جمهورية العراق

وزارة التعليم العالي والبحث العلمي

جامعة ديالى/كلية العلوم/ قسم الرياضيات

نظام تشفير هجين يعتمد على شفرة الهيل وعدد كاوسيان الصحيح و بروتوكول ذو المراحل الثلاث

رسالة مقدمة

إلى/جامعة ديالى/كلية العلوم/ قسم الرياضيات و هي جزء من متطلبات نيل شهادة الماجستير في علوم الرياضيات

من قبل الطالبة

آيات علي جعفر

بأشراف

أ. م. د. رفعت زيدان خلف

1444هـ

2022م

Chapter One
Theoretical Background

Chapter One

Theoretical Background

1.1 Introduction

This chapter includes the basic theoretical aspects of recognition system in the mathematical background that we need to use in this work and the definitions, concepts, and systems used in improving the discussed and also it presents the background for various necessary preprocessing issues and techniques that had been including concepts of number theory and linear algebra with the appraisal of cryptography and its types such as symmetric and asymmetric.

1.2 Mathematical Background

The following section of the chapter provides a mathematical background that includes the concepts, definitions, used in this thesis.

1.2.1 Linear Algebra [12]

1-Vector space over R:

A set of **V** with two binary operation: an (addition and scalar (number) multiplication of vectors in $\mathbb{R}^n$) so that

$Let \quad B, Y \in \mathbb{R}^n, \quad B = (b_1, b_2, \dots\dots, b_n), Y = (y_1, y_2, \dots, y_n)$ then:

$$B + Y = (b_1, b_2, \dots\dots, b_n) + (y_1, y_2, \dots\dots, y_n)$$

$$= b_1 + y_1, b_2 + y_2, \dots, b_n + y_n$$

$$a.B = a.(b_1, b_2, \dots\dots\dots, b_n) = a.b_1, ab_2, \dots, ab_n, \quad where \quad a \in R$$

2. Eigen values and Eigen vectors:

Let A be an $n \times n$ matrix. The real number λ is called an Eigen value of A if there exists a nonzero vector X in R^n such that

$$AX = \lambda X \quad \dots \quad (1)$$

Every nonzero vector X satisfying (1) is called an eigenvector of A associated with the Eigen values λ.

Example $(1.2.1)$

Let $A = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$, then

$$A\begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix} = 0\begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

So that $X_1 = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$ is an eigenvector of A associated with the eigenvalue $\lambda_1 = 0$, also

$X_2 = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$ is an eigenvector of A associated with the eigenvalue $\lambda_2 = 1$.

1.2.2 The inverse of a matrix[12]:

Let a be a given real number. Since 1 is the multiplicative identity in the set of real numbers, if a number b exists such that

$$ab=ba=1,$$

then b is called the reciprocal or multiplicative inverse of a and denoted a^{-1} (or $1/a$). The analog of this statement for square matrices reads as follows. Let A be a given n x n matrix. Since $I = I_n$ is the multiplicative identity in the set of n x n matrices, if a matrix B exists such that :

$$AB=BA=I$$

then B is called the (multiplicative) inverse of A and denoted A^{-1} (read A inverse).

Example (1.2.2):

If $A = \begin{bmatrix} 3 & 4 \\ -7 & -9 \end{bmatrix}$ then $A^{-1} = \begin{bmatrix} -9 & -4 \\ 7 & 3 \end{bmatrix}$

Since $A\,A^{-1} = \begin{bmatrix} 3 & 4 \\ -7 & -9 \end{bmatrix}\begin{bmatrix} -9 & -4 \\ 7 & 3 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I$

And $A^{-1}A = \begin{bmatrix} -9 & -4 \\ 7 & 3 \end{bmatrix}\begin{bmatrix} 3 & 4 \\ -7 & -9 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I$

1.3 Definitions and Basic Concepts: Number Theory

Definition 1.3.1 : Greatest common divisor (GCD)[13]:

Let p and q be two integers , at least one of the integers cannot be zero .Greatest common divisor (GCD) of p and q is the positive integer denoted by $d=gcd\,(p,q)$ satisfying:

1. d is divisible by p and q.
2. If c is divisible by p and q, then $c \leq d$.

