-key cryptography and public-key cryptography (refer to Figure 1.1). These two types are controlled by keys and some of the primitives are based on complex mathematical concepts.

Secret-key cryptography which is also known as symmetric-key cryptography, uses the same key for both encryption and decryption (refer to Figure 1.2). Secret-key algorithms can be classified into two main types: block ciphers and stream ciphers (refer to Figure 1.1). A block cipher splits the plaintext message into consecutive blocks, where each block has the same block size (normally 128 bits), and then encrypt each block with the same key. While a stream cipher divides the plaintext message into consecutive characters (byte or sometimes unit larger than a byte) or bits and then encrypts each character or bit with one element of the key stream.

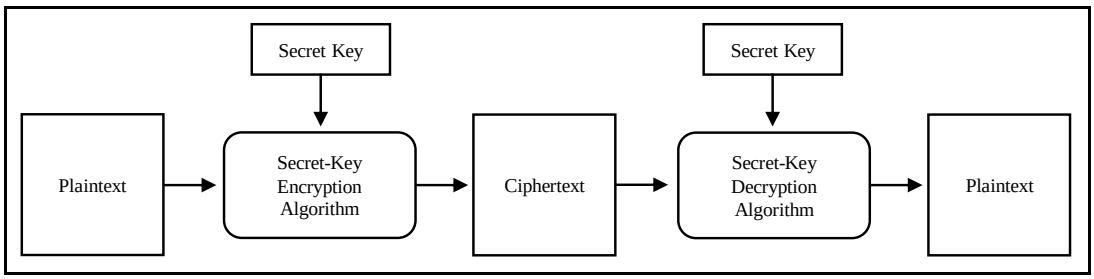

Figure 1.2: The concept of secret-key cryptography

Public-key cryptography is also known as asymmetric-key cryptography that has been suggested for solving the key distribution problem in the secret-key cryptography. Unlike secret-key cryptography, public-key cryptography does not use the same key to encrypt and decrypt a message. Instead, public-key cryptography uses two different keys but related mathematically; the public key which is known to everyone is used for encryption, and the corresponding private key which is kept

secret is used for decryption (refer to Figure 1.3). In addition, it is computationally infeasible to derive the private key from the public key (Ragab, 2004; Yahya, 2004; Amador et al., 2005; Stallings, 2006; Kessler, 2010). As shown in Figure 1.1, public-key cryptography can be classified into four main categories (Abhijit and Madhavan, 2009): key exchange, encryption, digital signature, and zero-knowledge proof of identity. In this research, we are focusing only on the public-key cryptography and its main categories as shown in Figure 1.1. A good explanation to public-key cryptography and its main types can be found in Chapter 2.

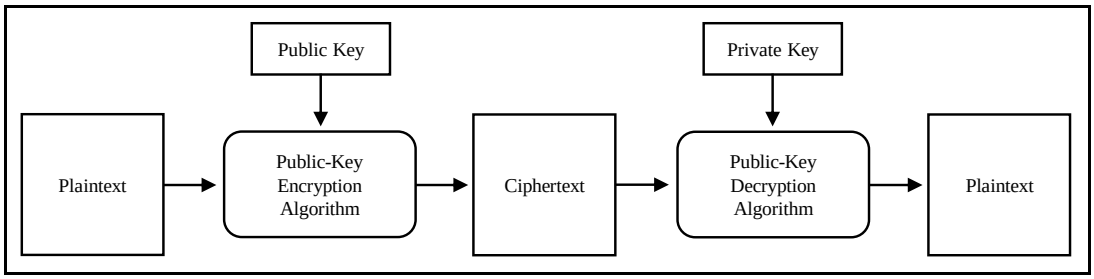

Figure 1.3: The concept of public-key encryption

Visual cryptography is a special type of cryptography for images (refer to Figure 1.1), in which it is based on the pixel level manipulation with Boolean operations (Hawkes et al., 2000; Fischer and Herfet, 2006; Pejaś and Zawalich, 2008). Visual cryptography is also known as the art of hiding pictures amongst other pictures (Busse, 2003).

The basic theory of visual cryptography was first introduced by Naor and Shamir in 1994 (Naor and Shamir, 1995) with their paper "Visual Cryptography". They proposed a perfectly safe method to solve the problem of encrypting written material (printed text, handwritten, notes, pictures, etc.) (Jessica, 2005).

The visual cryptography method divides the secret image into a set of shares (refer to Figure 1.4) and distributes those shares to participants. The secret image is

decrypted by using the properties of the human visual system without the need for complicated computations or mathematical primitives (Naor and Shamir, 1995; Biham and Itzkovitz, 1998; Jessica, 2005; Chan and Wu, 2008; Abdulla, 2010). Note that, pattern recognition by human visual system is a highly complex operation but can be done very casually by humans. The secret data seem to appear immediately when all or several of those transparency shares are stacked together according to the visual cryptography scheme used (Chan and Wu, 2008). The reconstruction secret image in visual cryptography schemes needs only the very simple Boolean 'OR' computation on the transparent shares which is done automatically by the human eye, while in the classical cryptographic systems, complex computer operations are required, comparatively.

