CAPITAL UNIVERSITY OF SCIENCE AND TECHNOLOGY, ISLAMABAD

Cryptanalysis of Matrix based Digital Signature and Encryption Schemes based on Block Cipher

by

Khushba Mumtaz

A thesis submitted in partial fulfillment for the degree of Master of Philosophy

in the
Faculty of Computing
Department of Mathematics

2020

To my parents, teachers and friends for their support and love.

CERTIFICATE OF APPROVAL

Cryptanalysis of Matrix based Digital Signature and Encryption Schemes based on Block Cipher

by

Khushba Mumtaz

(MMT173007)

THESIS EXAMINING COMMITTEE

S. No.	Examiner	Name	Organization
(a)	External Examiner	Dr. Ayesha Rafiq	IST, Islamabad.
(b)	Internal Examiner	Dr. Muhammad Afzal	CUST, Islamabad.
(c)	Supervisor	Dr. Rashid Ali	CUST, Islamabad.

Dr. Rashid Ali
Thesis Supervisor
May, 2020

Dr. Muhammad Sagheer
Head
Dept. of Mathematics
May, 2020

Dr. Muhammad Abdul Qadir
Dean
Faculty of Computing
May, 2020

Author's Declaration

I, **Khushba Mumtaz** hereby state that my M.Phil thesis titled "**Cryptanalysis of Matrix based Digital Signature and Encryption Schemes based on Block Cipher**" is my own work and has not been submitted previously by me for taking any degree from Capital University of Science and Technology, Islamabad or anywhere else in the country/abroad.

At any time if my statement is found to be incorrect even after my graduation, the University has the right to withdraw my M.Phil Degree.

(Khushba Mumtaz)
Registration No: MMT173007

Plagiarism Undertaking

I solemnly declare that research work presented in this thesis titled "**Cryptanalysis of Matrix based Digital Signature and Encryption Schemes based on Block Cipher**" is solely my research work with no significant contribution from any other person. Small contribution/help wherever taken has been dully acknowledged and that complete thesis has been written by me.

I understand the zero tolerance policy of the HEC and Capital University of Science and Technology towards plagiarism. Therefore, I as an author of the above titled thesis declare that no portion of my thesis has been plagiarized and any material used as reference is properly referred/cited.

I undertake that if I am found guilty of any formal plagiarism in the above titled thesis even after award of M.Phil Degree, the University reserves the right to withdraw/revoke my M.Phil Degree and that HEC and the University have the right to publish my name on the HEC/University website on which names of students are placed who submitted plagiarized work.

(Khushba Mumtaz)
Registration No: MMT173007

Acknowledgements

All praise be to **Almighty ALLAH** who has been bestowing me with his great bounties, gifted me a loving family and excellent teachers and enabled me to complete my dissertation.

I would like to express my special gratitude to my kind supervisor **Dr. Rashid Ali** for his constant motivation. He was always there whenever I found any problem. I really appreciate his efforts and guidance throughout my thesis and proud to be a student of such kind supervisor.

Also, many thanks are due to all teachers of CUST Islamabad, **Dr. Muhammad Sagheer, Dr. Abdul Rehman Kashif, Dr. Shafqat Hussain, Dr. M. Afzal, Dr. Dur-e-Shehwar and Dr. Samina Rashid** for conveying the excellent lectures.

I am grateful to the management staff of **Capital University of Science and Technology, Islamabad** for providing a friendly environment for studies.

I am thankful to all of my family members for becoming a bulwark of patience and support during my research work. However, my deepest gratitude is reserved for my Parents for their earnest prayers, unconditional love and unflinching support in completing my degree program. They supported and encouraged me throughout my life. I truly appreciate my father for all the prayers, without them, I would not have finished my degree.

I would also like to show my gratitude to my seniors specially, **Sir Tahir, Sir Awais** for guidance. Especially, I would like to acknowledge **Mr. Umer Zahoor** for their continuous support and patience during my research work. I remember the countless hours we were trying to learn and compile our Latex files to create the presentable output. He always drove me towards my goal.

Finally, I am obliged to all people who have shared their knowledge and supported me all along.

(Khushba Mumtaz)

Registration No: MMT173007

Abstract

The technique of digital signature is essential for safe transactions over open networks. It is used in a variety of applications to ensure the integrity of exchanged information and to demonstrate the identification of the originator to the receiver. We review the scheme of Kuppuswamy et al. the digital signature scheme based on block cipher.

This technique is a new version of the digital signature algorithm based on a linear block cipher or asymmetric algorithm initiated by Hill cipher with keys as invertible matrices over $\mathbb{Z}_n$. Through cryptanalysis, we found that the block digital signature scheme is insecure. In this thesis it is shown that the digital signature scheme can be broken by mounting a known-plaintext attack. In fact, a successful key recovery attack can be mounted with limited complexity.

Another topic that is discussed in the thesis is the use of self-invertible Hill cipher for encryption scheme by Kumar et al. The author proposed a method for Hill cipher algorithm based on self-invertible matrices.The use of self-invertible matrices reduces the decryption cost but it contributes nothing towards the security of the system. It is shown that the encryption scheme proposed by Kumar et al. is not secure and has security flaws. A successful cryptanalysis resulted in the full recovery of the secret key.

Contents

List of Figures

List of Tables

Abbreviations

AES	Advance Encryption Standard
CA	Certificate Authority
DES	Data Encryption Standard
DH	Diffie Hellman
DSA	Digital Signature Algorithm
EC	Elliptic Curve
ECC	Elliptic Curve Cryptography
PC	Personal Computer
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
RSA	Rivest Shamir Adleman
SSL	Secret Socket Layer
XOR	Exclusive OR

Symbols

M	Plaintext or Message
C	Ciphertext
K	Key
E	Encryption Algorithm
D	Decryption Algorithm
E_k	Encryption Key
D_k	Decryption Key
$\mathbb{Z}$	Set of integers
$\mathbb{N}$	Natural numbers
$\mathbb{G}$	Group
$\mathbb{R}$	Ring
$\mathbb{F}$	Field
H	Hash Function

Chapter 1

Introduction

1.1 Cryptography

A major issue with the data under communication over the public network is its safty. Cryptography plays a vital role in solving the safety problems of sensitive data. In this context cryptography has many contributions. The term "cryptography" derives from two Greek words **kryptos** which means "hidden" and **logos** which means "words". Cryptography is a science of secret communication, that is used to make the communication secure in the presence of a third party over an insecure channel by altering the original message into an unreadable form. For this purpose we use different methods for transformation of the original message into the coded form. Such methods are known as cryptography [1].

We also need to analyze these methods to check their effectiveness and performance for their improvement. The whole analysis is performed in another branch named as **cryptanalysis**. It observed that when there is some vulnerability in the cryptosystems, a cryptanalyst performs cryptanalysis.

The stability of any cryptosystem can be judges to break the cryptosystem by taking security analysis.

The cryptographic systems are split into two classes based on the use of key [2].

- Symmetric (Private) Key Cryptography

- Asymmetric (Public) Key Cryptography [3]

With symmetric key cryptography, both the sender and receiver use only one key to encrypt or decrypt the information. However, the main problem in this technique is the distribution of keys. Data Encryption Standard (DES) [4] and Advanced Encryption Standard (AES) [5] are the examples of symmetric key cryptography. To overcome the issue of key distribution, in 1976, asymmetric key cryptography was presented by Diffie-Hellman [6].

The asymmetric key cryptosystem utilizes two different keys i.e, (encryption key and decryption key). For the encryption process, one key is used while another id used for the decryption process. Since the encryption key is public, so anyone can encrypt the data but only the individual with the decryption key can decrypt that data because the decryption key is kept private. Examples of asymmetric key cryptography techniques include ElGamal [7], Rivest Shamir Adleman (RSA) [8], Elliptic curve cryptography (ECC) [9] etc.

Many cryptographic schemes are used to secure data for safe communication based on the keys of encryption and decryption. A cryptosystem is considered secure if the encryption and decryption keys are secure.

1.2 Digital Signatures

The digital signature is an essential part of different cryptographic primitive as verification, authorization and non-repudiation [6]. The main purpose of a digital signature is to allow an entity to define its identity with a small amount of information [10]. Public key cryptography and digital signature schemes presented by Diffie-Hellman and Martin Hellman are published in their article “New Direction in Cryptography” [6].

In their digital signature scheme, each user has identity i.e. a pair containing his/her public key and the corresponding secret key. Signatures are often verified by using the secret key of the sender. Rivest, Shamir, and Adleman presented the first digital signature scheme. Their scheme is based on the supposition that is called “RSA assumption”. Goldwasser et al. also worked on digital signature [11].

This scheme is not based on “signature trees”, but follows the so called paradigm of “hash-and-sign” (for more details also see [12]).

Rompher illustrated how a digital signature scheme can be constructed using one way method. Genaro and Helevi [13], Cramer and Shoup [14] proposed the first signature schemes whose efficiency is suitable for practical use and safe against adaptive chosen message attacks.

Electronic commerce and confidential network communications have played the fundamental role in the public key cryptosystem [15]. A digital signature is a confirmation that the received message is in its original form and not been altered during the communication [16]. However, it relies on the pieces of both the transferred data and the secret key which can be verified at any stage of communication. Digital signature is a data that is calculated cryptographic value and a secret key known only to the signer [17].

Cryptographers have been working on electronic signature techniques and investigating their characteristics for many years [18].

1.3 Hill Cipher

In 1929, the mathematician Lester S. Hill invented Hill cipher. The basic and most important part of Hill cipher is matrix multiplication. Hill cipher operates on groups of symbols like the digraphic cipher. It is extended to work on different size of blocks of symbols and technically polygraphic substitution cipher. In polygraphic substitutions each letter is replaced in different ways, according to their place in the document. The Hill cipher is based on linear algebra, including multiplication of matrixes.[19]

This performs by converting the plaintext letters into numbers, splitting the resultant sequence of numbers into blocks of n values, each of which is represented as a vector of n elements and multiplied by an invertible key matrix to produce the corresponding ciphertext block. Decryption works in the same way, except that it substitutes the key matrix with its inverse [19, 20]. In Hill cipher, a numerical value from 0 to 25 is allocated to all 26 alphabets for example $A = 0$, $B = 1$, ..., $Z = 25$ [21, 22].

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Table 1.1: Encryption scheme

There are m equations used during the encryption of m plaintext letters to m ciphers as given below:

$$\begin{aligned} C_1 &= (K_{11}P_1 + K_{12}P_2 + K_{13}P_3) \mod 26 \\ C_2 &= (K_{21}P_1 + K_{22}P_2 + K_{23}P_3) \mod 26 \\ C_3 &= (K_{31}P_1 + K_{32}P_2 + K_{33}P_3) \mod 26 \end{aligned} \tag{1.1}$$

the above used equations can be written in matrix form as follows:

$$\begin{bmatrix} C_1 \\ C_2 \\ C_3 \end{bmatrix} = \begin{bmatrix} K_{11} & K_{12} & K_{13} \\ K_{21} & K_{22} & K_{23} \\ K_{31} & K_{32} & K_{33} \end{bmatrix} \begin{bmatrix} P_1 \\ P_2 \\ P_3 \end{bmatrix} \tag{1.2}$$

in simple equation form is $C = KP$, in which C and P are an order 3 column vector describing plaintext and ciphertext, and K is a key of an order 3×3. All of the processes are under modulo 26. In the decryption invertible matrix of K is required. Equation

$$KK^{-1} = K^{-1}K = \mathrm{I}, \tag{1.3}$$

defines the inverse of a matrix 'K', where 'I' represents the identity matrix of 3 × 3. However, there are some matrices whose inverses do not exist, and when it happens, the Equation (1.3) will be satisfied. We apply K^{-1} on the ciphertext to retrieved the original text [20, 23]. We may write the general form as:

Encryption process:

$$C = E_k(P) = KP. \tag{1.4}$$

Decryption process:

$$P = D_k(C) = K^{-1}C = K^{-1}KP = P. \tag{1.5}$$

If the size of the block is m taken as, then there is a possibility of 26^m different blocks. Each of them can be considered as a letter in an alphabet. Hill's method is a monoalphabetic substitute for this alphabet [21].

1.4 Current Research

In this dissertation, we cryptanalysis the matrix based cryptographic schemes: One is the "Digital Signature Scheme based on Block Cipher" and other is the "Matrix based Encryption Scheme using Self-Invertible Hill Cipher".

Firstly, we focus on the digital signature scheme based on block cipher given by Kuppuswamy et al. [24]. Signed messages are often transmitted over an electronic network. He proposed a key generation algorithm for the digital signature scheme and described the methodology of a digital signature algorithm. We cryptanalysis digital signature scheme supported block cipher presented in [24].

Secondly, we focus on the paper encryption scheme based on self-invertible Hill cipher by Kumar et al. [25]. This article describes the methodology of the Hill cipher. Hill cipher is based on manipulations of the matrix. And in terms of standard arithmetic, this justifies that the mathematical operation given here is the addition, subtraction, the monadic operation, multiplication, and the division [10]. Then he justifies the self-invertible key matrix-generating algorithm. We cryptanalysis digital signature scheme supported block cipher presented in [25].

1.5 Thesis Layout

Our thesis is structured as follows:

In **Chapter 1,** we have mentioned the concept of cryptography, the cryptographic background and presented introduction to the basis terms related to cryptography. Furthermore, we mentioned the idea of digital signature and Hill cipher.

In **Chapter 2,** we present the fundamental definitions of cryptography and a few mathematical terms associated with our work. Additionally we describe cryptology, sorts of cryptography, the purpose of cryptography, some basic definition associated with encoding and the distinction between a digital certificate and digital signature. At the end of this chapter, we discuss the importance of digital signature.

In **Chapter 3,** we present the review of the digital signature scheme based on block cipher given by Kuppuswamy et al. [24]. For that purpose, we have discussed numerous well-known digital signature schemes. Ultimately we have described our finding *i.e.* digital signature cryptanalysis for block cipher with the help of an example.

In **Chapter 4,** we discuss the review of another cryptographic scheme that is encryption scheme based on self-invertible Hill cipher given by Kumar et al. [25]. For that purpose, we have got a bent to say modular arithmetic and its properties, strategies for generating a self-invertible matrix, we explain our work of cryptanalysis of encryption scheme based on self-invertible Hill cipher with the help of an example.

Finally the conclusion is presented in chapter 5.

Chapter 2

Preliminaries

A few fundamental definitions of terms related to cryptography and key management are provided in this chapter. Furthermore, some fundamental algebraic concepts are also illustrated for further assistance.

2.1 Cryptology

The term cryptology [26] is originated from two Greek terms **kryptos** means (Hidden or secret) and **logos** means (letters or words). Cryptology is a science that deals with hidden, disguised, or encrypted communications.[27] It includes communications security and communications intelligence. It consists of the following two fields of study:

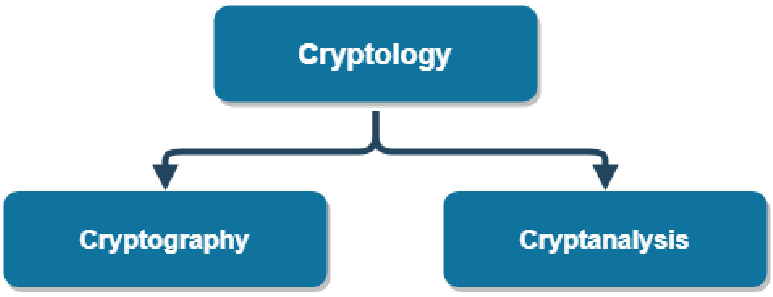

Figure. 2.1. Types of Cryptology

1. **Cryptography**
2. **Cryptanalysis**

2.1.1 Cryptography

Some basic definitions related to cryptography are

Plaintext: The data that is in the original form is known as plaintext (in some cases called **cleartext**).

Ciphertext: Ciphertext is a scrambled data or it is the information or message in coded form.

Key: A key is a piece of data (a parameter) that specifies the functional output of a cryptographic function.