Definition 1.3.2:[14]

Both integers p and q are named **relatively prime** when gcd(p, q) = 1.

Theorem 1. 3. 3 : (The Division Algorithm)[15]:

Given integers p and q, with $q > 0$, there are unique integers m and r so that $p = q.m + r$, with $0 \leq r < q$. p is named the dividend, r represents the remainder, q represents the divisor and m represents the quotient.

Lemma 1.3.4:[15]

Let p and q are two integers. when $p = q.m + r$, then,

$$gcd(p,q) = gcd\,(q,r).$$

Theorem 1.3.5:(Euclidean algorithm)[16]

Let p and q be two positive integers, where $p > q$ and consider the following sequence of repeated divisions:

$$\begin{aligned}
p &= q.a_1 + r_1 \quad , \quad 0 < r_1 < q \\
q &= r_1.a_2 + r_2 \quad , \quad 0 < r_2 < r_1 \\
r_1 &= r_2.a_3 + r_3 \quad , \quad 0 < r_3 < r_2 \\
r_2 &= r_3.a_4 + r_4 \quad , \quad 0 < r_4 < r_3 \\
&\vdots \\
r_{n-2} &= r_{n-1}.a_n + r_n \quad , \quad 0 < r_n < r_{n-1} \\
r_{n-1} &= r_n.a_{n+1} + 0
\end{aligned}$$

Then $gcd(p, q) = r_n$, the final remainder of non-zero remainder related to the process of division.

Definition modulus (MOD) 1.3.6[17]:

A modulo n, sometimes known as a mod n, is the remainder of the Euclidean division of two positive numbers, a and n, where a is the dividend and n is the divisor.

$a = n\,q + r$

$q = a/n$, q = quotient

$0 \leq r < n$

$r = a \bmod n$

1.4 Cryptography background

In this section, we will state some definitions, concepts, and profiles in the theory of numbers which will be needed to design and implement the proposed system.

1.4.1 Introduction to Cryptography

Strictly speaking, cryptography begins with the origin of writing the language back in 2000 BC the Egyptians used hieroglyphs to communicate between a selected class of people, usually the higher nobility[18].

In ancient Greece, secret writing was established by the so called scythe that became famous for its military purpose by the Spartans. From ancient Rome, the famous Caesar cipher arose. The first attempts at cryptography are certainly rooted in historical traditions. Without these early attempts at secure communication, it is controversial whether there is the individual or corporate privacy nowadays[19].

Modern cryptography may be separated into the following areas (Figure 1.1). Cryptology combines the studies of the two branches of cryptanalysis and cryptography.

Describes analyzing and diagnosing a cipher, discovering its weak points, and then performing the cipher cracking process.