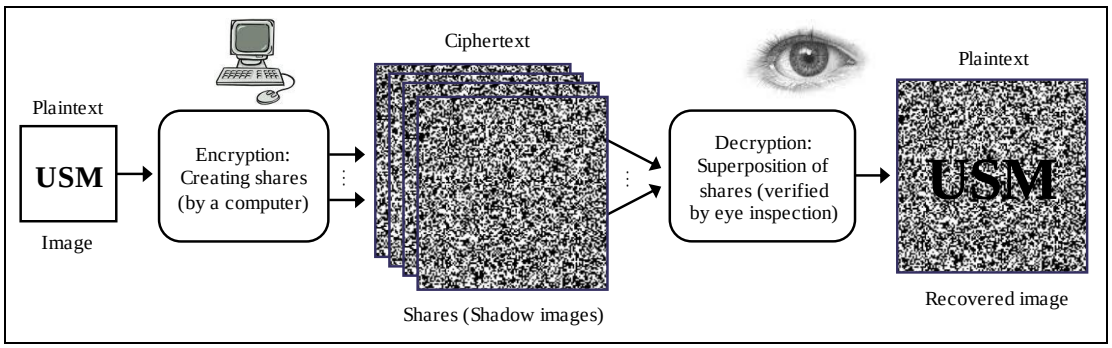

Figure 1.4: The concept of visual cryptography for black-and-white image

The characteristics of visual cryptography are (Yan et al., 2004; Patel, 2003):

- Simple to implement.
- Perfect security.
- The encryption does not need complex computations.
- The decryption can be done by human visual system (human eye) without any complex computations and without the assistance of a computing device.

The most important characteristic of the visual cryptography is the ability to recover the secret image without any calculations. It utilizes the human visual system to recover the secret image from some or all overlapping shares, therefore overcoming the drawback of the complex calculations needed in the conventional cryptographic systems (Hou, 2003). Note that the image recognition done by the human visual system is highly complex for a computer to imitate.

As shown in Figure 1.1, visual cryptography can be classified into two main models (types): conventional visual cryptography and non-expansion visual cryptography. A good explanation to visual cryptography and its main types can be found in Chapter 2.

Steganography is one of the trusted practical methods for performing information security. It is actually about finding the best place to hide an object in a way that is not recognized by others and at the same time does not affect the place that keeps the object. The word “Steganography” comes from Greek, which literally means “covered” or “hidden writing”. This lies in contrast to cryptography, where the enemy is allowed to detect, intercept and modify messages without being able to violate certain security premises guaranteed by a cryptosystem. The goal of steganography is to hide messages inside other harmless messages in a way that does not allow any enemy to even detect that there is a second secret message present (Johnson et al., 2001; Jaafar, 2003). Even though there are many implementations of steganography on the image domain, the fact is that visual cryptography and steganography are two sides of a coin. Steganography hides the existence of hidden data whereas the visual cryptography has the nature of revealing the existence of the hidden data (Jithesh and Senthil, 2010). Therefore, the work in this study is not related to steganography.

1.1 Motivation

The design of our research is motivated by the following points:

1. The existence of visual cryptography for sharing and encrypting images. Visual cryptography uses human visual system (human eye) to recover the secret without any complex decryption algorithms.
2. There is a need to construct new functional public-key cryptosystem, in which human visual system plays an important role in the decryption process.
3. Although there are many existing researches on secret-key visual cryptography, but there is no public-key visual cryptography research at the moment.
4. Use freely available but highly complex human visual system for decryption. Although humans cannot perform highly complex computations, but the human visual system can easily perform pattern recognition task which is a highly complex operation if it has to be done by a computer.

1.2 Research Questions

This research aims to answer the following questions:

- Can we achieve public-key concept for visual cryptography?
- Is non-expansion visual cryptography with Boolean operations can be used in public-key visual cryptography?

1.3 Research Problem

We conduct this study due to the importance of public-key cryptosystems in everyday life to attain and ensure privacy, authenticity, integrity, and non-repudiation of electronic information exchanges in the sphere of network communication.

The security of most currently available public-key cryptosystems is based on hard mathematical (difficulty number-theoretic) problems such as discrete logarithms in finite groups or integer factorization that require complex and heavy cryptographic computations. In general the two communicating parties must depend on high and powerful computing device (computer) to perform these computations. Until now, building a public-key cryptosystem with high security and without complex cryptographic computations has been a great challenge. Therefore, it is important to investigate new public-key cryptography primitives that require less complex cryptographic computations but relatively secure.

In this thesis, we proposed a new public-key cryptosystem with comparatively low and simple computations. The proposed public-key primitives are based on non-expansion visual cryptography and Boolean operations for overcoming the complex computations.