Encryption: Encryption is the technique to convert the plaintext into ciphertext by using the encryption key.

Decryption: Decryption is the technique to transform ciphertext back into plaintext by using the decryption key.

Cryptography is associated with the process of converting ordinary plaintext by using a key into unintelligible text known as ciphertext and vice-versa [3].

It is a process of storing and transmitting data in a specific form such that it can only be read and analyzed by those for whom it is intended. Cryptography not only secure data from misuse or manipulation, but it can also be used to authenticate users.

Cryposystem: A cryptosystem is a system where we use encryption function to transform ordinary data or message (plaintext) into secret codes (ciphertext) and transform secret codes back into a data using decryption. A cryptosystem consists of five basic components:

1. **Message Space M:** The set of all possible original messages (plaintext) m is known as message space.

2. **Key Space K:** The key space of an algorithm corresponds to the set of all possible permutations of a key.

3. **Encryption Function E:** takes plaintext as the input and transform it into ciphertext with the help of encryption key.

4. **Ciphertext Space C:** The set of all possible messages, that are scrambled with the help of key K is known as ciphertext space.

5. **Decryption Function D:** Takes ciphertext as the input and decodes it into plaintext, with the help of decryption key.

Cryptography not only secures the messages but also provides the following important applications [28].

1. **Confidentiality:** Confidentiality refers to the protection of data from unauthorized parties. It comes up with two embedded qualities, i.e. data confidentiality and privacy.

   (a) **Data Confidentiality:** It ensures the confidential information is not disclosed in the network to an unauthorized person.

   (b) **Privacy:** Authority assures to oneself that data associated to them will not be compromised.

2. **Integrity:** Integrity involves:

   (a) **Data Integrity:** is the overall accuracy, completeness, and consistency of the data. Data integrity also refers to data security in terms of compliance and compatibility of regulations.

   (b) **System Integrity:** A assured system that fulfills the proposed concepts in an unaffected manner that are free from illegal manipulation.

3. **Message Authentication**

   It involves validation which provides the originator's identifiable evidence. Two types of authentication services are provided in cryptography:

   (a) **Integrity Authentication:** Authentication of integrity can be used to verify that the data has not been modified.

   (b) **Source Authentication:** Source authentication verifies the identity, of user or device.

4. **Non-Repudiation**

   It assures that someone cannot deny something. Non-repudiation is a legal concept that is widely used in information security and refers to a service, which provides proof of the origin of data and the integrity of the data. In other words, non-repudiation makes it very difficult for sender to successfully deny who/where a message came from as well as the authenticity of that message.

   For example, when an application is made electronically, the purchaser cannot deny from the purchase request, if this transaction permits non-repudiation service.

There are two major classification of cryptography based on key dissemination known as Symmetric Key and Asymmetric Key Cryptography as shown in Figure 2.2

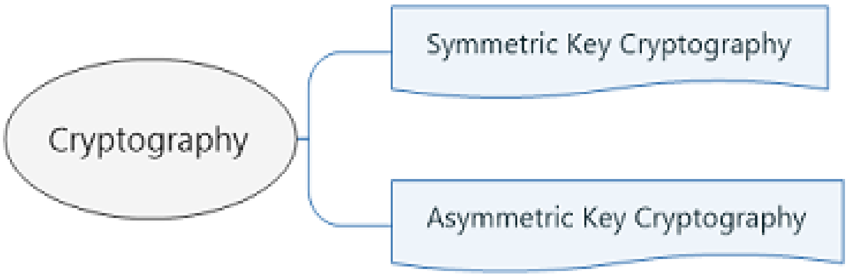

Figure. 2.2. Types of Cryptography

2.1.2 Symmetric Key Cryptography

The symmetric key cryptography is also known as secret key cryptography [29]. It uses the same encryption technique and similar or equal keys for encryption and decryption of the data. A typical symmetric key cryptographic model is displayed in Figure 2.3

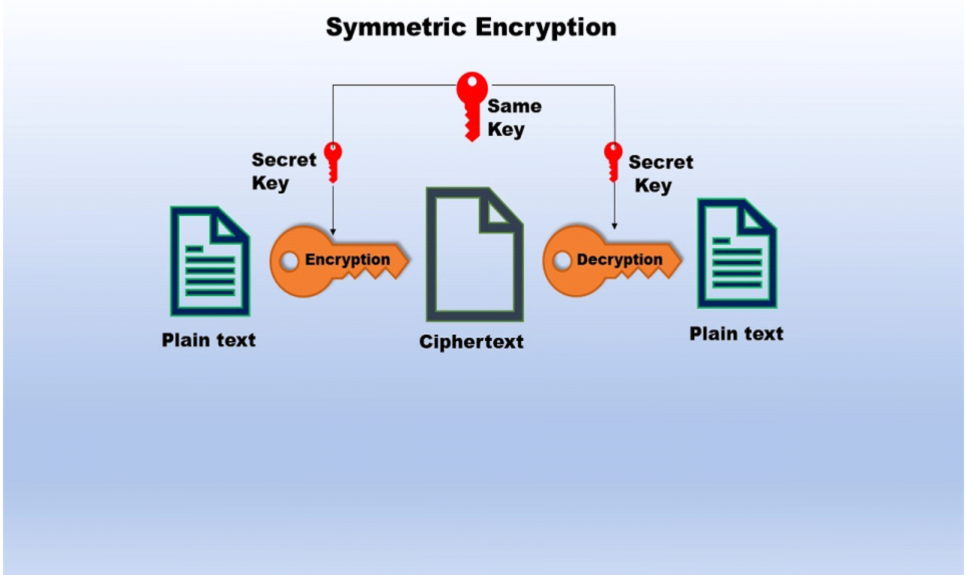

Figure. 2.3. Symmetric Key Cryptography

It utilizes a secret key which can be either a number, a word or a random letter string. The sender and the receiver should be familiar with the secret key used to encrypt and decrypt all documents. Examples include DES (Data Encryption Standard) [4] and AES (Advanced Encryption Standard) [5] etc.

These schemes are very effective and secure. Disadvantages of such cryptosystem include key management and related security issues.

2.1.3 Asymmetric Key Cryptography

Diffie-Hellman algorithm is one of the first techniques introduced in asymmetric encryption for the exchanging of keys. It was developed in 1976 by Martin Hellman and Whitfield Diffie [6]. This method eliminates the need for two communicating parties to switch keys.

"Asymmetric cryptography, also known as public key cryptography, uses public and private keys to encrypt and decrypt data. It ensures that malicious persons do not misuse the keys.

It is important to note that anyone with a secret key can decrypt the message and this is why asymmetrical encryption uses two related keys to boost the security. A public key is made freely available to anyone who might want to send you a message. The second private key is kept secret.

A message that is encrypted using a public key can only be decrypted using a private key, while also, a message encrypted using a private key can be decrypted using a public key. Security of the public key is not required because it is publicly available and can be passed over the internet. The asymmetric key has far better power in ensuring the security of information transmitted during communication. Asymmetric encryption is mostly used in day-to-day communication channels, especially over the Internet. Popular asymmetric key encryption algorithm includes ElGamal [30], RSA [31], Elliptic curve techniques [32], PKCS" [33].

As shown in Figure 2.4.

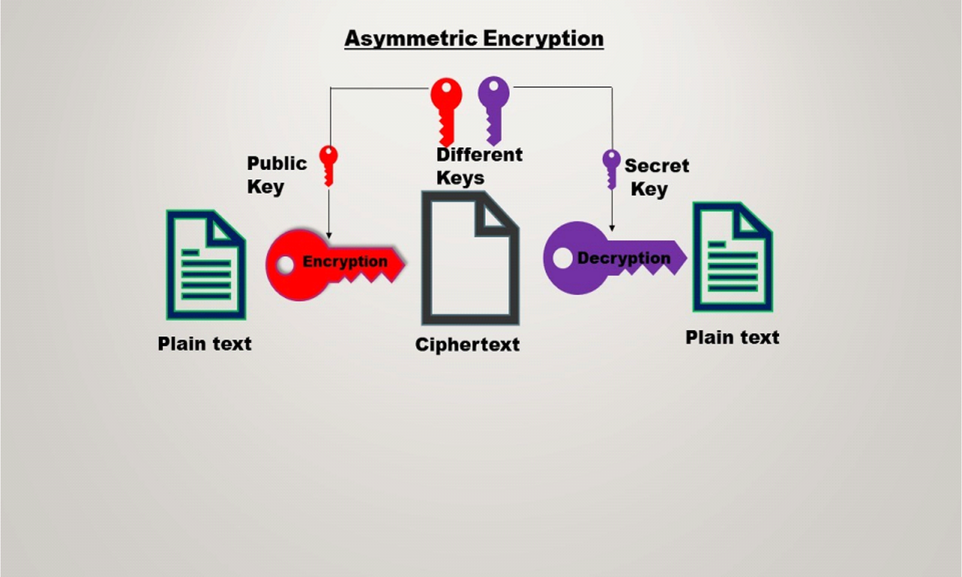

Figure. 2.4. Asymmetric Key Cryptography

The sender and the receiver are the two participants in the asymmetric encryption scheme. The sender acquires the public key of the receiver. At that stage the plaintext is encoded with the asymmetric encryption algorithm by utilizing the recipient's public key, and focus the ciphertext.

Then the ciphertext is sent to the receiver, who decodes the ciphertext with his private key and gets the sender's plaintext.

Due to the one-way nature of the encryption function, any sender is unable to read the messages of another sender, even though everyone has the knowledge of the public key of the recipient.

Examples of such a cryptosystem are RSA [31], ElGamal [30] and Diffie-Hellman key exchange [6].

2.2 Cryptanalysis

Cryptanalysis is the decryption and analysis of codes, ciphers or encrypted text without the knowledge of decryption key. Cryptanalysis uses mathematical formulas to search for algorithm vulnerabilities and break cryptographic information security systems. It is a mechanism to obtain plaintext from ciphertext without the knowledge of key [34].

If any one property from four properties (confidentiality, information integrity, message validation, and non-repudiation) are found to be weak in a cryptosystem then the cryptosystem is said to be vulnerable to an attack. Cryptanalysis is mostly used for attacking a secret message or finding a secret key or to check the quality of a cryptosystem.

Some known cryptanalysis attacks are stated below:

1. **Brute Force Attack**

   In this attack, to reveal the plaintext from the ciphertext, the attacker arbitrarily tries all the possible keys. The hardness of this attack is directly connected with a key size that is getting used. The larger of the key size, the larger will be the size of key space and hence harder will be the brute force attack [35].

2. **Chosen Plaintext Attack**

   For attacking a cryptosystem there are several structures, a chosen-plaintext attack is one of them. An attacker arbitrarily picks some plaintext utilizing this attack for encoding and gets the relating ciphertext. The goal of this attack is to reduce the encoding scheme security in order to extract additional data from the ciphertext [11, 36].

3. **Chosen Ciphertext Attack**

   It is a similar situation as the chosen plaintext, however, it is applied to decryption function. An attacker arbitrary chooses some ciphertext and tries to obtain the related plaintext. The reason for utilizing this attack is to acquire additional data identified to the plaintext [36].

4. **Ciphertext Attack**

   An attacker uses the ciphertext to achieve the key or plaintext. For breaking the system letter's frequency can be used. Typically, the attacker has no data concerning the plaintext however he attacks the original message by exploitation ciphertext attack.

5. **Known Plaintext Attack**

   In this attack, a pair of plaintext and ciphertext is known to a cryptanalyst. He uses previous data to decipher any further ciphertext or to determine the key [37].

6. **Man-in-the Middle Attack**

   In this attack, a hacker stays secretly across the public network between the two parties who want to communicate. The attacker totally controls the communication of both the sender and receiver. In this attack, two keys K_1 and K_2 are selected by the attacker. The statement between the sender and the receiver is completely controlled by the attacker in two phases. At first, the sender by using K_1 encrypts his message and sends this encrypted message to the receiver over a public network.

Since there is an attacker between the sender and receiver in this manner, an attacker gets the encrypted message except for the receiver. He/she can decrypt the encrypted message. Secondly, an attacker by using K_2 encodes a message and sends this encoded message to the receiver. He/she can likewise decrypt the reply achieved by the receiver.

That's how an attacker holds the communication between the two parties without their knowledge.

7. **Algebraic Attack**

   If the attacker has information about ciphertext and plaintext then he can break the cipher to unveil the secret key. In this attack, attacker expresses the cipher operation mode as a set of equations then solve it to obtain the key or some information regarding plaintext.

2.3 Mathematical Background

In this section we will present some elementary definitions that will be used throughout the thesis.

Definition 2.3.1 (Polygraphic Substitution Cipher)

"Polygraphic substitution divides the plaintext into groups of letters. Then, replace each group of letters by one of the predefined letters, numbers, graphic symbols, or by another group of characters" [38].

Definition 2.3.2 (Extended Euclidean Algorithm)

This algorithm is an extension to Euclidean algorithm, it is used to find greastest common divisor (gcd) of two integer a and b and also the coefficients x and y, of bezout's identity such that

$$ax + by = gcd(a, b).$$

Algorithm 2.3.1 Extended Euclidean Inverse Algorithm

Input: An integer r and modulo m.

Output: $r^{-1} \mod m$.

```
1. Boot six integers $A_i$ and $B_i$ for $i = 1, 2, 3$ as
   $(A_1, A_2, A_3) = (1, 0, m)$
   $(B_1, B_2, B_3) = (0, 1, r)$.
2. If $B_3 = 0$, return $A_3 = \gcd(r,m)$; no inverse of $r$ exist in $\mod m$.
3. If $B_3 = 1$ then return $B_3 = \gcd(r,m)$ and
   $B_2 = r^{-1} \mod m$.
4. Now divide $A_3$ with $B_3$ also find the quotient $Q$ when $A_3$ is divided by $B_3$.
5. Set $(T_i = (A_i - Q.B_i))$ ; $i = 1, 2, 3$.
6. Set $(A_1, A_2, A_3) = (B_1, B_2, B_3)$.
7. Set $(B_1, B_2, B_3) = (T_1, T_2, T_3)$.
8. Goto step number 2.
```

Definition 2.3.3 (Group)

"Let G be a non-empty set. G is said to be a group [39] under a binary operation define as $* : G \times G \to G$ for all r, s and $t \in G$. If it satisfies the following properties:

a. Associativity

G is claimed to be associative under '$*$' if for any r, s, $t \in G$ the subsequent equality holds.

$$(r * s) * t = r * (s * t).$$

b. Identity Element

An element $e \in G$ is claimed to be an identity in G if,

$$e * r = r = r * e \ \forall \ r \ \in \ G.$$

c. Inverse

For every $r \in G$ there exists $r' \in G$ such that,

$$r * r' = e = r' * r$$

then r' is said to be inverse of r in G. A set along with one binary operation is named as **Groupoid**. A **Groupoid** satisfying associative property is known as **Semi-group**. A **Semi-group** with an identity element is named as **Monoid**. A **Monoid** with inverses is known as **Group**."

Example 2.3.7: Some well known groups are :

1. With binary operation '+', the $\mathbb{Z}$ set of all integers, the $\mathbb{Q}$ set of rational numbers, the $\mathbb{R}$ set of real and $\mathbb{C}$ set of complex numbers.

2. The sets $\mathbb{Q} \setminus 0$, $\mathbb{R} \setminus 0$ and $\mathbb{C} \setminus 0$ also form group under multiplication as binary operation.

3. The general linear group $GL(n, \mathbb{R})$ is a group under operation of matrix operation.

Definition 2.3.4 (Cyclic Group)

"A Group G generated by a one element $h \in G$ is called cyclic group, where h is known as generator of G denoted by $\langle$ h $\rangle$. If h generates G then each element i $\in G$ can be written as h^s for some integer s and we write $G = \langle$ h $\rangle$. Moreover, every cyclic group is an abelian group.

i.e. for all i, $j \in G$"

$$i * j = h^s h^t = h^{s+t} = h^{t+s} = h^t h^s = j * i,$$

where s, $t \in \mathbb{Z}$.