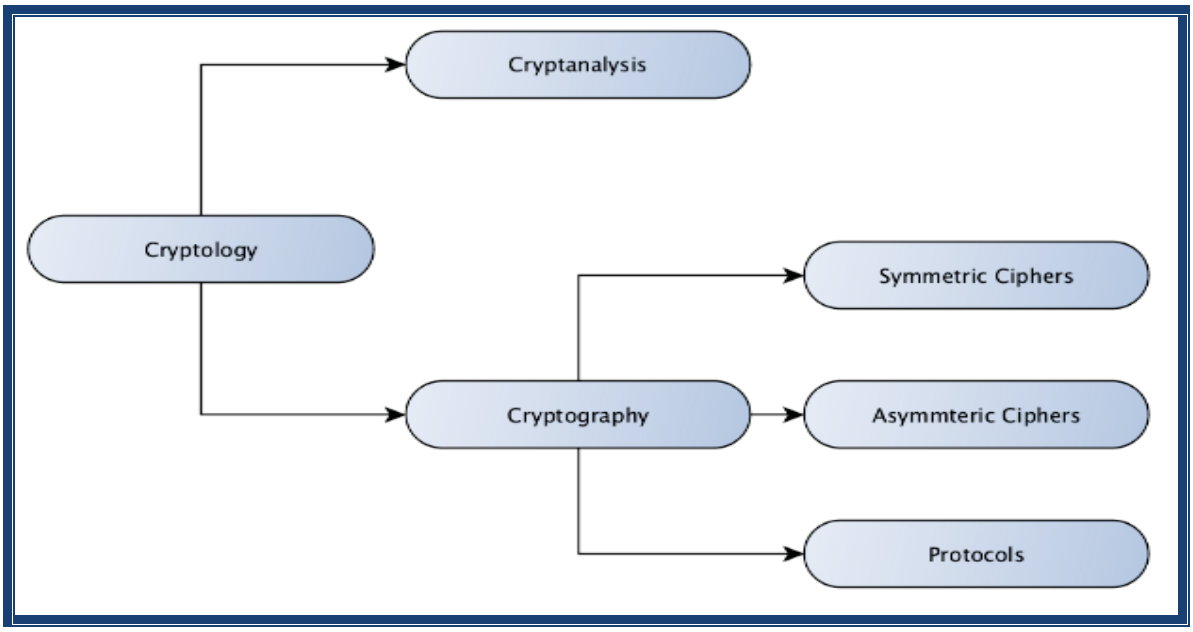

Figure 1.1 Areas of expertise in cryptology

Cryptography is derived from the two Latin words crypt and graph (in plain English, secret and writing) and is therefore referred to as the science of secret writing. It serves the cause of hiding confidential information (also called plaintext) within a message. Cryptography can be implemented by three different approaches, symmetric Ciphers, Asymmetric Ciphers, and Protocols(Figure 1.1).

Cryptography should provide some of the Following:

Confidentiality:

Even if public communication channels are used, information about the content of secured communication should not be gained.

Data integrity:

An unauthorized tempering of content from secured communications should not be possible even if an adversary has access to the communication channel.

Data origin authentication:

Unwarranted modification and/or misrepresentation of the true origin of some communication should be averted.

The basic algorithm for cryptography (and so to speak, for all encryption methods) is outlined in the equation:

Plaintext = Decrypted (Encrypted Plaintext)[22].

1.4.2 Symmetric Key Algorithm

Algorithms that use an identical key for encrypting plaintext and decrypting a coded Message (Figure 1.2) are called symmetric key algorithms. In some cases, symmetric key algorithms also use similar functions for encryption and decryption (e.g. the Data Encryption Standard

(DES) uses widely identical functions). The major drawback of these algorithms is that all parties who are involved in the secure communication need to have the key, as well as the particular function for encryption and decryption.

The transmission of the key or the so-called shared secret needs to be carried out through a secure communication link to prevent the compromise of encrypted communications[23].

Once the key is exchanged, further communications can be carried out using hopefully faster/more convenient public communication channels. As a drawback of the symmetric key algorithm, it must be admitted, that there is a problem with the potentially large number of keys: As each communication group holds its key.