1.4 Research Scope

Our study in this thesis focuses on visual public-key cryptosystem (i.e., visual key exchange, visual digital signature, and visual zero-knowledge proof of identity) which have special advantages as we will mention in the following chapters. The scope of this research is limited to applying the concepts of the non-expansion visual cryptography and Boolean operations on the public-key concept for producing a new

model of visual public-key cryptosystem with a comparatively less complex computation.

1.5 Research Objective

Since the Boolean operation is simple, fast and very adaptive to visual cryptography, our proposed methods will use simple Boolean computations instead of complex and heavy cryptographic computations. Instead of generating and computing large and long random integer values and manipulating them by using computational heavy and complex operations as in the classical public-key cryptosystems, our methods in this study generates shadow images called visual shares and manipulates them by using simple Boolean operations.

In this study, we aim to combine the advantages of the non-expansion visual cryptography and Boolean operations with the concept of the public-key cryptography for overcoming the problems as stated in Section 1.3 and then producing a new public-key cryptosystem that requires less complex computations. The primary objectives of our research are:

- To introduce alternative methods to the classical public-key primitives based on non-expansion visual cryptography concept and Boolean operations with a comparatively low and simple computation.
- To assess the security of the proposed visual public-key cryptosystem which is based on the strength and the performance of the proposed visual public-keys algorithms.

1.6 Research Methodology

To achieve the objectives as stated in Section 1.5, this research follows the following research methodology:

- Perform a literature survey on the public-key cryptography and on the visual cryptography.
- Introduce new public-key primitives which are based on the idea of non-expansion visual cryptography and Boolean operations, as follows:
    1. Introduce a new key exchange algorithm based on non-expansion visual cryptography and Boolean operations.
    2. Introduce a new digital signature algorithm based on non-expansion visual cryptography and Boolean operation.
    3. Introduce a new zero-knowledge proof of identity algorithm based on non-expansion visual cryptography and Boolean operation.
- Perform security analysis and calculate computational complexity for the proposed visual public-key cryptosystem.
- Compare the proposed visual public-key cryptosystem with the current standard in public-key cryptosystems.

A general block diagram of the proposed method is shown in Figure 1.5. Figure 1.6 shows the main types of public-key cryptography and the proposed visual public-key cryptosystem.