Definition 2.3.5 (Abelian Group)

"A group is said to an abelian group if it satisfies commutative property"

$$p * m = m * p,$$

for all p, $m \in \mathbb{R}$.

Definition 2.3.6 (Ring)

"Let $\mathbb{R}$ be a non-empty set together with two binary operations '+' and '.'. It is said to be a ring [39] under '+' and '.', if the following axioms are satisfied by $\mathbb{R}$.

1. $\mathbb{R}$ is an **abelian group** under addition, meaning that:
   - $(a + b) + c = a + (b + c)$ for all a, b, c in R (that is, + is **associative**).
   - $a + b = b + a$ for all a, b in R (that is, + is **commutative**).
   - There is an element 0 in R such that $a + 0 = a$ for all a in R (that is, 0 is the **additive identity**).
   - For each a in R there exists $-a$ in R such that a + (-a) = 0 (that is, $-a$ is the **additive inverse** of a).

2. $\mathbb{R}$ is a **monoid** under multiplication, meaning that:
   - $(a\ .\ b)\ .\ c = a\ .\ (b\ .\ c)$ for all a, b, c in R (that is, . is **associative**).
   - There is an element 1 in R such that $a\ .\ 1 = a$ and $1\ .\ a = a$ for all a in R (that is, 1 is the **multiplicative identity**).

3. Multiplication is **distributive** with respect to addition, meaning that:
   - $a\ .\ (b + c) = (a\ .\ b) + (a\ .\ c)$ for all a, b, c in R (left distributivity).
   - $(b + c)\ .\ a = (b\ .\ a) + (c\ .\ a)$ for all a, b, c in R (right distributivity)."

OR

"A non-empty set $\mathbb{R}$ along with two binary operations, addition (+) and multiplication (.), denoted by $(\mathbb{R}, +, .)$ is said to be a ring [40] if it satisfies the subsequent properties:

1. $(\mathbb{R}, +)$ is an **abelian group**.

2. $(\mathbb{R}, .)$ is a **monoid**.

3. **Distributive properties** of multiplication over addition holds. That is, for all p, m, $\ell \in R$, we have

- $p \ . \ (m + \ell) = p \ . \ m + p \ . \ \ell$

- $(p + m) \ . \ \ell = p \ . \ \ell + m \ . \ \ell$"

Example 2.3.6. Followings are the examples of ring.

1. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ form ring under usual addition and multiplication.

2. Suppose p is a prime, then the integers mod p ($\mathbb{Z}_p$) is a ring.

Definition 2.3.7 (Commutative Ring)

"A ring is known as commutative ring if commutative property with respect to multiplication holds, that is"

$$p \ . \ m \ = \ m \ . \ p \text{ for all } p, \ m \ \in \ R.$$

Example 2.3.6.

"($\mathbb{Z}$, +, .), ($\mathbb{R}$, +, .) are some examples of commutative ring."

Definition 2.3.8 (Field)

"A non-empty set $\mathbb{F}$ with two binary operations addition (+) and multiplication (.) is called a field [41] if the following properties holds, for all a, b, c $\in \mathbb{F}$."

1. $\mathbb{F}$ is abelian under addition.

2. A ring in which non zero elements form an abelian group with respect to the binary operation '.' is known a field. $\mathbb{F}$ forms an abelian group under multiplication (only nonzero elements).

Example 2.3.7. Some well known fields are:

1. $\mathbb{R}$ and $\mathbb{C}$ forms the field under usual multiplication and addition.

2. For every prime p, set of integers ($\mathbb{Z}_p$) under mod p is a field.

Definition 2.3.9 (Finite Field) [41]

"A field with finite number of elements is called a finite field."

Example 2.2.8. Examples of finite field are:

1. $\mathbb{Z}$ mod p where p is a prime number is finite field.

2. Galois field is a finite fields. For instance, $GF(2)$, $GF(2^3)$, $GF(3)$.

2.4 Modular Arithmetic

In this section, all the arithmetic operations are computed under modulo an integer m are discussed [22]. Many digital signature and encryption schemes are based on modular mathematic. Based on this, for the Hill cipher algorithm, the self-invertible matrix is produced. The modulo operator has subsequent characteristics:

1. $c = d$ mod m if $n|(c$ - $d)$.

2. c mod $m = d$ mod $m \implies c = d$ mod m.

3. $c = d$ mod $m \implies d = c$ mod m.

4. $c = d$ mod m and $d = e$ mod $m \implies c = e$ mod m.

Let the set $\mathbb{Z}_m$ = [0, 1, ..., m - c] of residues modulo m. If this set $\mathbb{Z}_m$ contains modular arithmetic, arithmetic operations are presented by the following equations:

- **Addition:**

$$(c + d) \mod m = [(c \mod m) + (d \mod m)] \mod m.$$

- **Negation:**

$$-c \mod m = p - (c \mod m).$$

- **Subtraction:**

$$(c - d) \mod m = [(c \mod m) - (d \mod m)] \mod m.$$

- **Multiplication:**

$$(c * d) \mod m = [(c \mod m) * (d \mod m)] \mod m.$$

- **Division:**

$$(c/d) \mod m = e,$$

when

$$c = (d * e) \mod m.$$

- **Commutative Law:**

$$(a + b) \mod m = (b + a) \mod m.$$

$$(a * b) \mod m = (b * a) \mod m.$$

- **Associative law:**

$$((a + b) + c) \mod m = (a + (b + c)) \mod m.$$

- **Distribution Law:**

$$(a * (b + c)) \mod m = ((a * b) \mod m + (a * c) \mod m) \mod m.$$

- **Identities:**

◇ Additive identity:

$$(0 + x) \mod m = x \mod m.$$

◇ Multiplicative identity:

$$(1 * a) \mod m = a \mod m.$$

- **Inverses:**

◇ Additive inverse: For each $b \in \mathbb{Z}_m$, $\exists$ a such that

$$(b + a) \mod m = 0,$$

then

$$a = -b.$$

◇ Multiplicative inverse: For each $b \in Z_m$, $\exists$ a such that

$$(b * a) \mod m = 1.$$

- **Modular congruence additiveness:**

For e, f, g, h, and m entities, if

$$e = g \mod m,$$

and

$$f = h \mod m,$$

then

$$e + f = g + h \mod m.$$

Proof.

Because of

$$e = g \mod m, \; m \mid e - g.$$

Similarly, because of

$$f = h \mod m, \; m \mid f - h.$$

Using an outcome "that the sum of two numbers divisible by m is itself divisible by m", therefore we can conclude that

$$m \mid (e - g) + (f - h).$$

Arithmetically reshuffling, it follows

$$m \mid (e+f)-(g+h)$$

$$\text{so } e+f=g+h \mod m.$$

Modular compatibility multiplications:

For e, f, g, h, and m entities, if $e = g$ mod m and $f = h$ mod m, then $ef = gh$ mod m.

Proof.

Because of

$$e=g \mod m, \;\; m \mid e-g.$$

Similarly, because of

$$f=h \mod m, \;\; m \mid f-h.$$

We can use the linear condonation theorem from these two divisibility criteria to demonstrate that.

$$m \mid [f(e-g)+g(f-h)].$$

Which will algebraically simplify

$$m \mid ef-gh, \text{so } ef=gh \mod m.$$

2.5 Digital Signature

A digital signature is linked with a person as a digital identity. Asymmetric cryptography is commonly used in digital signatures. Users have a secret key that is available only to them. They also have a public key that everyone can use.

It is important to use digital signatures to verify the identity of someone. Each user has their own specific digital signature. Digital signatures can be used to sign documents, because of this uniqueness. Non-repudiation and integrity can be used with digital signatures. Digital signatures, such as handwritten signatures, are special for every signer. Providers with digital signature systems such as DocuSign adopt a particular procedure, called PKI. PKI requires that the provider produce two long numbers, called keys, using a mathematical algorithm. One key is public, and one key is private.

When a signer signs a document electronically, the signature is produced using a private key from the signer, which the signer always kept secure. The mathematical procedure acts as a cipher, generating data that follows the signed document, calling it a hash, and encrypting it. The resulting digital signature is encrypted files. Additionally, the signature is associated with the signing of the paper. If after signing, the document changes, the digital signature is invalidated. Various best-known digital signature schemes are given below.[42]

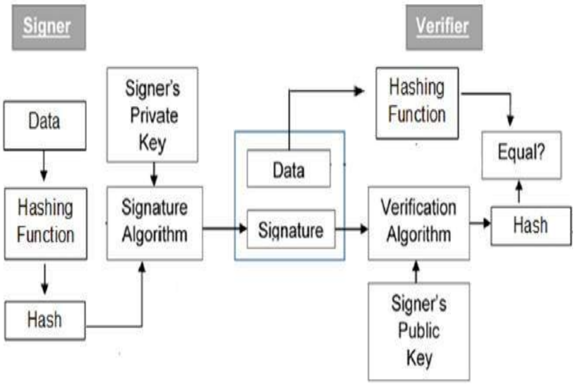

Figure. 2.5. Digital Signature

2.5.1 Elgamal Signature Scheme

Recall that given a finite group $\mathbb{Z}_p$ and a fixed element $a \in \mathbb{Z}_p$, finding an integer x from the knowledge of $y = a^x \bmod p$ is a computationally hard problem. This problem is known as discrete logarithm problem (DLP).

The Elgamal signature scheme [43] is a digital signature scheme based on the numerical complexity of discrete logarithms. The global parameters of Elgamal digital signature are a prime p_1, base element g_1 and hash function H. This scheme is described in the following steps:

Key Generation

Alice generates his private and public key pairs as follows:

- Choose arbitrarily a secret key x_1 with $1 < x_1 < p_1$ - 1.
- Calculate $y_1 = g_1^{x_1}$ mod p_1.
- The public key is (p_1, g_1, y_1).

Signature Generation

The signer will perform the following steps to sign the message m_1:

- Choose a random k_1 s.t $0 < k_1 < p_1$ - 1 and find gcd (k_1, p_1 - 1) = 1.
- Calculate $r_1 = g_1^{k_1}$ mod p_1.
- Compute s_1 = (H(m_1) - x_1r_1) k_1^{-1} mod p_1 - 1.

Then the pair (r_1, s_1) is the numeral signature of the message m_1.

Verification

Signature (r_1, s_1) is confirmed if:

- $g_1^{H(m_1)} = y_1^{r_1}\ r_1^{s_1}$ mod p_1

where $0 < r_1 < p_1$ and $0 < s_1 < p_1$ - 1.

The verifier accepts the signature if above conditions are satisfied otherwise reject it.

Correctness

The correctness of the scheme follows from the subsequent steps:

As, s_1 = (H(m_1) - x_1r_1)k_1^{-1} mod p_1 - 1.

- H(m_1) = $x_1r_1 + s_1k_1$ mod p_1 - 1.

From Fermat's little theorem,

- $g_1^{H(m_1)} = g_1^{x_1r_1}\ g_1^{k_1s_1}$ mod p_1.
- $g_1^{H(m_1)} = (g^{x_1})^{r_1}\ (g^{k_1})^{s_1}$ mod p_1.
- $g_1^{H(m_1)} = (y_1^{r_1})(r_1^{s_1})$ mod p_1.

2.5.2 RSA Digital Signature Scheme:

The digital signature scheme of the RSA applies the private key of the sender to a message generating a signature. Through the verification process, the signature is verified by applying the correct public key to the message and signature, providing either a valid or invalid result. The RSA signature scheme [44] is also based on difficulty of computing discrete logarithms. To sign message m_1 following steps should be performed:

Key Generation

- Choose two large prime numbers r_1 and s_1.
- Calculate $g_1 = r_1 \cdot s_1$ where g_1 is modulo.
- Calculate $\varphi(g_1) = (r_1 \text{ - } 1)(s_1 \text{ - } 1)$.
- Take $e_1 = 1, \cdots, \varphi(g_1)$ s.t $\gcd(e_1, \varphi(g_1)) = 1$.
- Calculate d_1 such that $d_1 \cdot e_1 = 1 \bmod \varphi(g_1)$.

Signature Generation

To sign message Alice performs the subsequent steps:

- Calculate $S_1 = m_1^{d_1} \bmod g_1$.

Verification

If $m_1^j = m_1$ then accepts the message otherwise reject it.

- Calculate $m_1^j = S_1^{e1} \bmod g_1$.

Correctness

The correctness of the scheme is shown in the subsequent steps:
As, m_1^j= $S_1^{e^1}$ mod g_1 and $S_1 = m_1^{d_1}$ mod g_1.

- $m_1^j = (m_1^{d_1})^{e_1} \bmod g_1$.
- m_1^j= $(m^{d_1 . e_1}) \bmod g_1$.
- m_1^j= $m_1 \bmod g_1$.

2.5.3 Importance of Digital Signature

1. **Unique to the signer**

   Authentication: Since certificate verified by a third party was used to apply the signature, the receivers recognize that the sender have signed it.

   Non-repudiation: Non-repudiation is the guarantee that one cannot reject something's validity. Non-repudiation is a legal concept that is commonly used in information security, which applies to a service that provides proof of data sources and data integrity.

2. **Unique to the Document**

   Message integrity: When the signature is confirmed, it ensures that when the signature was implemented, the data in the document matched what was in it. Even the smallest change to the original document would make this check fail.

3. **Encryption with Digital Signature**

   In several digital communications, it is necessary to exchange encrypted messages than plaintext to attain confidentiality. A public sender encryption key is available in the open domain in the public key encryption scheme which ensures that anyone can fake their identity and transmit an encrypted message to the receiver. It makes it necessary for users utilizing PKC for encryption to check for digital signatures as well as encrypted data to ensure confidentiality and non-repudiation of messages. This can be archived through the

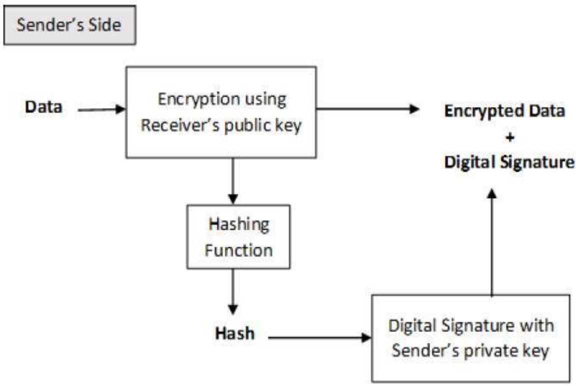
Sender's Side
Data
Encryption using Receiver's public key
Encrypted Data + Digital Signature
Hashing Function
Hash
Digital Signature with Sender's private key

Figure. 2.6. Encryption with Digital Signature

combination of digital signatures and encryption schemes. There are two possibilities, sign-then-encrypt and encrypt-then-sign.

However, the sign-then-encryption-based cryptosystem can be used by the recipient to fake the sender's identity and send the data to third parties. This approach is therefore not favored. The encrypt-then-sign method is more effective and widely accepted. This is shown in Figure (2.6), after obtaining the encrypted data and signing on it, the recipient first verifies the signature using the public key from the sender. After ensuring the signature's validity, then he recovers the data using his private key through decryption.

Chapter 3

Digital Signature Scheme based on Block Cipher

In this chapter, we discuss the digital signature scheme presented by Kuppuswamy et al. [24]. The analysis of the scheme shows that it has many security flaws. In this chapter, it is shown that the scheme is vulnerable to a known-plaintext attack.

3.1 Introduction

A PKI (Public Key Infrastructure) is a structure in cryptography that connects public keys to the respective identities of entities (such as individuals and organizations). The connection is created through a registration process and certificate issuance by a certificate authority (CA). This can be achieved by an automated process or under human supervision

depending on the level of security of the connection. The PKI is basically used for safe and sound transfers between businesses or government entities.

Few companies or agencies may want to digitally sign all employee's documents created by them.