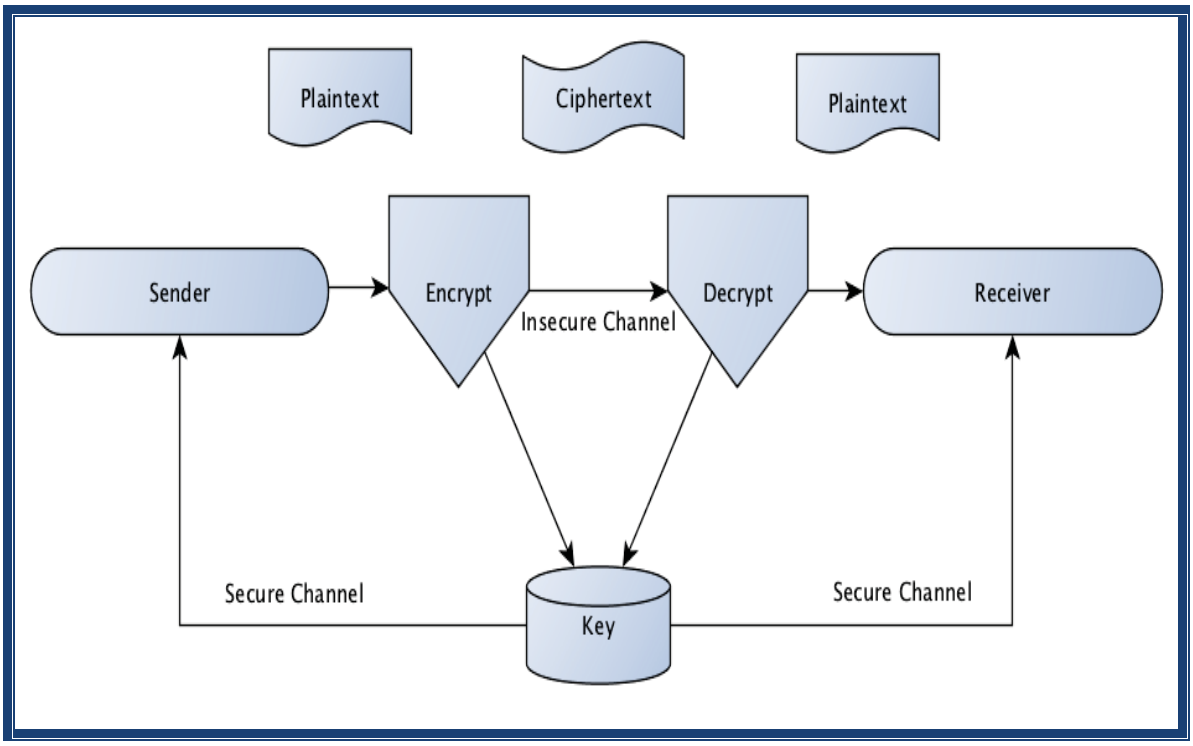

Figure 1.2 Basic proceeding of symmetric key algorithms

1.4.3 Asymmetric/Public-Key Algorithm

The invention of Public-Key algorithms (also called asymmetric key algorithms) goes back to the year 1979 when Whitfield Diffie and Martin Hellman proposed "new directions In cryptography" (Diffie and Hellman,1976). This milestone paper introduced how two parties could communicate privately with two different keys using a public channel (see Figure 1.3). The first key, the encryption key, is different and cannot be calculated (within a meaningful time) from the second key, the decryption key. In other words, it is not necessary to keep the Public-Key for encrypting a plaintext secret as long as the Private Key for decrypting the cipher text is confidential.

With this approach, even an intruder could encrypt messages but still cannot decrypt a cipher text without the corresponding Private Key. Using this approach, the key is only a secret of one person/entity and not a secret of a pair or group of entities like with symmetric key algorithms [24].