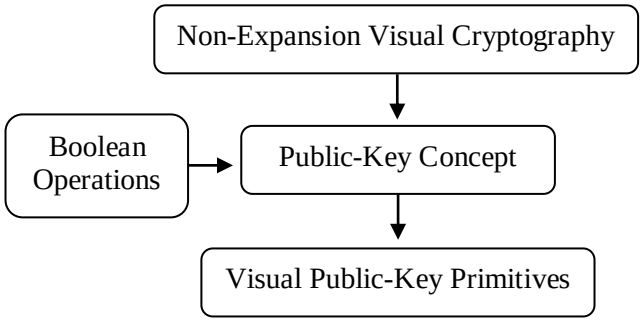

Figure 1.5: General block diagram of the proposed method

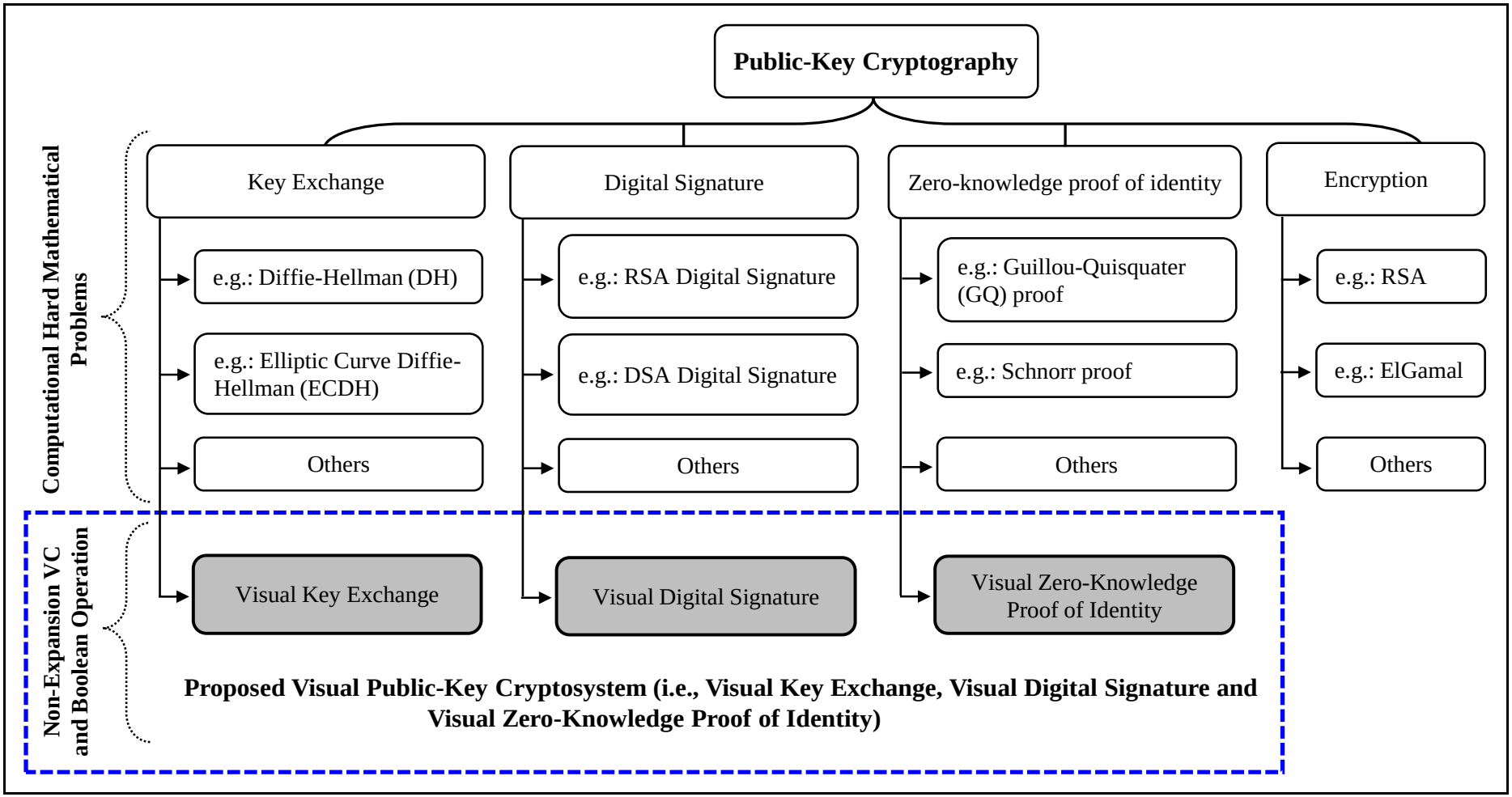

Figure 1.6: Main branches of public-key cryptography and the proposed visual public-key cryptosystem

1.7 Research Contribution

In general, this research has two main contributions. The first contribution is the introduction of the public-key visual cryptography model. The second contribution is the design and implementation of the new approaches to the visual public-key cryptosystem which are based on the non-expansion visual cryptography and Boolean operations. The outcome of this study is a new concept of public-key primitives cryptosystem which uses the human visual system for decryption without the need to rely on complex, heavy computations.

The proposed visual public-key cryptosystem in this study depends on Boolean computation, which is fast, simple and highly adaptable to visual cryptography. The proposed visual public-key cryptosystem have great impact on the field of information security and have a wide potential usage especially on visual based applications.

Chapters 3 and 4 in this thesis contain specification and explanation of the new visual public-key protocols and comparison between these protocols with the classical public-key algorithms. Additionally, an encryption scheme using the visual key exchange protocol (the proposed first protocol) and existing non-expansion visual cryptography is proposed. Such visual encryption scheme hypothetically should run faster than a dedicated visual public-key encryption protocol, as currently found in the conventional cryptosystem.

1.8 Thesis Organization

The work conducted in this thesis is organized in seven chapters with appendices. This chapter provides an introduction to the work by giving a brief

overview of the related concepts, the motivations, the problem, the questions, the scope, the objectives, the methodology and the contributions of this study.

In Chapter 2, we give an overview of the concepts of public-key cryptography and visual cryptography. The public-key cryptography is classified into four categories: key exchange, encryption, digital signature, and zero-knowledge proof of identity. The visual cryptography is classified into two models, conventional visual cryptography model, and non-expansion (probabilistic) visual cryptography model. The schemes of visual cryptography for every model are discussed in detail as well.

In Chapter 3, we explain the ideas of our new protocols as a new key exchange, a new digital signature and a new zero-knowledge proof of identity, based on the non-expansion visual cryptography and Boolean operations. In addition, we explain a new encryption scheme based on the visual key exchange protocol and the non-expansion visual cryptography.

Chapter 4 presents the security analysis and computational complexity analysis of our new visual public-key protocols. Brief performance comparisons between our new visual public-key protocols with the well-known conventional public-key algorithms are presented in this chapter. In addition, this chapter presents the security analysis and computational complexity of the new visual encryption scheme and also gives a brief performance comparison between the conventional encryption scheme and the proposed visual encryption scheme. Knowledge contribution of the research will also be explained.

Finally, Chapter 5 gives the conclusion and the future work for this study. The conclusion depends on the results which we have obtained through the implementation of the study to be clarified and summarized for the reader.

In Appendices A and B we gave some experimental examples which are used to help the reader to understand the work of conventional and non-expansion visual cryptography models. Appendix C gave basic information on invertible and non-invertible matrices and Appendix D gave basic information on *K*-satisfiability (*K-SAT*) problems especially the 3-*SAT* and 4-*SAT* cases.