A signature scheme is a signing procedure that is processed in electronic form, then this signed document can be distributed over a network of computers. In this chapter we will discuss signature scheme that uses PKI for signature generation. For a digital signature, the recipient gets the message and the signature. To verify the authenticity, the sender must add a validation technique to the message

combined with the signature. The relationship between a signature and a message is one-to-one.

The digital signature scheme presented in [24], is depending on the linear block cipher. Originally the Hill cipher [45] is a symmetric key scheme but the present signature scheme [24] it is used as an asymmetric key scheme.

3.2 Digital Signature Scheme

The three phase of the signature scheme proposed by Kuppuswamy et al. [24] is explained in the following algorithm.

The scheme first generates public and private key pair and then sign the document by using the secret key. The receiver then verifies the document by using the public key of the sender.

1. **Key Generation** Choose an $\mathbf{n} \times \mathbf{n}$ matrix as the key component and the global settings of the digital signature algorithm are a number n for the order of the matrix and a prime number p.

Algorithm 3.1.1 Key Generation

Input: An $n \times n$ matrix and a prime number p.

Output: Public key E mod p and private key D mod p.

Step 1. Arbitrary invertible matrix 'K' of order $n \times n$.

Step 2. Determine the inverse K^{-1} of the matrix K mod p such that

$$K * K^{-1} \bmod p = I.$$

Step 3. Choose arbitrary integer 'ℓ' and multiply it with matrix 'K' to obtain 'D'. It will be treated as the private key.

Step 4. Determine the inverse ℓ^{-1} of the integer 'ℓ' modulo p.

Step 5. Calculate the public key E as

$$E = \ell^{-1} * K^{-1} \bmod p.$$

Hence calculated public key is E and calculated private key is D.

2. **Signature Generation**

   To sign the message 'M', Alice will perform the following step:

   Compute
   $$S = (D * M\ ) \bmod\ p,$$

   where S is the digital signature of message M generated by Alice using her private key D and the public key p. Then he sends calculated digital signature to Bob through public network.

3. **Signature Verification**

   Bob receives Alice's digital signature and verify by using the following way:

   Compute
   $$M' = (E * S) \bmod\ p,$$

   where E is the public key of Alice. If $M' = M$ then accepts the message otherwise reject it.

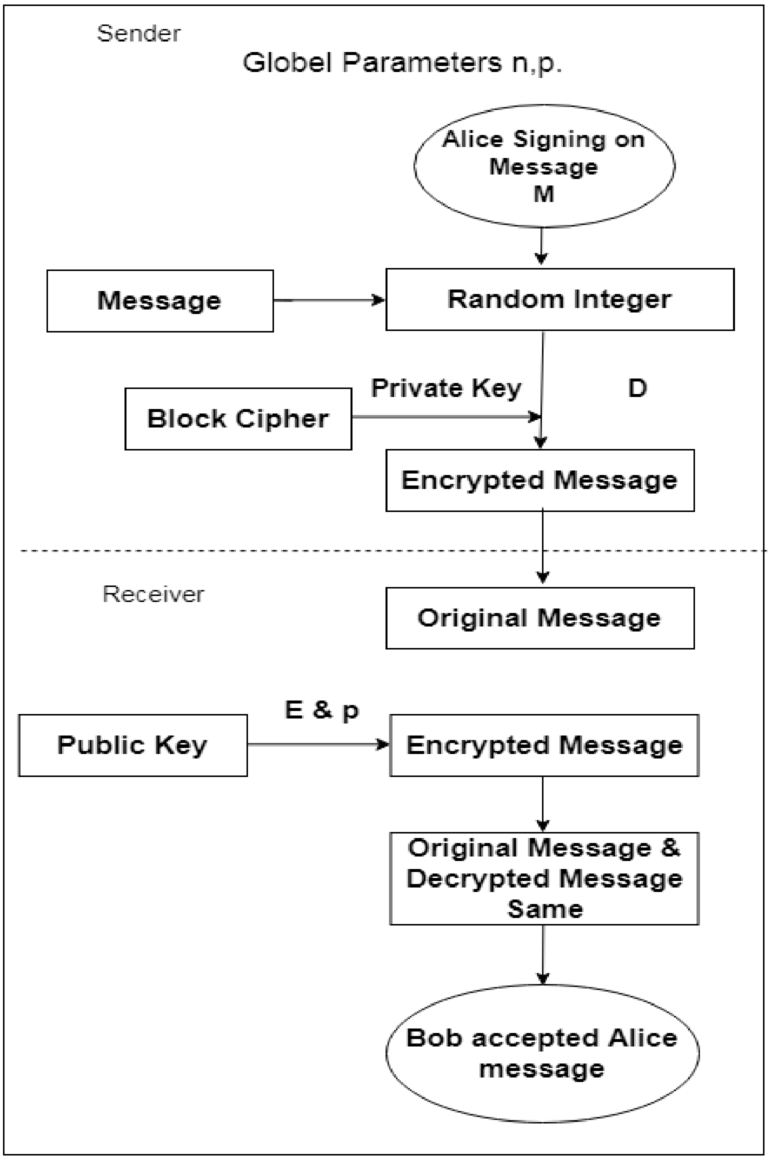

Figure. 3.1. Digital Signature Architecture

Correctness

The correctness of the scheme, follows from the following steps:

As, $M' = (E * S) \bmod p$ and $S = (D * M) \bmod p$.

- $M' = (E * S) \bmod p$.
- $M' = (E * D * M) \bmod p$.
- $M' = ((E * D) * M) \bmod p$.
- $M' = ((\ell^{-1} * K^{-1}) * (\ell * K)) * M) \bmod p$.

- $M' = M \bmod p.$

Remark 3.2.1. Given

$$E = \ell^{-1} * K^{-1} \bmod p,$$

it is hard to compute ℓ and K and the private key D.

The digital signature algorithm is illustrate by the following two examples with $n = 2$ and $n = 3$.

Example 3.2.1. Suppose $n = 2$, $p = 37$, and $M =$ **'DEAN OMAR'**.

Step 1. Alice selects a random prime number *i.e.*,

$$p = 37.$$

Step 2. Choose the arbitrary invertible matrix

$$K = \begin{bmatrix} 3 & 4 \\ 1 & 2 \end{bmatrix} \bmod 37.$$

Step 3. Compute K^{-1} using extended Euclidean algorithm

$$adj(K) = \begin{bmatrix} 2 & -4 \\ -1 & 3 \end{bmatrix} \bmod 37$$

$$\left|K\right| = 6 - 4 = 2 \bmod 37$$

$$K^{-1} = \left|K\right|^{-1} \times adj(K)$$

$$K^{-1} = 2^{-1} \times \begin{bmatrix} 2 & -4 \\ -1 & 3 \end{bmatrix} \bmod 37$$

$$2^{-1} = 19 \bmod 37$$

$$K^{-1} = 19 \times \begin{bmatrix} 2 & -4 \\ -1 & 3 \end{bmatrix} \bmod 37$$

$$K^{-1} = \begin{bmatrix} 1 & 35 \\ 18 & 20 \end{bmatrix} \bmod 37.$$

Step 4. Choose arbitrary integer $\ell = 4$ and compute the private key by using the following equation

$$D = \ell * K \bmod 37$$

$$D = 4 * \begin{bmatrix} 3 & 4 \\ 1 & 2 \end{bmatrix} \bmod 37 = \begin{bmatrix} 12 & 16 \\ 4 & 8 \end{bmatrix} \bmod 37$$

$$D = \begin{bmatrix} 12 & 16 \\ 4 & 8 \end{bmatrix} \bmod 37.$$

Step 5. Compute inverse of integer using extended Euclidean algorithm

$$4^{-1} = 28 \bmod 37; \text{Verify } (4^{-1} * 28) \bmod 37 = 1.$$

Step 6. Compute

$$E = \ell^{-1} * K^{-1}$$

$$E = 28 * \begin{bmatrix} 1 & 35 \\ 18 & 20 \end{bmatrix} \bmod 37 = \begin{bmatrix} 28 & 18 \\ 23 & 5 \end{bmatrix} \bmod 37,$$

so public key

$$E = \begin{bmatrix} 28 & 18 \\ 23 & 5 \end{bmatrix} \bmod 37.$$

Signature Generation

Alice selects a message to be sign as **'DEAN OMAR'**. Signing message in numerical form is 4, 5, 1, 14, 15, 13, 1, 18. As $n = 2$ Alice generate the blocks of the whole message into two characters each block.

For signature generation Alice performed the following step:

$$\text{Signature} = (\text{Private key} * \text{Message}) \bmod p$$

$$\begin{bmatrix} 12 & 16 \\ 4 & 8 \end{bmatrix} * \begin{bmatrix} 4 \\ 5 \end{bmatrix} \bmod 37 = \begin{bmatrix} 128 \\ 56 \end{bmatrix} \bmod 37 = \begin{bmatrix} 17 \\ 19 \end{bmatrix}.$$

Likewise the rest of the value have been computed:

$$\begin{bmatrix} 12 & 16 \\ 4 & 8 \end{bmatrix} * \begin{bmatrix} 1 \\ 14 \end{bmatrix} \bmod 37 = \begin{bmatrix} 236 \\ 116 \end{bmatrix} \bmod 37 = \begin{bmatrix} 14 \\ 5 \end{bmatrix}$$

$$\begin{bmatrix} 12 & 16 \\ 4 & 8 \end{bmatrix} * \begin{bmatrix} 15 \\ 13 \end{bmatrix} \bmod 37 = \begin{bmatrix} 388 \\ 164 \end{bmatrix} \bmod 37 = \begin{bmatrix} 18 \\ 16 \end{bmatrix}$$

$$\begin{bmatrix} 12 & 16 \\ 4 & 8 \end{bmatrix} * \begin{bmatrix} 1 \\ 18 \end{bmatrix} \bmod 37 = \begin{bmatrix} 300 \\ 148 \end{bmatrix} \bmod 37 = \begin{bmatrix} 4 \\ 0 \end{bmatrix}.$$

So she gets the signatures 17, 19, 14, 5, 18, 16, 4, 0. Now Alice sends the signature and message to Bob.

Signature Verification

Bob confirms Alice's sign with the help of public keys

$$E = \begin{bmatrix} 28 & 18 \\ 23 & 5 \end{bmatrix} \text{ and } p = 37.$$

For verification Bob compute:

$$\text{Message} = (\text{Public key} * \text{Signature}) \bmod p$$

$$\begin{bmatrix} 28 & 18 \\ 23 & 5 \end{bmatrix} * \begin{bmatrix} 17 \\ 19 \end{bmatrix} \bmod 37 = \begin{bmatrix} 818 \\ 486 \end{bmatrix} \bmod 37 = \begin{bmatrix} 4 \\ 5 \end{bmatrix}.$$

Likewise, he derives others using public key

$$\begin{bmatrix} 28 & 18 \\ 23 & 5 \end{bmatrix} * \begin{bmatrix} 14 \\ 5 \end{bmatrix} \text{ mod } 37 = \begin{bmatrix} 248 \\ 96 \end{bmatrix} \text{ mod } 37 = \begin{bmatrix} 1 \\ 14 \end{bmatrix}$$

$$\begin{bmatrix} 28 & 18 \\ 23 & 5 \end{bmatrix} * \begin{bmatrix} 18 \\ 16 \end{bmatrix} \text{ mod } 37 = \begin{bmatrix} 472 \\ 200 \end{bmatrix} \text{ mod } 37 = \begin{bmatrix} 15 \\ 13 \end{bmatrix}$$

$$\begin{bmatrix} 28 & 18 \\ 23 & 5 \end{bmatrix} * \begin{bmatrix} 4 \\ 0 \end{bmatrix} \text{ mod } 37 = \begin{bmatrix} 48 \\ 16 \end{bmatrix} \text{ mod } 37 = \begin{bmatrix} 1 \\ 18 \end{bmatrix}.$$

Our original message 4, 5, 1, 14, 15, 13, 1, 18. Since signature and received message both are same. Thus, message has been confirmed and acknowledged.

Example 3.2.2. Suppose $n = 3$, $p = 37$, and $M =$ "**HELLO OMAR**".

Key Generation

Step 1. Alice selects a random prime number *i.e.*,

$$p = 37.$$

Step 2. Choose the arbitrary invertible matrix

$$K = \begin{bmatrix} 1 & 2 & 3 \\ 0 & 1 & 4 \\ 5 & 6 & 0 \end{bmatrix} \text{ mod } 37.$$

Step 3. Compute K^{-1} using extended Euclidean algorithm

Calculating cofactor matrix:

$$C_{11} = (-1)^{1+1} \begin{vmatrix} 1 & 4 \\ 6 & 0 \end{vmatrix} = -24$$

$$C_{12} = (-1)^{1+2} \begin{vmatrix} 0 & 4 \\ 5 & 0 \end{vmatrix} = 20$$

$$C_{13} = (-1)^{1+3} \begin{vmatrix} 0 & 1 \\ 5 & 6 \end{vmatrix} = -5$$

$$C_{21} = (-1)^{2+1} \begin{vmatrix} 2 & 3 \\ 6 & 0 \end{vmatrix} = 18$$

$$C_{22} = (-1)^{2+2} \begin{vmatrix} 1 & 3 \\ 5 & 0 \end{vmatrix} = -15$$

$$C_{23} = (-1)^{2+3} \begin{vmatrix} 1 & 2 \\ 5 & 6 \end{vmatrix} = 4$$

$$C_{31} = (-1)^{3+1} \begin{vmatrix} 2 & 3 \\ 1 & 4 \end{vmatrix} = 5$$

$$C_{32} = (-1)^{3+2} \begin{vmatrix} 1 & 3 \\ 0 & 4 \end{vmatrix} = -4$$

$$C_{33} = (-1)^{3+3} \begin{vmatrix} 1 & 2 \\ 0 & 1 \end{vmatrix} = 1.$$

Thus, the cofactor matrix of K is,

$$[K_{ij}] = \begin{bmatrix} -24 & 20 & -5 \\ 18 & -15 & 4 \\ 5 & -4 & 1 \end{bmatrix}.$$

Now find the transpose of $[K_{ij}]$

$$\begin{bmatrix} -24 & 18 & 5 \\ 20 & -15 & -4 \\ -5 & 4 & 1 \end{bmatrix},$$

now,

$$d = det(K) = \begin{vmatrix} 1 & 2 & 3 \\ 0 & 1 & 4 \\ 5 & 6 & 0 \end{vmatrix} = 1\begin{vmatrix} 1 & 4 \\ 6 & 0 \end{vmatrix} - 2\begin{vmatrix} 0 & 4 \\ 5 & 6 \end{vmatrix} + 3\begin{vmatrix} 0 & 1 \\ 5 & 6 \end{vmatrix}$$

$$= 1(0 - 24) - 2(0 - 20) + 3(0 - 5) \bmod 37$$
$$= -24 + 40 - 15 \bmod 37$$
$$= 1 \bmod 37.$$

So required K^{-1} is,

$$K^{-1} = d^{-1} * [K_{ij}]^T$$

$$K^{-1} = 1^{-1} * \begin{bmatrix} -24 & 18 & 5 \\ 20 & -15 & -4 \\ -5 & 4 & 1 \end{bmatrix} \bmod 37$$

$$1^{-1} \bmod 37 = 1 \bmod 37$$

$$K^{-1} = \begin{bmatrix} -24 & 18 & 5 \\ 20 & -15 & -4 \\ -5 & 4 & 1 \end{bmatrix} \bmod 37 = \begin{bmatrix} 13 & 18 & 5 \\ 20 & 22 & 33 \\ 32 & 4 & 1 \end{bmatrix} \bmod 37.$$

Step 4. Choose arbitrary integer $\ell = 3$ and compute the private key by using the following equation

$$D = \ell * K \bmod 37$$

$$D = 3 * \begin{bmatrix} 1 & 2 & 3 \\ 0 & 1 & 4 \\ 5 & 6 & 0 \end{bmatrix} \bmod 37 = \begin{bmatrix} 3 & 6 & 9 \\ 0 & 3 & 12 \\ 15 & 18 & 0 \end{bmatrix} \bmod 37$$

$$D = \begin{bmatrix} 3 & 6 & 9 \\ 0 & 3 & 12 \\ 15 & 18 & 0 \end{bmatrix} \bmod 37.$$

Step 5. Compute inverse of integer by using extended Euclidean algorithm

$$3^{-1} \bmod 37 = 25; \text{Verify } (3^{-1} * 25) \bmod 37 = 1.$$

Step 6. Compute

$$E = \ell^{-1} * K^{-1}$$

$$E = 25 * \begin{bmatrix} 13 & 18 & 5 \\ 20 & 22 & 33 \\ 32 & 4 & 1 \end{bmatrix} \bmod 37 = \begin{bmatrix} 325 & 450 & 125 \\ 500 & 550 & 825 \\ 800 & 100 & 25 \end{bmatrix} \bmod 37$$

$$E = \begin{bmatrix} 29 & 6 & 14 \\ 19 & 32 & 11 \\ 23 & 26 & 25 \end{bmatrix} \bmod 37.$$

Signature Generation

Alice selects a message to be sign as "**HELLO OMAR**". Signing message in numerical form is 8, 5, 12, 12, 15, 15, 13, 1, 18. As $n = 3$ Alice generate the blocks of the whole message into three characters each block.