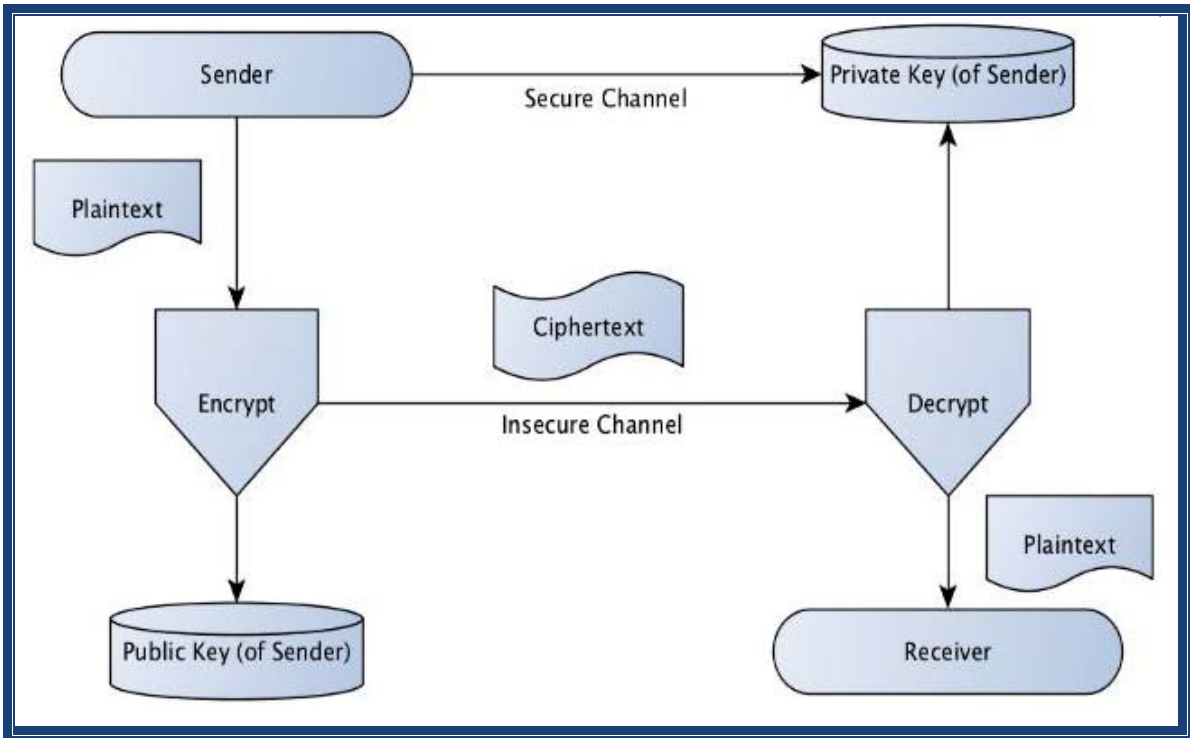

Figure 1.3 Basic proceeding of asymmetric key algorithms

1.4.4 Cryptanalysis:[25]

Cryptanalysis is the study of studying information systems to learn about their hidden components (from the Greek kryptós, "hidden," and analein, "to analyze"). Even when the cryptographic secret is unknown, cryptanalysis is used to circumvent cryptographic security measures and access the contents of encrypted messages.

Cryptanalysis also involves the study of side-channel attacks, which do not aim to exploit flaws in the cryptographic algorithms themselves but rather flaws in their implementation. This is in addition to the mathematical analysis of cryptographic algorithms.

The study of decrypting encrypted messages is known as cryptanalysis. Cryptologists, mathematicians, and other scientists involved in the process are presumed to be lacking the secret key required for encryption and decryption through cryptanalysis. This type of cryptosystem weak points investigation is distinct from a brute force attack.

1.4.5 The Entropy[26]:

Entropy is the term used in cryptography to describe the unpredictability that is gathered by a system for use in algorithms that need random data. A cryptosystem may become susceptible and unable to properly encrypt data if it has insufficient entropy.

المستخلص

أصبح استخدام التشفير أمرًا بالغ الأهمية في عالم التكنولوجيا. يتطلب نقل البيانات عبر القنوات الرقمية تقنيات لمنع تعرض البيانات للهجوم. شفره هيل هي طريقة التشفير الشائعة ؛ لذلك ، تم إدخال العديد من التقنيات. يستخدم هذا النوع من أنظمة التشفير مفتاحًا واحدًا لعملية التشفير وفك التشفير. في هذه الرسالة، سنعمم مفهوم شفره هيل على الأعداد الصحيحة الغاوسية و اقتراح طريقة تنفيذ بروتوكول التمريرات الثلاثية في شفره هيل على الأعداد الصحيحة الغاوسية. الأعداد الصحيحة الغاوسية في نظرية الأعداد هي أعداد عقديه، بحيث تكون أجزائها الحقيقية والخيالية أعدادًا صحيحة. حلقات الأعداد الصحيحة الغاوسية متشابهة مع الحلقات الصحيحة العادية. لذلك ، فإن الطريقة المقترحة أقوى من الطريقة الكلاسيكية لأن مهاجمة الطريقة المقترحة تحتاج إلى ضعف الوقت اللازم لمهاجمة شفره هيل الكلاسيكي.

وأخيرًا ، تم اقتراح طريقة إنشاء مصفوفة ذاتية الانعكاس لخوارزمية شفره هيل على الأعداد الصحيحة الغاوسية. لا يوجد دائمًا معكوس المصفوفة المستخدمة لتشفير النص العادي. لذلك ، إذا لم تكن المصفوفة قابلة للانعكاس ، فلا يمكن فك تشفير النص المشفر. في طريقة إنشاء المصفوفة ذاتية الانعكاس ، تكون المصفوفة المستخدمة للتشفير هي نفسها قابلة للعكس. لذلك ، أثناء فك التشفير ، لا نحتاج إلى إيجاد معكوس المصفوفة. علاوة على ذلك ، تقضي هذه الطريقة على التعقيد الحسابي الذي ينطوي عليه إيجاد معكوس المصفوفة عند فك التشفير في شفره هيل .