CHAPTER 2

LITERATURE REVIEW

2.0 Introduction

The focus of this chapter is to review and discuss topics relevant to the current research work. In the first part of this chapter, an overview of public-key cryptography and its categories is provided. Thereafter, an introduction on the concept of visual cryptography is given, describing the visual cryptography models and techniques from the literature.

This chapter is organized into four main sections, based on the literature survey of the public-key and visual cryptography. Section 2.1 provides the definition and purpose of public-key cryptography. Section 2.1 is further divided into subsections. These subsections explain and discuss the categories of public-key (asymmetric-key) cryptography, namely; the key exchange, the public-key encryption, the digital signature and the zero-knowledge proof of identity. Section 2.2 concentrates on the definition and purpose of visual cryptography. This section is also divided into subsections, which review the types of visual cryptography models with their schemes for black-and-white (binary) images and illustrates the important applications of visual cryptography. In Section 2.3, a brief comparison between the public-key cryptography and visual cryptography is made. Finally, Section 2.4 provides a summary for the chapter.

2.1 Public-Key (Asymmetric-Key) Cryptography

Public-key cryptography is one of the key contributions in the history of cryptography. In 1976, Diffie and Hellman (Diffie and Hellman, 1976) introduced the first concept of public-key (asymmetric-key) cryptography, to solve the problem of key exchange, which is associated with secret-key (symmetric-key) cryptography. Public-key cryptography has a pair of keys; one key is known as the public key which is publically known by the public and another key is the private key which is kept secret by the owner (Jaafar and Samsudin, 2010a; RSA Laboratories, 2010). Using public-key cryptography mechanism, all communications between two parties over an open network involves only the public keys, without the need for the exchange of any private keys (Anoop, 2007).

In recent times, public-key cryptosystems are being used in everyday life, to attain privacy, authenticity, integrity and non-repudiation in the sphere of network communications (Chen, 2004; Laih and Chen, 2004; Stallings, 2006). Currently, most public-key algorithms are based on the difficulty to compute and solve hard mathematical problems which require computationally heavy and complex operations (Aladdin R&D Team, 2000; Lenstra, 2006). Additionally, these problems can be classified into two main categories based on their running time, Polynomial (*P*) time and Non-deterministic Polynomial (*NP*) time. The problem is said to be in *P* if it can be solved by deterministic algorithm in polynomial time, whereas it is in *NP* if it can be solved by nondeterministic algorithm in polynomial time (Menezes et al., 1996; RSA Laboratories, 2010).

Figure 2.1 shows the most important, conventional public-key cryptography which can be categorized into key exchange, public-key encryption, digital signature and zero-knowledge proof of identity; where each category includes many different

algorithms. The following subsections discuss and explain each category of the public-key cryptography with practical examples.

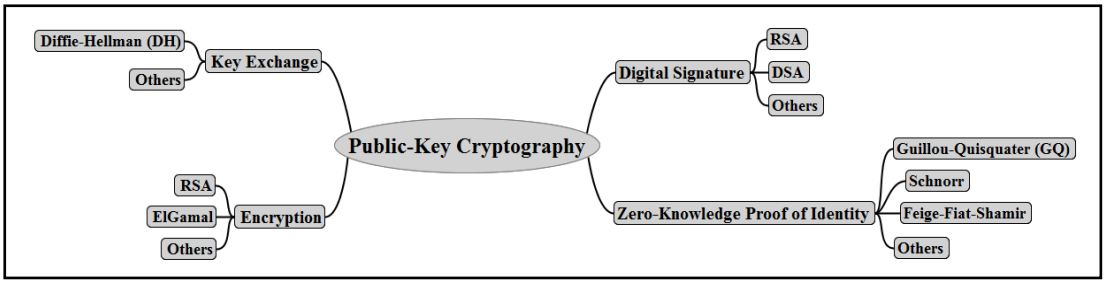

Figure 2.1: Major categories of public-key cryptography

2.1.1 Key Exchange

The first important method in public-key cryptography is key exchange which ensures the confidential construction of a shared secret key between two parties, in real-time and on an open network. A shared secret key could enable two parties, who may not have had any previous communication, to encrypt their communications (Carts, 2001; Palmgren, 2005).

2.1.1.1 Diffie-Hellman (DH) Key Exchange Protocol

Whitfield Diffie and Martin Hellman (Diffie and Hellman, 1976) proposed an interesting protocol, the Diffie-Hellman (DH) key exchange protocol, to ensure secure communications without the need of exchanging secret data. In this regards, they amazed the computer security world in 1976 with their paper "New Directions in Cryptography", which introduced the idea of public-key cryptography (Diffie and Hellman, 1976; Hellman, 1978; Ford, 1994; Palmgren, 2005; Stallings, 2006).