For signature generation Alice performed the following step:

$$\text{Signature} = (\text{Private key} * \text{Message}) \bmod p$$

$$\begin{bmatrix} 3 & 6 & 9 \\ 0 & 3 & 12 \\ 15 & 18 & 0 \end{bmatrix} * \begin{bmatrix} 8 \\ 5 \\ 12 \end{bmatrix} \bmod 37 = \begin{bmatrix} 162 \\ 159 \\ 210 \end{bmatrix} \bmod 37 = \begin{bmatrix} 14 \\ 11 \\ 25 \end{bmatrix}$$

$$\begin{bmatrix} 3 & 6 & 9 \\ 0 & 3 & 12 \\ 15 & 18 & 0 \end{bmatrix} * \begin{bmatrix} 12 \\ 15 \\ 15 \end{bmatrix} \bmod 37 = \begin{bmatrix} 261 \\ 225 \\ 450 \end{bmatrix} \bmod 37 = \begin{bmatrix} 2 \\ 3 \\ 6 \end{bmatrix}$$

$$\begin{bmatrix} 3 & 6 & 9 \\ 0 & 3 & 12 \\ 15 & 18 & 0 \end{bmatrix} * \begin{bmatrix} 13 \\ 1 \\ 18 \end{bmatrix} \bmod 37 = \begin{bmatrix} 207 \\ 219 \\ 213 \end{bmatrix} \bmod 37 = \begin{bmatrix} 22 \\ 34 \\ 28 \end{bmatrix}.$$

So she gets the signatures 14, 11, 25, 2, 3, 6, 22, 34, 28. Now Alice sends the signature and message to Bob.

Signature Verification

Bob confirms Alice's sign with the help of public keys

$$E = \begin{bmatrix} 29 & 6 & 14 \\ 19 & 32 & 11 \\ 23 & 26 & 25 \end{bmatrix} \text{ and } p = 37.$$

For verification Bob compute:

$$\text{Message} = (\text{Public key} * \text{Signature}) \bmod p$$

$$\begin{bmatrix} 29 & 6 & 14 \\ 19 & 32 & 11 \\ 23 & 26 & 25 \end{bmatrix} * \begin{bmatrix} 14 \\ 11 \\ 25 \end{bmatrix} \bmod 37 = \begin{bmatrix} 822 \\ 893 \\ 1233 \end{bmatrix} \bmod 37 = \begin{bmatrix} 8 \\ 5 \\ 12 \end{bmatrix}$$

$$\begin{bmatrix} 29 & 6 & 14 \\ 19 & 32 & 11 \\ 23 & 26 & 25 \end{bmatrix} * \begin{bmatrix} 2 \\ 3 \\ 6 \end{bmatrix} \bmod 37 = \begin{bmatrix} 160 \\ 200 \\ 274 \end{bmatrix} \bmod 37 = \begin{bmatrix} 12 \\ 15 \\ 15 \end{bmatrix}$$

$$\begin{bmatrix} 29 & 6 & 14 \\ 19 & 32 & 11 \\ 23 & 26 & 25 \end{bmatrix} * \begin{bmatrix} 22 \\ 34 \\ 28 \end{bmatrix} \bmod 37 = \begin{bmatrix} 1234 \\ 1814 \\ 2090 \end{bmatrix} \bmod 37 = \begin{bmatrix} 13 \\ 1 \\ 18 \end{bmatrix}.$$

Our original message 8, 5, 12, 12, 15, 15, 13, 1, 18. Thus, signature and received message both are same. Message has been verified and accepted.

3.3 Cryptanalysis

In this section, we discuss the security of digital signature scheme 3.2 based on a block cipher. Originally the Hill cipher [45] is a symmetric key scheme but the present signature scheme [24] it is used as an asymmetric key scheme. The digital signature scheme works as fellows:

$$\text{Signature} = (\text{Message} * \text{Private key}) \bmod p. \tag{3.1}$$

The generated signature and the original message are sent to Bob. He is uses the public key of sender (Alice) and message to verify Alice's signature.

$$\text{Message} = (\text{Public key} * \text{Signature}) \bmod p. \tag{3.2}$$

First note that from the key generation (Algorithm 3.1.1), we have,

Public keys: The square matrix E of order n and a prime p.

Private key: The Square matrix D of order n.

Since we have the information about public keys E, p and our aim is to find the private key D. From the general method of the cryptanalysis attack:

Let Message vector $m = \begin{bmatrix} m_1 \\ m_2 \end{bmatrix}$; Signature $s = \begin{bmatrix} s_1 \\ s_2 \end{bmatrix}$; Private key $D = \begin{bmatrix} k_{11} & k_{12} \\ k_{21} & k_{22} \end{bmatrix}$.

Suppose also that the public key matrix be given by $E = \begin{bmatrix} e_{11} & e_{12} \\ e_{21} & e_{22} \end{bmatrix}$.

From (3.2), we have

$$\underset{\substack{\uparrow \\ \text{unknown}}}{\begin{bmatrix} m_1 \\ m_2 \end{bmatrix}} = \underset{\substack{\uparrow \\ \text{known}}}{\begin{bmatrix} e_{11} & e_{12} \\ e_{21} & e_{22} \end{bmatrix}} * \underset{\substack{\uparrow \\ \text{known}}}{\begin{bmatrix} s_1 \\ s_2 \end{bmatrix}}$$

In the above procedure, we have the information about public key and signature that Alice sends to Bob. We multiply both of them and get the message $\begin{bmatrix} m_1 \\ m_2 \end{bmatrix}$.

Now from (3.1)

$$\underset{\substack{\uparrow \\ \text{known}}}{\begin{bmatrix} s_1 \\ s_2 \end{bmatrix}} = \underset{\substack{\uparrow \\ \text{unknown}}}{\begin{bmatrix} k_{11} & k_{12} \\ k_{21} & k_{22} \end{bmatrix}} * \underset{\substack{\uparrow \\ \text{known}}}{\begin{bmatrix} m_1 \\ m_2 \end{bmatrix}}$$

This will results in four linear equations in four unknowns. If the matrix D is invertible mod p, we can find D the private key from this scheme.

The next examples illustrates the known plaintext attack on the data from 3.2.1.

Example 3.3.1. Digital signature scheme is vulnerable to a known-plaintext attack, because it is linear (if you know the plaintext and the corresponding ciphertext, the key can be recovered). An adversary who intercepts multiple pairs of plaintext/ciphertext characters provides a system of linear equations that can be solved easily. If system is inconsistent, only a few more plaintext/ciphertext pairs need to be added.

Let $D = \begin{bmatrix} k_{11} & k_{12} \\ k_{21} & k_{22} \end{bmatrix}$ be the private key and $m = \begin{bmatrix} m_1 \\ m_2 \end{bmatrix}$ be the message.

For the Example 3.2.1, we have the digital signature **2, 12, 11, 0, 18, 5, 23, 23**

which corresponds to "***DEAN OMAR***" **4, 5, 1, 14, 15, 13, 1, 18**.

We have the signature $s = \begin{bmatrix} 2 \\ 12 \end{bmatrix}$ and public keys $E = \begin{bmatrix} 27 & 2 \\ 8 & 33 \end{bmatrix}$, $p = 37$.

Recall that the message array is rearranged by using public key $E = \begin{bmatrix} 27 & 2 \\ 8 & 33 \end{bmatrix}$, signature factor $s = \begin{bmatrix} 2 \\ 12 \end{bmatrix}$ and the original message is $m = \begin{bmatrix} m_1 \\ m_2 \end{bmatrix}$.

For instance, the (m_1, m_2) is recovered as follows by using the signature $(s_1, s_2) = (2, 12)$.

$$\begin{bmatrix} m_1 \\ m_2 \end{bmatrix} = \begin{bmatrix} 27 & 2 \\ 8 & 33 \end{bmatrix} * \begin{bmatrix} 2 \\ 12 \end{bmatrix} \text{ mod } 37$$

$$\begin{bmatrix} m_1 \\ m_2 \end{bmatrix} = \begin{bmatrix} 78 \\ 412 \end{bmatrix} \text{ mod } 37 = \begin{bmatrix} 4 \\ 5 \end{bmatrix}.$$

We get a message from the above procedure.

Choosing the signature pair $(2, 12)$ and $(11, 0)$ with corresponding message element pairs $(4, 5)$ and $(1, 14)$ respectively. We mount the attack as follows:

$$\begin{bmatrix} 2 \\ 12 \end{bmatrix} = \begin{bmatrix} k_{11} & k_{12} \\ k_{21} & k_{22} \end{bmatrix} * \begin{bmatrix} 4 \\ 5 \end{bmatrix} \text{ mod } 37$$

$$4k_{11} + 5k_{12} = 2 \mod 37$$

$$4k_{21} + 5k_{22} = 12 \mod 37$$

and

$$\begin{bmatrix} 11 \\ 0 \end{bmatrix} = \begin{bmatrix} k_{11} & k_{12} \\ k_{21} & k_{22} \end{bmatrix} * \begin{bmatrix} 1 \\ 14 \end{bmatrix} \text{ mod } 37$$

$$k_{11} + 14k_{12} = 11 \mod 37$$

$$k_{21} + 14k_{22} = 0 \mod 37.$$

Now we solve the following linear system of equations in mod 37

$$4k_{11} + 5k_{12} = 2 \mod 37 \tag{3.3}$$

$$k_{11} + 14k_{12} = 11 \mod 37 \tag{3.4}$$

and

$$4k_{21} + 5k_{22} = 12 \mod 37 \tag{3.5}$$

$$k_{21} + 14k_{22} = 0 \mod 37 \tag{3.6}$$

starting with (3.4), we have

$$k_{11} + 14k_{12} = 11 \mod 37$$

$$\Longrightarrow k_{11} = 11 - 14k_{12} \mod 37 \tag{3.7}$$

substituting in (3.3) to get

$$4(11 - 14k_{12}) + 5k_{12} = 2 \mod 37$$

$$\Longrightarrow 44 - 56k_{12} + 5k_{12} = 2 \mod 37$$

$$-51k_{12} = 42 \mod 37$$

$$k_{12} = \frac{42}{51} = \frac{5}{14} \mod 37 = 5(14)^{-1} \mod 37$$

$$k_{12} = 5(8) = 40 \mod 37$$

$$k_{12} = 3 \mod 37.$$

Using the value of k_{12} in (3.7)

$$k_{11} = 11 - 14(3) = -31 \mod 37$$

$$k_{11} = 6 \mod 37.$$

Similarly from (3.6), we have

$$k_{21} + 14k_{22} = 0 \mod 37$$

$$\Longrightarrow k_{21} = -14k_{22} \mod 37 \tag{3.8}$$

uses the value of k_{21} in Equation (3.5), we get

$$4(-14k_{22}) + 5k_{22} = 12 \mod 37$$

$$-51k_{22} = 12 \mod 37$$

$$k_{22} = \frac{12}{51} = \frac{12}{23} \mod 37$$

$$k_{22} = 12(23^{-1}) \mod 37$$

$$k_{22} = 12(29) = 348 \mod 37$$

$$k_{22} = -15 \mod 37.$$

Using the value of k_{22} in Equation (3.8), we get

$$k_{21} = -14(15) = -210 \mod 37$$

$$k_{21} = 12 \mod 37.$$

Hence the private key is recovered as

$$D = \begin{bmatrix} k_{11} & k_{12} \\ k_{21} & k_{22} \end{bmatrix} = \begin{bmatrix} 6 & 13 \\ 12 & 15 \end{bmatrix}.$$

Now the attack can alter the original message and send it to Bob by using Alice's private key.

Example 3.3.2. Let $D = \begin{bmatrix} k_{11} & k_{12} & k_{13} \\ k_{21} & k_{22} & k_{23} \\ k_{31} & k_{32} & k_{33} \end{bmatrix}$ be the private key and $m = \begin{bmatrix} m_1 \\ m_2 \\ m_3 \end{bmatrix}$ be the message. For the Example 3.2.2, we have the digital signature **14, 11, 25, 2, 3, 6, 22, 34, 28** which corresponds to "***HELLO OMAR***" **8, 5, 12, 12, 15, 15, 13, 1, 18.** Since we have the signature $\mathbf{s} = \begin{bmatrix} 14 \\ 11 \\ 25 \end{bmatrix}$, Public keys $E = \begin{bmatrix} 29 & 6 & 14 \\ 19 & 32 & 11 \\ 23 & 26 & 25 \end{bmatrix}$ and $p = 37$.

Recall that the message array is rearranged by using public key $E = \begin{bmatrix} 29 & 6 & 14 \\ 19 & 32 & 11 \\ 23 & 26 & 25 \end{bmatrix}$, signature $s = \begin{bmatrix} 14 \\ 11 \\ 25 \end{bmatrix}$ and the original message array is $m = \begin{bmatrix} m_1 \\ m_2 \\ m_3 \end{bmatrix}$.