The DH key exchange protocol was fundamentally different from all other previous cryptography methods for two major reasons. First, it uses two different keys, namely; public and private keys which are mathematically linked, instead of one shared secret key commonly used in symmetric-key cryptography. Second, it is based on mathematical problems which require heavy cryptographic computations, instead of substitution and permutation (Carts, 2001; Xue, 2007).

The DH key exchange protocol begins when each of the parties (users *A* and *B*) generates a private key. Each party then generates the corresponding public key. Note that the public key is derived from the private key, and the two keys are mathematically linked. The two parties then exchange their public keys. Each party now has its own private key and the other party's public key. So, the two parties can compute a unique shared key, which is known only to both of them. In order to have confidence in this scheme, it must be accepted that it is computationally impossible to derive the private key from the public key (Diffie and Hellman, 1976; Hellman, 1978; Ford, 1994; Palmgren, 2005; Stallings, 2006).

Suppose that the users *A* and *B* (Alice and Bob) want to exchange a key between them. The DH key exchange protocol (refer to Figure 2.2) works as follows (Diffie and Hellman, 1976):

Initial parameters: Alice and Bob agree on two publicly known parameters: a prime number *P* and an integer *G*, which is a primitive root of *P*.

The protocol: It consists of the following two stages.

1. **First stage:** Alice builds her public key and Bob builds his public key. Below are the details of this stage, which is performed simultaneously by Alice and Bob.

   Steps generated by user *A* (Alice)

   - Chooses a random private integer, $X_A < P$.

- Calculates her public key Y_A, as follows: $Y_A = G^{X_A} \bmod P$.
- Sends her public key Y_A to Bob.

Steps generated by user *B* (Bob)

- Chooses a random private integer, $X_B < P$.
- Calculates his public key Y_B, as follows: $Y_B = G^{X_B} \bmod P$.
- Sends his public key Y_B to Alice.

2. **Second stage:** Alice calculates the shared secret key K_A and Bob calculates the shared secret key K_B, where K_A and K_B are identical keys. Below are the details of this stage for Alice and Bob.

   Steps generated by user *A* (Alice)

   - Receive Bob's public key Y_B.
   - Calculates the shared secret key K_A, as follows: $K_A = (Y_B)^{X_A} \bmod P$.

   Steps generated by user *B* (Bob)

   - Receive Alice's public key Y_A.
   - Calculates the shared secret key K_B, as follows: $K_B = (Y_A)^{X_B} \bmod P$.

Figure 2.2 shows the work of conventional Diffie-Hellman key exchange protocol.

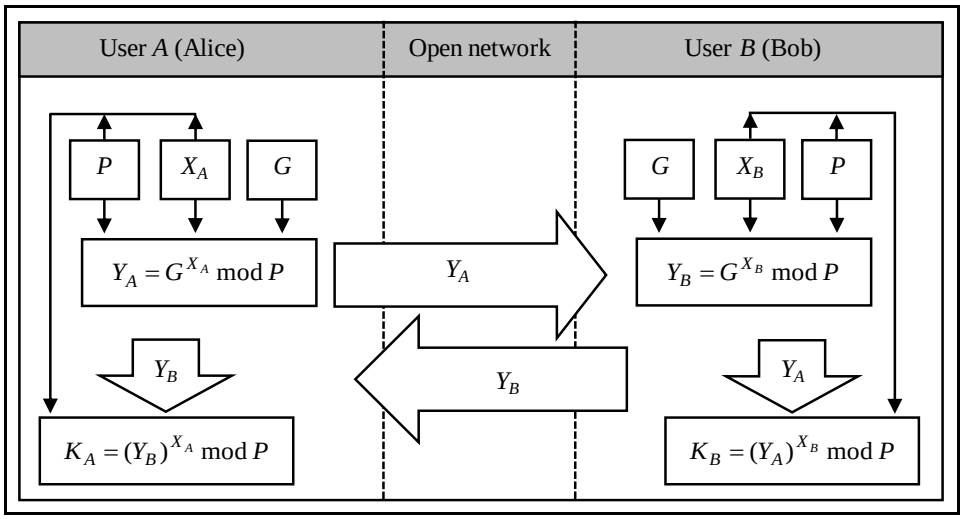

Figure 2.2: The conventional Diffie-Hellman (DH) key exchange protocol (adapted from Ford, 1994)

DH key exchange is an interesting and widespread protocol which is accessible in numerous connectivity protocols. At a time when the lifespan of old technologies are calculated in months, this protocol is almost celebrating its 34th anniversary and is still playing an active role in important Internet protocols. The security of the DH key exchange protocol is established under the assumption that calculating discrete logarithms is a hard problem. The task of calculating discrete logarithms for large prime numbers is considered unfeasible, where the large prime numbers exceed 1024 bits (Diffie and Hellman, 1976; Carts, 2001; Rothe, 2005; Stallings, 2006; Elaine et al., 2006).

Example 2.1 This is a working example of the Diffie-Hellman key exchange protocol with small numbers. In this example, Alice and Bob agree to use a prime number $p = 23$ and an integer $G = 5$. Alice generates her private number $X_A = 6$, and computes $Y_A = G^{X_A} \bmod p = 5^6 \bmod 23 = 8$, then sends Bob $Y_A = 8$. Similarly, Bob generates his private number $X_B = 15$, and computes $Y_B = G^{X_B} \bmod p = 5^{15} \bmod 23 = 19$, then sends Alice $Y_B = 19$. After that, Alice calculates $K_A =$

$Y_B^{X_A} \bmod p = 19^6 \bmod 23 = 2$. Similarly, Bob calculates $K_B = Y_A^{X_B} \bmod p = 8^{15} \bmod 23 = 2$. Note that both Alice and Bob have arrived at the same value ($K = K_A = K_B$).

In real implementation, normally, the shared secret key that is being established by DH key exchange protocol is used to encrypt and decrypt the subsequent communications using faster symmetric-key (secret-key) cipher.

2.1.2 Public-Key Encryption

The public-key encryption is one of the main branches and applications of the public-key cryptography proposed in 1976 by Diffie-Hellman (Diffie and Hellman, 1976). Public-key encryption allows two parties to communicate securely over an insecure channel, without having prior knowledge of each other to establish a shared secret key. Using public-key encryption mechanism, all communications between two parties over an unprotected channel involves only public keys and without the need for exchanging the private (secret) key (Anoop, 2007). Public-key encryption depends on two different keys, but which are mathematically linked. The first key, the public key, is put in a public and used for encryption while the second key is the private (secret) key, which is kept secret and used for decryption. In addition, it is computationally difficult to derive the private key from the public key (Hellman, 1978; Amador et al., 2005; Stallings, 2006; Xue, 2007). In the process of encryption, the sender encrypts his or her confidential information in such a way that only the intended recipient can decrypt the confidential information (Anoop, 2007; Jaafar and Samsudin, 2010a).

Figure 2.3 shows the concept of public-key encryption technique. For this system, suppose that the receiver, Bob, has private and public keys, which are (PR_R)

and (PU_R) respectively. The receiver's public key (PU_R) is publicly known, used for encryption and the receiver's private key (PR_R) is kept secret, used for decryption. Suppose that the sender, Alice, wants to send an original secret message (*SM*) to the receiver (Bob), Alice (the sender) encrypts her secret message (*SM*) using Bob's public key (PU_R) to get the encrypted secret message, which is known as cipher message (*CM*), and sends it to Bob (the receiver). The receiver (Bob) could thus decrypt the cipher message (*CM*) by using only his private key (PR_R).

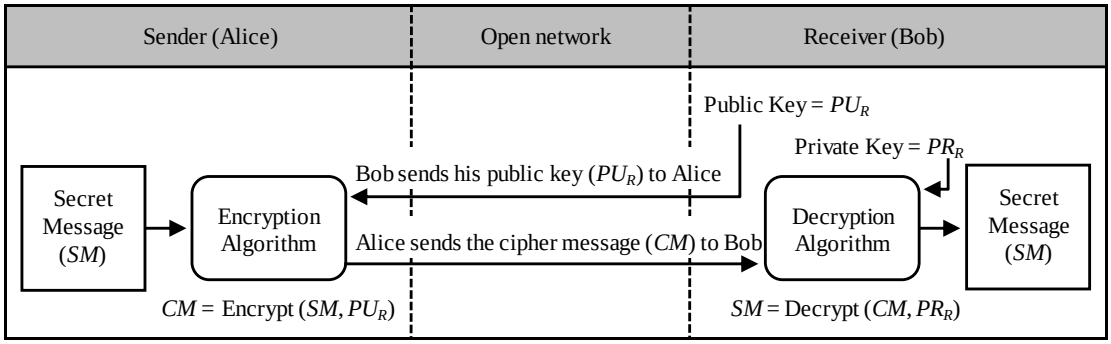

Figure 2.3: The concept of public-key encryption technique

Some public-key encryption algorithms are popular, for example; RSA, ElGamal and ECC (Elliptic Curve Cryptograph). The RSA public-key encryption algorithm invented by Rivest, Shamir and Adleman in 1977 and was published in 1978 (Rivest et al., 1978) is the first practical encryption algorithm, based on the concept of the public-key cryptography. ElGamal public-key encryption algorithm (ElGamal, 1985) and elliptic curve public-key encryption algorithm (Koblitz, 1987) on the other hand are among the popular public-key encryption algorithms published after the RSA. The security of most of the public-key encryption algorithms is based on discrete logarithms in finite groups or integer factorization (Laih and Chen, 2004; Amador et al., 2005; Stallings, 2006).

2.1.2.1 The RSA Public-Key Encryption Algorithm

The Rivest-Shamir-Adleman (RSA) is one of the most widely used public-key encryption algorithm. The security of the RSA algorithm is based on the difficulty of factoring large primes. Normally, 1024-2048 bits lengths of numbers are used, which make the computation very expansive. With the 1024-2048 bits key, the RSA is considered secure against brute force attack (Rivest et al., 1978; Stallings, 2006; Elaine et al., 2006; Alia, 2008). Figure 2.4 shows the RSA public-key encryption protocol.