For instance, the (m_1, m_2, m_3) is recovered as follows by using the signature $(s_1, s_2, s_3) = (14, 11, 25)$.

$$\begin{bmatrix} m_1 \\ m_2 \\ m_3 \end{bmatrix} = \begin{bmatrix} 29 & 6 & 14 \\ 19 & 32 & 11 \\ 23 & 26 & 25 \end{bmatrix} * \begin{bmatrix} 14 \\ 11 \\ 25 \end{bmatrix} \mod 37$$

$$\begin{bmatrix} m_1 \\ m_2 \\ m_3 \end{bmatrix} = \begin{bmatrix} 822 \\ 893 \\ 1233 \end{bmatrix} \mod 37 = \begin{bmatrix} 8 \\ 5 \\ 12 \end{bmatrix}.$$

Hence we got message from above procedure. Choosing the signature pair $(14, 11, 25)$, $(2, 3, 6)$, and $(22, 34, 28)$ with corresponding massage element pairs $(8, 5, 12)$, $(12, 15, 15)$, and $(13, 1, 18)$ respectively. We mount the attack as follows:

$$\begin{bmatrix} 14 \\ 11 \\ 25 \end{bmatrix} = \begin{bmatrix} k_{11} & k_{12} & k_{13} \\ k_{21} & k_{22} & k_{23} \\ k_{31} & k_{32} & k_{33} \end{bmatrix} * \begin{bmatrix} 8 \\ 5 \\ 12 \end{bmatrix} \mod 37$$

$$8k_{11} + 5k_{12} + 12k_{13} = 14 \mod 37 \tag{3.9}$$

$$8k_{21} + 5k_{22} + 12k_{23} = 11 \mod 37 \tag{3.10}$$

$$8k_{31} + 5k_{32} + 12k_{33} = 25 \mod 37 \tag{3.11}$$

and

$$\begin{bmatrix} 2 \\ 3 \\ 6 \end{bmatrix} = \begin{bmatrix} k_{11} & k_{12} & k_{13} \\ k_{21} & k_{22} & k_{23} \\ k_{31} & k_{32} & k_{33} \end{bmatrix} * \begin{bmatrix} 12 \\ 15 \\ 15 \end{bmatrix} \mod 37$$

$$12k_{11} + 15k_{12} + 15k_{13} = 2 \mod 37 \tag{3.12}$$

$$12k_{21} + 15k_{22} + 15k_{23} = 3 \mod 37 \tag{3.13}$$

$$12k_{31} + 15k_{32} + 15k_{33} = 6 \mod 37. \tag{3.14}$$

Similarly from Equation (3.1)

$$\begin{bmatrix} 22 \\ 34 \\ 28 \end{bmatrix} = \begin{bmatrix} k_{11} & k_{12} & k_{13} \\ k_{21} & k_{22} & k_{23} \\ k_{31} & k_{32} & k_{33} \end{bmatrix} * \begin{bmatrix} 13 \\ 1 \\ 18 \end{bmatrix} \mod 37$$

$$13k_{11} + k_{12} + 18k_{13} = 22 \mod 37 \tag{3.15}$$

$$13k_{21} + k_{22} + 18k_{33} = 34 \mod 37 \tag{3.16}$$

$$13k_{31} + k_{32} + 18k_{33} = 28 \mod 37. \tag{3.17}$$

Solving with (3.9) and (3.12), we have

$$24k_{11} + 15k_{12} + 36k_{13} = 42 \mod 37 \tag{3.18}$$

$$\underline{-12k_{11} \pm 15k_{12} \pm 15k_{13} = -22 \mod 37} \tag{3.19}$$

$$12k_{11} + 21k_{13} = 3 \mod 37. \tag{3.20}$$

Solving with (3.12) and (3.15), we have

$$12k_{11} + 15k_{12} + 15k_{13} = 2 \mod 37 \tag{3.21}$$

$$\underline{-195k_{11} \pm 15k_{12} \pm 270k_{13} = -330 \mod 37} \tag{3.22}$$

$$35k_{11} + 33k_{13} = 32 \mod 37. \tag{3.23}$$

Solving with (3.20) and (3.23), we have

$$420k_{11} + 735k_{13} = 105 \mod 37 \tag{3.24}$$

$$\underline{-420k_{11} \pm 396k_{13} = -384 \mod 37} \tag{3.25}$$

$$6k_{13} = 17 \mod 37 \tag{3.26}$$

$$k_{13} = (6^{-1})17 \mod 37$$

$$6^{-1} \text{mod } 37 = 31 \mod 37$$

$$\implies k_{13} = (31)17 \mod 37$$

$$k_{13} = 9 \mod 37.$$

Substituting in (3.23) to get

$$35k_{11} + 33(9) = 32 \mod 37$$

$$35k_{11} = 32 - 297 \mod 37$$

$$35k_{11} = -265 = 31 \mod 37$$

$$k_{11} = (35^{-1})31 = (18)(31) \mod 37$$

$$k_{11} = 558 = 3 \mod 37.$$

Using the value of k_{11} and k_{13} in (3.9)

$$8(3) + 5k_{12} + 12(9) = 14 \mod 37$$

$$5k_{12} = 14 - 132 = -118 \mod 37$$

$$5k_{12} = 30 \mod 37$$

$$k_{12} = (5^{-1})30 \mod 37$$

$$k_{12} = (15)30 = 450 = 6 \mod 37.$$

Hence required solution is $k_{11} = 3$; $k_{12} = 6$; $k_{13} = 9$.
Similarly from (3.10), (3.13) and (3.16), we get $k_{21} = 0$; $k_{22} = 3$; $k_{23} = 12$. And similarly from (3.11), (3.14) and (3.17), we get $k_{31} = 15$; $k_{32} = 18$; $k_{33} = 0$.
Hence the private key is recovered as

$$D = \begin{bmatrix} k_{11} & k_{12} & k_{13} \\ k_{21} & k_{22} & k_{23} \\ k_{31} & k_{32} & k_{33} \end{bmatrix} = \begin{bmatrix} 3 & 6 & 9 \\ 0 & 3 & 12 \\ 15 & 18 & 0 \end{bmatrix}.$$

Which is the key used for the signature. Hence we successfully found the key used for the digital signature scheme proposed by Kuppuswamy et al. [24] using the known-plaintext attack. Results of the simulation show that the original digital signature can be revealed successfully. Now the attacker can sign any other document or message with Alice's private key. The receiver will not be able to judge that the message is not signed by Alice.

Chapter 4

Encryption Scheme based on Self-Invertible Hill Cipher

In this chapter, we discuss the encryption scheme based on self-invertible Hill cipher presented by Kumar et al. [25]. This article describes the cryptographic scheme for the Hill cipher algorithm to generate a self-invertible matrix. The cryptanalysis of the above mentioned scheme shows that it has many security flaws. In this chapter, we show that the proposed scheme is vulnerable to known-plaintext attack. First we recall the Hill cipher scheme in the next section.

4.1 Hill Cipher

The Hill cipher is a polygraphic substitution cipher based on linear algebra. It is invented in 1929 by Lester S. Hill. This was the first polygraphic cipher that became practical (though barely) for work on more than three symbols at once. Hill used matrices and matrix multiplication to mix up the plaintext. Hill cipher algorithm takes m plaintext letters and replaces them with m numbers.

Alice wants to share the information with Bob. Before sharing the information both parties fix a common secret key K as an $n \times n$ invertible matrix modulo an integer m. The set of alphabet is also fixed, for example 26. Alice will perform the following steps.

Algorithm 4.1.1 (Hill Encryption Algorithm)

Input: An $n \times n$ invertible matrix and a plaintext M.

Output: Ciphertext vectors w_i; $(i = 1, 2, ..., t)$.

Step 1. Take the message/plaintext M (by eliminating all spaces and marks of punctuation) to be sent to Bob.

Step 2. English alphabets $A, B, C, ..., Z$ assigned a numerical value, including A = 0, B = 1, ... Z = 25. The size of the set of alphabets will determine the work in modulus "m" for the arithmetic operations. In the present case m = 26.

Step 3. Split the number string into size n blocks. Remember if K is a matrix of $n \times n$ so block size is n. Also note that, if the document is not uniformly split into n size blocks then we pad the words at the end of the document, this can be achieved arbitrarily.

Step 4. Write each block from Step 3 as a size n column vector. Thus a series of n-dimensional vectors, v_1**,** v_2**, ...,** v_t can be obtained.

Step 5. Take each vector v_i; i = 1, 2, ... t and multiply it by encryption key K to compute the corresponding ciphertext vectors w_i; i.e $Kv_i = w_i$ $(i = 1, 2, ..., t)$.

Step 6. Take the vectors w_i; i = 1, 2, ... t, write the vector entries in sequence, convert elements of each vector into their corresponding characters as described in Step 2 and get the alphabetic ciphertext.

Now Bob has the encrypted message and the encryption key, therefore he can decode the received message sent by Alice. The decryption algorithm is basically same as the algorithm for encryption, except that K^{-1} is used instead of K.

Since $KM = C$, and K is invertible thus one we can calculate $M = K^{-1}C$. We will call the decryption key matrix $D = K^{-1}$, thus $DC = M$. Remember that this inverse is taken under modulo m.

Algorithm 4.1.2 Hill Decryption Algorithm

Input: Ciphertext vectors w_i; $(i = 1, 2, ..., t)$.

Output: Plaintext vectors v_i; $(i = 1, 2, ..., t)$.

Step 1. Calculate

$$K^{-1} \bmod m.$$

It will be treated as the decryption key.

Step 2. Convert the received ciphertext into string of integers.

Step 3. For each ciphertext column vector w_i, compute the corresponding plaintext vectors v_i as:

$$v_i = K^{-1} v_i \ \bmod \ m.(i = 1,\ 2,\ ...,\ t)$$

Example 4.1.1. Encryption using Hill Cipher

To encrypt a document by using the Hill cipher, we need to convert the **keyword** into a key matrix (ordered 2 x 2 or 3 x 3) matrix operating with **digraphs** and **trigraphs**, respectively. Transform the plaintext as a column vector into digraphs (or trigraphs). Then conduct matrix operations by taking the alphabet length module (*i.e.* 26) over each vector. To provide the ciphertext, these vectors are then changed into letters.

The plaintext message **"retreat now"** will be encrypted by using the **BACKUP** keyphrase and 3 x 3 matrix. Turning the key phrase into a matrix is the first step. Note that the key phrase is a few short letters, therefore with the end of the letter, we fill with the final elements.

$$\begin{pmatrix} B & A & C \\ K & U & P \\ A & B & C \end{pmatrix}$$

the keyword is written in the form of matrix.

$$\begin{pmatrix} 1 & 0 & 2 \\ 10 & 20 & 15 \\ 0 & 1 & 2 \end{pmatrix}$$

the key matrix discovered by taking the keyword letters numeric values.

The plaintext is split into trigraphs (we use a 3 x 3 matrix, so we need three letter groups), and transform these into vector columns. Since the plaintext does not match perfectly into the vectors of the column, to get the plaintext of the right size, we need to pad it with some nulls. Then convert plaintext into column vectors.

$$v_1 = \begin{bmatrix} r \\ e \\ t \end{bmatrix}; v_2 = \begin{bmatrix} r \\ e \\ a \end{bmatrix}; v_3 = \begin{bmatrix} t \\ n \\ o \end{bmatrix}; v_4 = \begin{bmatrix} w \\ x \\ x \end{bmatrix}$$

the plaintext in column vectors was split into trigraphs. Remember the inclusion of nulls to make it column vectors of the proper length.

$$v_1 = \begin{bmatrix} 17 \\ 4 \\ 19 \end{bmatrix}; v_2 = \begin{bmatrix} 17 \\ 4 \\ 0 \end{bmatrix}; v_3 = \begin{bmatrix} 19 \\ 13 \\ 14 \end{bmatrix}; v_4 = \begin{bmatrix} 22 \\ 23 \\ 23 \end{bmatrix}$$

the plaintext was transformed into the vectors of numeric columns.

Now, combine the top row of the key matrix with the column vector to encrypt the top element of the subsequent column vector in order to perform multiplication in matrix. Then encrypt the key matrix centerline with the column vector to induce the subsequent column vector center component. And likewise for the bottom row. In this way we get six numbers as the result of the product of the first elements of key matrix with the top element of column vector of plaintext. Multiply by the middle component of the column vector the second component of the key matrix row, and multiply the key matrix row's third element by the column vector's bottom element. By adding the three responses altogether we have.

$$\begin{bmatrix} 1 & 0 & 2 \\ 10 & 20 & 15 \\ 0 & 1 & 2 \end{bmatrix} \begin{bmatrix} 17 \\ 4 \\ 19 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 1 \times 17 + 0 \times 4 + 2 \times 19 \\ 10 \times 17 + 20 \times 4 + 15 \times 19 \\ 0 \times 17 + 1 \times 4 + 2 \times 19 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} 3 \\ 15 \\ 16 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} d \\ p \\ q \end{bmatrix} \bmod 26.$$

Likewise, the rest of the trigraphs are encoded as fellow:

$$\begin{bmatrix} B & A & C \\ K & U & P \\ A & B & C \end{bmatrix} \begin{bmatrix} r \\ e \\ a \end{bmatrix} = \begin{bmatrix} 1 & 0 & 2 \\ 10 & 20 & 15 \\ 0 & 1 & 2 \end{bmatrix} \begin{bmatrix} 17 \\ 4 \\ 0 \end{bmatrix} = \begin{bmatrix} 17 \\ 250 \\ 4 \end{bmatrix} = \begin{bmatrix} 17 \\ 16 \\ 4 \end{bmatrix} \bmod 26 = \begin{bmatrix} r \\ q \\ e \end{bmatrix}$$

$$\begin{bmatrix} B & A & C \\ K & U & P \\ A & B & C \end{bmatrix} \begin{bmatrix} t \\ n \\ o \end{bmatrix} = \begin{bmatrix} 1 & 0 & 2 \\ 10 & 20 & 15 \\ 0 & 1 & 2 \end{bmatrix} \begin{bmatrix} 19 \\ 13 \\ 14 \end{bmatrix} = \begin{bmatrix} 47 \\ 660 \\ 41 \end{bmatrix} = \begin{bmatrix} 21 \\ 10 \\ 15 \end{bmatrix} \bmod 26 = \begin{bmatrix} v \\ k \\ r \end{bmatrix}$$

$$\begin{bmatrix} B & A & C \\ K & U & P \\ A & B & C \end{bmatrix} \begin{bmatrix} w \\ x \\ x \end{bmatrix} = \begin{bmatrix} 1 & 0 & 2 \\ 10 & 20 & 15 \\ 0 & 1 & 2 \end{bmatrix} \begin{bmatrix} 22 \\ 23 \\ 23 \end{bmatrix} = \begin{bmatrix} 68 \\ 1025 \\ 69 \end{bmatrix} = \begin{bmatrix} 16 \\ 11 \\ 17 \end{bmatrix} \bmod 26 = \begin{bmatrix} q \\ l \\ r \end{bmatrix}.$$

This provides us the final ciphertext **"dpqrq evkpq lr"**.

Decryption using Hill Cipher

The inverse matrix should be found to decode a ciphertext encoded using the Hill cipher. The decryption method is the same as encoding if we have the inverse matrix. The inverse key matrix is multiplied by the cipher column vectors then taking the alphabet size of the results modulo and transform the numbers back to letters.

In particular, perform the calculation below to determine the inverse of the key matrix, where K is the key matrix, d is the key matrix determinant and adj(K) is a K matrix adjoint.

$$K^{-1} = d^{-1} \times adj(K), \tag{4.1}$$

as

$$\text{K} = \begin{bmatrix} k_{11} & k_{12} & k_{13} \\ k_{21} & k_{22} & k_{23} \\ k_{31} & k_{32} & k_{33} \end{bmatrix}$$

$$d = det(K) = \begin{vmatrix} 1 & 0 & 2 \\ 10 & 20 & 15 \\ 0 & 1 & 2 \end{vmatrix} = 1\begin{vmatrix} 20 & 15 \\ 1 & 2 \end{vmatrix} - 0\begin{vmatrix} 10 & 15 \\ 0 & 2 \end{vmatrix} + 2\begin{vmatrix} 10 & 20 \\ 0 & 1 \end{vmatrix}$$

$$= 1(40 - 15) - 0(20 - 0) + 2(10 - 0) \text{ mod } 26$$

$$= 25 - 0 + 20 \text{ mod } 26$$

$$= 45 \text{ mod } 26$$

$$= 19 \text{ mod } 26.$$

Using extended Euclidean algorithm, compute d^{-1} mod 26.

$$19^{-1} \text{ mod } 26 = 11; \text{Verify } (19^{-1} * 11) \text{ mod } 26 = 1.$$

Calculating cofactor matrix of K:

$$C_{11} = (-1)^{1+1}\begin{vmatrix} 20 & 15 \\ 1 & 2 \end{vmatrix} = 25$$

$$C_{12} = (-1)^{1+2}\begin{vmatrix}10 & 15\\ 0 & 2\end{vmatrix} = -20$$

$$C_{13} = (-1)^{1+3}\begin{vmatrix}10 & 20\\ 0 & 1\end{vmatrix} = 10$$

$$C_{21} = (-1)^{2+1}\begin{vmatrix}0 & 2\\ 1 & 2\end{vmatrix} = 2$$

$$C_{22} = (-1)^{2+2}\begin{vmatrix}1 & 2\\ 0 & 2\end{vmatrix} = 2$$

$$C_{23} = (-1)^{2+3}\begin{vmatrix}1 & 0\\ 0 & 1\end{vmatrix} = -1$$

$$C_{31} = (-1)^{3+1}\begin{vmatrix}0 & 2\\ 20 & 15\end{vmatrix} = -40$$

$$C_{32} = (-1)^{3+2}\begin{vmatrix}1 & 2\\ 10 & 15\end{vmatrix} = 5$$

$$C_{33} = (-1)^{3+3}\begin{vmatrix}1 & 0\\ 10 & 20\end{vmatrix} = 20.$$

Thus, the cofactor matrix of K is

$$[K_{ij}] = \begin{bmatrix}25 & -20 & 10\\ 2 & 2 & -1\\ -40 & 5 & 20\end{bmatrix},$$

now find the transpose of $[K_{ij}]$

$$\begin{bmatrix}25 & 2 & -40\\ -20 & 2 & 5\\ 10 & -1 & 20\end{bmatrix},$$

so required K^{-1} is

$$K^{-1} = d^{-1} * [K_{ij}]^T$$

$$K^{-1} = 19^{-1} * \begin{bmatrix} 25 & 2 & -40 \\ -20 & 2 & 5 \\ 10 & -1 & 20 \end{bmatrix} \text{mod } 26$$

$$K^{-1} = 11 * \begin{bmatrix} 25 & 2 & -40 \\ -20 & 2 & 5 \\ 10 & -1 & 20 \end{bmatrix} \text{mod } 26$$

$$K^{-1} = \begin{bmatrix} 275 & 22 & -440 \\ -220 & 22 & 55 \\ 110 & -11 & 220 \end{bmatrix} \text{mod } 26$$

$$K^{-1} = \begin{bmatrix} 15 & 22 & 2 \\ 14 & 22 & 3 \\ 6 & 15 & 12 \end{bmatrix} \text{mod } 26.$$

We computed the inverse of the key matrix, now we multiply K^{-1} by each cipher to get the plaintext matrix:

Decryption of trigraphs:

$$\begin{bmatrix} 15 & 22 & 2 \\ 14 & 22 & 3 \\ 6 & 15 & 12 \end{bmatrix} \begin{bmatrix} d \\ p \\ q \end{bmatrix} = \begin{bmatrix} 15 & 22 & 2 \\ 14 & 22 & 3 \\ 6 & 15 & 12 \end{bmatrix} \begin{bmatrix} 3 \\ 15 \\ 16 \end{bmatrix} = \begin{bmatrix} 55 \\ 535 \\ 42 \end{bmatrix} = \begin{bmatrix} 17 \\ 4 \\ 19 \end{bmatrix} \text{mod } 26 = \begin{bmatrix} r \\ e \\ t \end{bmatrix}$$

$$\begin{bmatrix} 15 & 22 & 2 \\ 14 & 22 & 3 \\ 6 & 15 & 12 \end{bmatrix} \begin{bmatrix} r \\ q \\ e \end{bmatrix} = \begin{bmatrix} 15 & 22 & 2 \\ 14 & 22 & 3 \\ 6 & 15 & 12 \end{bmatrix} \begin{bmatrix} 17 \\ 16 \\ 4 \end{bmatrix} = \begin{bmatrix} 17 \\ 250 \\ 4 \end{bmatrix} = \begin{bmatrix} 17 \\ 4 \\ 0 \end{bmatrix} \text{mod } 26 = \begin{bmatrix} r \\ e \\ a \end{bmatrix}$$

$$\begin{bmatrix} 15 & 22 & 2 \\ 14 & 22 & 3 \\ 6 & 15 & 12 \end{bmatrix} \begin{bmatrix} v \\ k \\ r \end{bmatrix} = \begin{bmatrix} 15 & 22 & 2 \\ 14 & 22 & 3 \\ 6 & 15 & 12 \end{bmatrix} \begin{bmatrix} 21 \\ 10 \\ 15 \end{bmatrix} = \begin{bmatrix} 47 \\ 660 \\ 41 \end{bmatrix} = \begin{bmatrix} 19 \\ 13 \\ 14 \end{bmatrix} \text{mod } 26 = \begin{bmatrix} t \\ n \\ 0 \end{bmatrix}$$

$$\begin{bmatrix} 15 & 22 & 2 \\ 14 & 22 & 3 \\ 6 & 15 & 12 \end{bmatrix} \begin{bmatrix} q \\ l \\ r \end{bmatrix} = \begin{bmatrix} 15 & 22 & 2 \\ 14 & 22 & 3 \\ 6 & 15 & 12 \end{bmatrix} \begin{bmatrix} 16 \\ 11 \\ 17 \end{bmatrix} = \begin{bmatrix} 68 \\ 1025 \\ 69 \end{bmatrix} = \begin{bmatrix} 22 \\ 23 \\ 23 \end{bmatrix} \bmod 26 = \begin{bmatrix} w \\ x \\ x \end{bmatrix}.$$

This provides us the final plaintext **"retreat now"**.

Example 4.1.2. Since the Hill cipher technique is linear technique for the cryptanalysis. To evaluate the key matrix, just two bigraph need to be found. If we have to know that 'TH' is encrypted to 'GK' and 'ER' is encrypted to 'BD', we compute the collection of the equations and discover the key matrix for coding. To break the cipher, we must focus on the above described. The technique being presented here may impact on the understanding of several phrases in the message. Consider the ciphertext:

"FUPCMTGZKYUKBQFJHUKTZKKIXTTA".

We know that somewhere in the text phrase will "OF THE" occurs. This implies that on the following cases is right (recall the character pairs in Hill cipher encryption):

"FU PC MT GZ KY UK BQ FJ HU KT ZK KI XT TA

OF TH E. .. ..

.O FT HE .. ..

.. OF TH E. .. ..

.. .O FT HE .. ..

.. .. OF TH E. .. ..

.. .. .O FT HE .. .."

and so on. If the second row is right, you have got the following: $PC \to FT$ *i.e.* PC pairs are decrypted FT, and $MT \to HE$. Set the equation now (replacement of A by 0, B by 1, O by 14, etc.) which collects this data:

$$D\begin{bmatrix} P \\ C \end{bmatrix} = \begin{bmatrix} F \\ T \end{bmatrix} \rightarrow D\begin{bmatrix} 15 \\ 2 \end{bmatrix} = \begin{bmatrix} 5 \\ 19 \end{bmatrix} \bmod 26 \tag{4.2}$$

as well because of the following equation:

$$D\begin{bmatrix} M \\ T \end{bmatrix} = \begin{bmatrix} H \\ E \end{bmatrix} \rightarrow D\begin{bmatrix} 12 \\ 19 \end{bmatrix} = \begin{bmatrix} 7 \\ 4 \end{bmatrix} \bmod 26 \tag{4.3}$$

and calculate the D matrix, which is the key for decryption. The above Equations (4.2, 4.3) are combined into one single equation as:

$$D\begin{bmatrix} 15 & 12 \\ 2 & 19 \end{bmatrix} = \begin{bmatrix} 5 & 7 \\ 19 & 4 \end{bmatrix} \bmod 26.$$

Rearrange the equations now to find the numbers that we want to calculate:

$$D = \begin{bmatrix} 5 & 7 \\ 19 & 4 \end{bmatrix} \begin{bmatrix} 15 & 12 \\ 2 & 19 \end{bmatrix}^{-1} \tag{4.4}$$

K^{-1} be the inverse of the matrix K and d is the determinant of the matrix K. such that

$$K \times K^{-1} = I \bmod 26,$$

where the identity matrix is I. The below equation tells us how to discover K^{-1} by using K:

$$K^{-1} = d^{-1} \times adj(K),$$

where $d \times d^{-1} = I \bmod 26$, and adj (K) is a K matrix adjugate. The determinant of the matrix we are calculated as

$$ac - bd \bmod 26 = 15 * 19 - 12 * 2 = 261 = 1 \bmod 26.$$

In addition, the inverse of the determinant 1 must also be found. The matrix adjugate is calculated as follows:

$$\operatorname{adj}\left(\begin{bmatrix} 15 & 12 \\ 2 & 19 \end{bmatrix}\right) = \begin{bmatrix} 19 & -12 \\ -2 & 15 \end{bmatrix}.$$

Compute the inverse:

$$K^{-1} = 1^{-1} \times \left(\begin{bmatrix} 15 & 12 \\ 2 & 19 \end{bmatrix}\right) = 1 \times \begin{bmatrix} 19 & -12 \\ -2 & 15 \end{bmatrix} = \begin{bmatrix} 19 & 14 \\ 24 & 15 \end{bmatrix},$$

now go back to Equation (4.4) in order to determine D.

$$D = \begin{bmatrix} 5 & 7 \\ 19 & 4 \end{bmatrix} \begin{bmatrix} 15 & 12 \\ 2 & 19 \end{bmatrix}^{-1} = \begin{bmatrix} 5 & 7 \\ 19 & 4 \end{bmatrix} \begin{bmatrix} 19 & 14 \\ 24 & 15 \end{bmatrix} = \begin{bmatrix} 263 & 175 \\ 457 & 326 \end{bmatrix}$$
$$= \begin{bmatrix} 3 & 19 \\ 15 & 14 \end{bmatrix} \bmod 26.$$

This is our decryption key. But, if we try to decrypt the sentence, we should have:

“FRFTHEZYSSQYVFETLVBAFVACONFZ”,

that is not the required answer. This means that one of our first assumptions was incorrect in all our original assumptions, the idea used that at the second position our crib ‘OF THE’ started. Drag ‘OF THE’ through each place until we get English at the output to determine the specific task, we want to perform. If we use an 18 offset, combining $KT \to FT$ and $ZK \to HE$ and continue the above process by obtaining the matrix:

$$\begin{bmatrix} 17 & 5 \\ 18 & 23 \end{bmatrix},$$

attempt to decipher our ciphertext:

“DEFENDTHEEASTWALLOFTHECASTLE”,

which is finally the required answer. The method we used here is called 'crib dragging', if simulate it manually then it could be tiresome. Putting a computer program in writing is much easier to attempt. But it is quiet handsome task for a computing machine.

Decryption of Hill cipher requires the inverse of the matrix, but there is an issue with decryption, that is not always the inverse of the matrix exist. [21]. If the matrix is not invertable, then it is not possible to decrypt the encrypted text. To handel with this problem, the author of [25], proposed the use of self invertible matrices. In the self-invertible matrix generation technique, the matrix used for encryption is self-invertible matrix. So, at the time of decryption, we do not need to find the inverse matrix. Moreover, this approach eliminates the computational complexity involved in finding the inverse of the matrix when performed the decryption.

4.2 Self-Invertible Matrix

If a matrix is equal to the inverse of itself then it is known as the self-invertible matrix. The analyses provided for the self-invertible matrix generation are valid for the positive integer matrix, these matrices are formed by the residues of the prime number of the modulo arithmetic.

$$\text{Let } A = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nm} \end{bmatrix},$$

be an $m \times m$ self-invertible matrix divided into the blocks A_{11}, A_{12}, A_{21}, and A_{22} as follows.

$$A = \begin{bmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{bmatrix}$$

A_{11} is a matrix of 1×1 order $= \begin{bmatrix} a_{11} \end{bmatrix}$,

A_{12} is a matrix of $1 \times (m-1)$ order $= \begin{bmatrix} a_{12} & a_{13} & a_{1n} \end{bmatrix}$,

A_{21} is a matrix of $(m-1) \times 1$ order $= \begin{bmatrix} a_{21} \\ a_{31} \\ \ldots \\ a_{n1} \end{bmatrix}$ and,

A_{22} is a matrix of $(m-1) \times (m-1)$ order $= \begin{bmatrix} a_{22} & a_{23} & \ldots & a_{2n} \\ a_{32} & a_{33} & \ldots & a_{3n} \\ \ldots & \ldots & \ldots & \ldots \\ a_{n2} & a_{n3} & \ldots & a_{nm} \end{bmatrix}$,

for A be self-invertible, we must have

$$A_{12}A_{21} = I - A_{11}^2 = \begin{bmatrix} 1 - a^{2_{11}} \end{bmatrix}. \tag{4.5}$$

And

$$A_{12}(a_{11}I + A_{22}) = \mathbf{0}. \tag{4.6}$$

Also,

$$a_{11} = \text{- (one of the eigenvalues of } B_{22} \text{ other than 1).}$$

Since $A_{21}A_{12}$ is a singular matrix of rank 1,

$$A_{21}A_{12} = I - A_{22}^2, \tag{4.7}$$

therefore, A_{22}^2 must have a rank $(m-2)$ with eigenvalue $+1$ of multiplicity $(m-2)$.

Therefore, A_{22} must have eigenvalues ±1.

In order to find any self-invertible matrix A we have to start with a random $(m-1) \times (m-1)$ matrix A_{22} having eigenvalue of either $+1$ or -1 or both and then obtain other matrices A_{21} and A_{12} by solving (4.7) and (4.5) term by term. Thus we have the following algorithm for generation a self-invertible matrix.

Algorithm 4.2.1

Input: A matrix 'A_{22}' of an order $(m-1) \times (m-1)$.

Output: Self-invertible matrix 'A' of an order $m \times m$.

Step 1. Select A_{22}, a non-singular $(m-1) \times (m-1)$ matrix with (m − 2) eigenvalues of either +1 or −1 or both.

Step 2. Calculate the rest of the eigenvalues; λ of A_{22}.

Step 3. Put $a_{11} \in A$

$$a_{11} = -\ \lambda.$$

Step 4. Use the Equation (4.7) to get a consistent solution for A_{12} and A_{21} components.

Step 5. Construct the matrix A. Which is required self-invertible matrix of an order $m \times m$.

Generation of self-invertible matrix is illustrates by the following two examples with $m = 2$ and $m = 3$.

Example 4.2.1. (Generation of Self-Invertible Matrix)

Let $A_{22} = \begin{bmatrix} 2 & 5 \\ 1 & 6 \end{bmatrix}$ which has eigenvalues $\lambda = \pm 1, 7$.

So, $A_{11} = -\ 7 = \begin{bmatrix} 6 \end{bmatrix}$ mod 13.

From Equation (4.7), we have

$$A_{21}A_{12} = \mathrm{I} - A_{22}^2$$

$$A_{21}A_{12} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} - \begin{bmatrix} 2 & 5 \\ 1 & 6 \end{bmatrix}^2$$

$$A_{21}A_{12} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} - \begin{bmatrix} 9 & 40 \\ 8 & 41 \end{bmatrix}$$

$$A_{21}A_{12} = \begin{bmatrix} -8 & -40 \\ -8 & -40 \end{bmatrix}$$

$$\begin{bmatrix} a_{21}a_{12} & a_{21}a_{13} \\ a_{31}a_{12} & a_{31}a_{13} \end{bmatrix} = \begin{bmatrix} 5 & 12 \\ 5 & 12 \end{bmatrix} \text{ mod } 13,$$

then $a_{21}a_{12} = 5$. So, $a_{21} = 5$, $a_{12} = 1$.

$a_{21}a_{13} = 12$. $a_{13} = (5^{-1})(12) = (5)(12) = 5$ mod 13.

$a_{31}a_{12} = 5$. $a_{31} = (1^{-1})(5) = (1)(5) = 5$ mod 13.

Consistent solution is $A_{12} = \begin{bmatrix} 1 & 5 \end{bmatrix}$, and $A_{21} = \begin{bmatrix} 5 \\ 5 \end{bmatrix}$.

Hence required self-invertible matrix is

$$A = \begin{bmatrix} 6 & 1 & 5 \\ 5 & 2 & 5 \\ 5 & 1 & 6 \end{bmatrix}.$$

Example 4.2.2. Let $A_{22} = \begin{bmatrix} 9 & 6 & 10 \\ 12 & 10 & 2 \\ 5 & 3 & 4 \end{bmatrix}$ which has eigenvalues $\lambda = \pm 1, 10$.

So, $A_{11} = -\ 10 = \begin{bmatrix} 3 \end{bmatrix}$ mod 13.