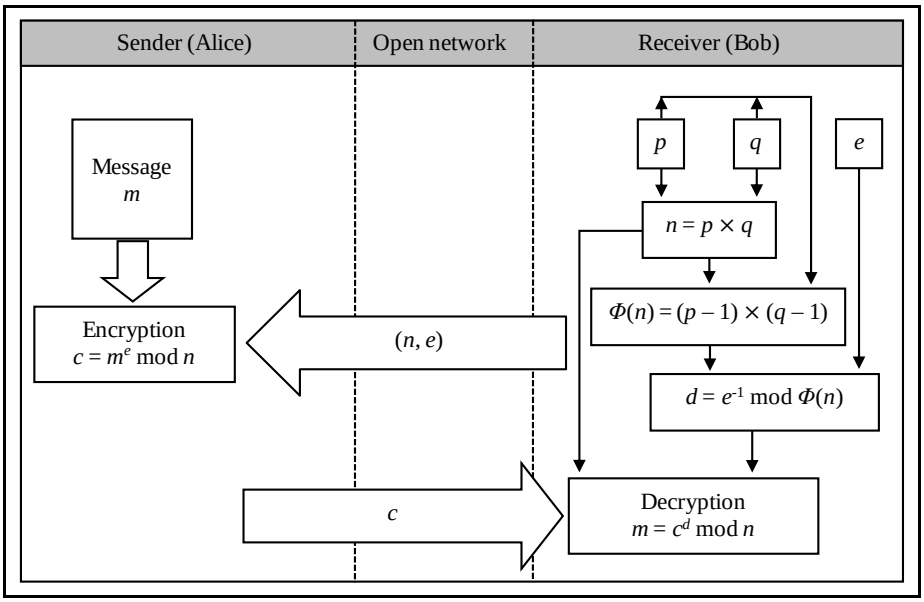

Figure 2.4: RSA public-key encryption protocol

Typically, the RSA public-key encryption algorithm consists of three phases, as follows:

1. **A key generation phase:** In this phase, the receiver (Bob) generates the public key (n, e) and the corresponding private key (n, d). The details of this phase are as follows:

- Generate randomly, two large prime numbers (p, q) which are secret and of roughly the same length in bits, but which must not be equal and not close to each other.
- Compute; $n = p \times q$, where n is the product of the two prime numbers (p, q).
- Compute; $\Phi(n) = (p - 1) \times (q - 1)$.
- Choose a random integer number e, such that $1 < e < \Phi(n)$ and $gcd(e, \Phi(n)) = 1$.
- Compute the private key d, such that $d = e^{-1} \bmod \Phi(n)$.
- Public key is (n, e) and private key is d.

2. **Encryption phase:** This phase is carried out by a sender (Alice) who intends to send a message m to the receiver (Bob). The details of this phase are as follows:
   - Get the receiver's public key (n, e).
   - Represent the message as a positive integer m, $0 < m < n$.
   - Compute the encrypted message $c = m^e \bmod n$.
   - Send the encrypted message c to the receiver.

3. **Decryption phase:** This phase is generated by a receiver (Bob). The details of this phase are as follows:
   - Get the encrypted message c from the sender.
   - Recover the original message m, $m = c^d \bmod n$.

Example 2.2 This is a working example of the RSA public-key encryption algorithm with small numbers. In this example, the receiver (Bob) chooses $p = 47$, $q = 71$, and computes $n = p \times q = 47 \times 71 = 3337$ and $\Phi(n) = (p-1) \times (q-1) = (47-1) \times (71-1) = 3220$. Also Bob chooses $e = 79$ and computes the private key (decryption key) $d = e^{-1} \bmod \Phi(n) = (79)^{-1} \bmod 3220 = 1019$. He sends his public key $(n, e) = (3337, 79)$ to sender. The sender (Alice) chooses the message $m = 688$ and computes the encrypted message $c = m^e \bmod n = (688)^{79} \bmod 3337 = 1570$. She sends the encrypted message $c = 1570$ to Bob. When Bob receives the encrypted message c, he uses his private key $d = 1019$ to recover the message m, $m = c^d \bmod n = (1570)^{1019} \bmod 3337 = 688$.

2.1.2.2 ElGamal Public-Key Encryption Algorithm

In 1985, Taher ElGamal (ElGamal, 1985) proposed an alternative to the RSA for both public-key encryption and digital signature. The ElGamal algorithm is based on the Diffie-Hellman key exchange protocol therefore; the security of the ElGamal algorithm depends on the difficulty of computing the discrete logarithms in a large prime modulus. The encryption in the ElGamal algorithm is probabilistic because the same plaintext gives a different ciphertext each time it is encrypted. Figure 2.5 shows the ElGamal public-key encryption protocol.