From Equation (4.7), we have

$$A_{21}A_{12} = \text{I} - A_{22}^2 \; A_{21}A_{12} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} - \begin{bmatrix} 9 & 6 & 10 \\ 12 & 10 & 2 \\ 5 & 3 & 4 \end{bmatrix}^2$$

$$A_{21}A_{12} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} - \begin{bmatrix} 203 & 144 & 142 \\ 238 & 178 & 148 \\ 101 & 72 & 72 \end{bmatrix}$$

$$A_{21}A_{12} = \begin{bmatrix} -202 & -144 & -142 \\ -238 & -177 & -148 \\ -101 & -72 & -71 \end{bmatrix}$$

$$\begin{bmatrix} a_{21}a_{12} & a_{21}a_{13} & a_{21}a_{14} \\ a_{31}a_{12} & a_{31}a_{13} & a_{31}a_{14} \\ a_{41}a_{12} & a_{41}a_{13} & a_{41}a_{14} \end{bmatrix} = \begin{bmatrix} 6 & 12 & 1 \\ 9 & 5 & 8 \\ 3 & 6 & 7 \end{bmatrix} \text{ mod } 13,$$

then $a_{21}a_{12} = 6$. So, $a_{21} = 6$, $a_{12} = 1$.

$a_{21}a_{13} = 12$. $a_{13} = (6^{-1})(12) = (11)(12) = 2 \text{ mod } 13$.

$a_{21}a_{14} = 1$. $a_{13} = (6^{-1})(1) = 11 \text{ mod } 13$.

$a_{31}a_{12} = 9$. $a_{31} = (1^{-1})(9) = (1)(9) = 9 \text{ mod } 13$.

$a_{41}a_{12} = 3$. $a_{41} = (1^{-1})(3) = (1)(3) = 3 \text{ mod } 13$.

One of the consistent solution is $A_{12} = \begin{bmatrix} 1 & 2 & 11 \end{bmatrix}$, and $A_{21} = \begin{bmatrix} 6 \\ 9 \\ 3 \end{bmatrix}$.

Hence required self-invertible matrix is

$$A = \begin{bmatrix} 3 & 1 & 2 & 11 \\ 6 & 9 & 6 & 10 \\ 9 & 12 & 10 & 2 \\ 3 & 5 & 3 & 4 \end{bmatrix}.$$

Another consistent solution is $A_{12} = \begin{bmatrix} 11 & 9 & 4 \end{bmatrix}$, and $A_{21} = \begin{bmatrix} 10 \\ 2 \\ 5 \end{bmatrix}$. So,

$$A = \begin{bmatrix} 3 & 11 & 9 & 4 \\ 10 & 9 & 6 & 10 \\ 2 & 12 & 10 & 2 \\ 5 & 5 & 3 & 4 \end{bmatrix}.$$

4.3 Cryptanalysis

Cryptanalysis is the strategy of breaking codes and algorithms. If we try to break a Hill cipher, it becomes hard to guess this using frequency analysis, especially when we use a large key size. Frequency analysis can be effective if applied in bigraph for very lengthy ciphertexts (for a cipher of 2 by 2), but for encryption using bigraph of small ciphertexts, it would becomes infeasible.

The first thing to note is that each key matrix row encodes to one letter independently of the rest of the key matrix when encoding in Hill cipher.

$$\begin{bmatrix} K_{11} & K_{12} & K_{13} \\ K_{21} & K_{22} & K_{23} \\ K_{31} & K_{32} & K_{33} \end{bmatrix} \begin{bmatrix} a \\ b \\ c \end{bmatrix} = \begin{bmatrix} aK_{11} & bK_{12} & cK_{13} \\ aK_{21} & bK_{22} & cK_{23} \\ aK_{31} & bK_{32} & cK_{33} \end{bmatrix} \bmod 26,$$

while taking multiplication the highest row of the left matrix is simply concerned within the highest cell of the ciphertext matrix, the middle cell is simply concerned with the bottom row, etc. We can use this fact to reduce number of keys significantly we can also verify for authorized Hill cipher interruption.

Example 4.3.1. Hill cipher is vulnerable to a known-plaintext attack, because it is linear (if you know the plaintext and the corresponding ciphertext, the key can be recovered). An adversary who intercepts multiple pairs of plaintext/ciphertext characters sets up a linear system of equations that can be solved easily. If this system is inconsistent, then just a few more pairs of plaintext/ciphertext must be added. Let $K = \begin{bmatrix} K_{11} & K_{12} & K_{13} & K_{14} \\ K_{21} & K_{22} & K_{23} & K_{24} \\ K_{31} & K_{32} & K_{33} & K_{34} \\ K_{41} & K_{42} & K_{43} & K_{44} \end{bmatrix}$ be the self-invertible key that uses in [25].

Suppose that ciphertext starts with "**dcckid mcjc iffegi**" which is the same as "**lester Hill cipher**" to determine the key matrix. Since **lest→dcck, erhi→idmc, llci→jcif and pher→fegi**

$$\begin{bmatrix} K_{11} & K_{12} & K_{13} & K_{14} \\ K_{21} & K_{22} & K_{23} & K_{24} \\ K_{31} & K_{32} & K_{33} & K_{34} \\ K_{41} & K_{42} & K_{43} & K_{44} \end{bmatrix} \begin{bmatrix} 11 \\ 4 \\ 5 \\ 6 \end{bmatrix} = \begin{bmatrix} 3 \\ 2 \\ 2 \\ 10 \end{bmatrix} \text{ mod } 13$$

$$\begin{bmatrix} K_{11} & K_{12} & K_{13} & K_{14} \\ K_{21} & K_{22} & K_{23} & K_{24} \\ K_{31} & K_{32} & K_{33} & K_{34} \\ K_{41} & K_{42} & K_{43} & K_{44} \end{bmatrix} \begin{bmatrix} 4 \\ 4 \\ 7 \\ 8 \end{bmatrix} = \begin{bmatrix} 8 \\ 3 \\ 12 \\ 2 \end{bmatrix} \text{ mod } 13$$

$$\begin{bmatrix} K_{11} & K_{12} & K_{13} & K_{14} \\ K_{21} & K_{22} & K_{23} & K_{24} \\ K_{31} & K_{32} & K_{33} & K_{34} \\ K_{41} & K_{42} & K_{43} & K_{44} \end{bmatrix} \begin{bmatrix} 11 \\ 11 \\ 2 \\ 8 \end{bmatrix} = \begin{bmatrix} 9 \\ 2 \\ 8 \\ 5 \end{bmatrix} \text{ mod } 13$$

$$\begin{bmatrix} K_{11} & K_{12} & K_{13} & K_{14} \\ K_{21} & K_{22} & K_{23} & K_{24} \\ K_{31} & K_{32} & K_{33} & K_{34} \\ K_{41} & K_{42} & K_{43} & K_{44} \end{bmatrix} \begin{bmatrix} 2 \\ 7 \\ 4 \\ 4 \end{bmatrix} = \begin{bmatrix} 5 \\ 4 \\ 6 \\ 8 \end{bmatrix} \text{ mod } 13.$$

Now to solve for K, we convert the matrices into the systems of linear equations as follows:

$$11K_{11} + 4K_{12} + 5K_{13} + 6K_{14} = 3 \quad \text{mod } 13 \tag{4.8}$$

$$11K_{21} + 4K_{22} + 5K_{23} + 6K_{24} = 2 \quad \text{mod } 13 \tag{4.9}$$

$$11K_{31} + 4K_{32} + 5K_{33} + 6K_{34} = 2 \quad \text{mod } 13 \tag{4.10}$$

$$11K_{41} + 4K_{42} + 5K_{43} + 6K_{44} = 10 \quad \text{mod } 13 \tag{4.11}$$

$$4K_{11} + 4K_{12} + 7K_{13} + 8K_{14} = 8 \quad \text{mod } 13 \tag{4.12}$$

$$4K_{21} + 4K_{22} + 7K_{23} + 8K_{24} = 3 \mod 13 \tag{4.13}$$

$$4K_{31} + 4K_{32} + 7K_{33} + 8K_{34} = 12 \mod 13 \tag{4.14}$$

$$4K_{41} + 4K_{42} + 7K_{43} + 8K_{44} = 2 \mod 13 \tag{4.15}$$

$$11K_{11} + 11K_{12} + 2K_{13} + 8K_{14} = 9 \mod 13 \tag{4.16}$$

$$11K_{21} + 11K_{22} + 2K_{23} + 8K_{24} = 2 \mod 13 \tag{4.17}$$

$$11K_{31} + 11K_{32} + 2K_{33} + 8K_{34} = 8 \mod 13 \tag{4.18}$$

$$11K_{41} + 11K_{42} + 2K_{43} + 8K_{44} = 5 \mod 13 \tag{4.19}$$

$$2K_{11} + 7K_{12} + 4K_{13} + 4K_{14} = 5 \mod 13 \tag{4.20}$$

$$2K_{21} + 7K_{22} + 4K_{23} + 4K_{24} = 4 \mod 13 \tag{4.21}$$

$$2K_{31} + 7K_{32} + 4K_{33} + 4K_{34} = 6 \mod 13 \tag{4.22}$$

$$2K_{41} + 7K_{42} + 4K_{43} + 4K_{44} = 8 \mod 13. \tag{4.23}$$

There are twelve unknowns and twelve linear equations. Solving (4.8) and (4.16), we have

$$\begin{array}{c} 11K_{11} + 4K_{12} + 5K_{13} + 6K_{14} = 3 \mod 13 \\ -11K_{11} \pm 11K_{12} \pm 2K_{13} \pm 8K_{14} = \pm 9 \mod 13 \\ \hline -7K_{12} - 3K_{13} + 2K_{14} = 6 \mod 13. \end{array} \tag{4.24}$$

Solving (4.12) and (4.20), we have

$$\begin{array}{c} 4K_{11} + 4K_{12} + 7K_{13} + 8K_{14} = 8 \mod 13 \\ -4K_{11} \pm 14K_{12} \pm 8K_{13} \pm 8K_{14} = \pm 10 \mod 13 \\ \hline -10K_{12} - K_{13} = -2 \mod 13. \end{array} \tag{4.25}$$

Solving (4.8) and (4.12), we have

$$\begin{array}{c} 44K_{11} + 16K_{12} + 20K_{13} + 24K_{14} = 12 \mod 13 \\ \\ -44K_{11} \pm 44K_{12} \pm 77K_{13} \pm 88K_{14} = \pm 88 \mod 13 \\ \hline -28K_{12} - 57K_{13} - 64K_{14} = -76 \mod 13 \end{array}$$

$$2K_{12} + 5K_{13} + 12K_{14} = 11 \mod 13. \tag{4.26}$$

Again solving (4.16) and (4.20), we get

$$\begin{array}{c} 22K_{11} + 22K_{12} + 4K_{13} + 16K_{14} = 18 \mod 13 \\ \\ -22K_{11} \pm 77K_{12} \pm 44K_{13} \pm 44K_{14} = \pm 55 \mod 13 \\ \hline -55K_{12} - 40K_{13} - 28K_{14} = -37 \mod 13 \end{array}$$

$$3K_{12} + K_{13} + 5K_{14} = 11 \mod 13. \tag{4.27}$$

Solving (4.24) and (4.26), we get

$$\begin{array}{c} 42K_{12} - 18K_{13} + 12K_{14} = 36 \mod 13 \\ \\ \pm 2K_{12} \pm 5K_{13} \pm 12K_{14} = \pm 11 \mod 13 \\ \hline 40K_{12} - 23K_{13} = 25 \mod 13 \end{array}$$

$$K_{12} + 3K_{13} = 12 \mod 13. \tag{4.28}$$

Solving (4.25) and (4.27), we get

$$\begin{array}{c} 10K_{12} + K_{13} = 2 \mod 13 \\ \\ \pm 10K_{12} \pm 30K_{13} = \pm 120 \mod 13 \\ \hline 29K_{13} = 118 \mod 13 \end{array}$$

$$K_{13} = (3^{-1})(1) = 9 \mod 13.$$

Substituting in (4.28) to get

$$K_{12} + 3(9) = 12 \mod 13$$

$$K_{12} = 12 - 27 = -15 = 11 \mod 13.$$

Substituting the value of K_{13} and K_{12} in (4.27) to get

$$3(11) + 9 + 5K_{14} = 11 \mod 13$$

$$5K_{14} = 11 - 42 = -31 = 8 \mod 13$$

$$5K_{14} = (5^{-1})(8) = (8)(8) = 4 \mod 13.$$

Substituting the value of K_{13}, K_{12} and K_{14} in (4.8) to get

$$11K_{11} + 4(11) + 5(9) + 6(4) = 3 \mod 13$$

$$11K_{11} = 3 - 113 = -110 = 7 \mod 13$$

$$K_{11} = (11^{-1})(7) = (6)(7) = 42 = 3 \mod 13.$$

Hence the required solution of unknows are $K_{11} = 3$, $K_{12} = 11$, $K_{13} = 9$ and $K_{14} = 4$. Similarly solve the rest of the equations to get the self-invertible key

$$K = \begin{bmatrix} K_{11} & K_{12} & K_{13} & K_{14} \\ K_{21} & K_{22} & K_{23} & K_{24} \\ K_{31} & K_{32} & K_{33} & K_{34} \\ K_{41} & K_{42} & K_{43} & K_{44} \end{bmatrix} = \begin{bmatrix} 3 & 11 & 9 & 4 \\ 10 & 9 & 6 & 10 \\ 2 & 12 & 10 & 2 \\ 5 & 5 & 3 & 4 \end{bmatrix}.$$

Which is the required self-invertible key used for encryption and decryption. Hence we successfully found the key used for the encryption and decryption scheme proposed by Kumar et al. [25] using the known-plaintext attack. Results of the simulation show that the original plaintext can be revealed successfully. Now the attacker can encrypt any other document or message with Alice's private key. The receiver will not be able to judge that the message is not encrypted by Alice.

Chapter 5

Conclusion

In this thesis, we review two articles "Digital Signature Scheme based on block cipher" proposed by Kuppuswamy et al. [24] and "Encryption Scheme based on Self-Invertible Hill Cipher" presented by Kumar et al. [25]. Both schemes are based on matrices over the integer $\mathbb{Z}_n$. The proposed method of digital signature scheme based on the linear block cipher or Hill cipher. Originally the Hill cipher [45] is a symmetric key scheme but the present signature scheme [24] it is used as an asymmetric key scheme. Underlying hard problem of this scheme is to compute ℓ and K and the private key D if $E = \ell^{-1} * K^{-1}$ is given. An adversary that intercepts multiple pairs of plaintext/ciphertext characters sets up a linear system of equations that can be easily solved to give unique values of required unknowns. If this system turns out to be inconsistent, then we include a few more plaintext/ciphertext pairs to get the private key. We have taken the cryptanalysis of digital signature scheme presented in [24] by finding the private key. Hence we successfully found the key used for the digital signature scheme proposed by Kuppuswamy et al. [24] using the known-plaintext attack. Results of the simulation show that the original digital signature can be revealed successfully. Now the attacker can sign any other document or message with the sender (Alice) private key. The receiver will not be able to judge that the message is not signed by Alice. The encryption scheme based on self-invertible Hill cipher [25] is also based on the linear block ciphers. An effective methods for the Hill cipher algorithm to produce a self-invertible matrix is proposed by Kumar et al. This proposed method of self-invertible matrix generation can also be used in other algorithms where the inversion of the matrix is necessary. We observed that the use of self-invertible matrices can just make the decryption process efficient as the receiver does not have to compute the inverse the key matrix over $\mathbb{Z}_n$. This has nothing to do with the security flaws in the original Hill cipher algorithm. We found that Hill cipher based on self-invertible matrices is also vulnerable to a known-plaintext attack, because it becomes linear system of equations (if you know the plaintext and the corresponding ciphertext, the key can be recovered). If this system is inconsistent, then a few more plaintext/ciphertext pairs need to be added to get the private key. Results of the cryptanalysis show that the secret key use in the Hill cipher scheme can be revealed successfully. The attacker can now decrypt any other document or message that was encrypted with this secret key.

Bibliography

[1] M. M. E. R. M. Abobeah and H. M. Harb, "Public-key cryptography techniques evaluation," *International Journal of Computer Networks and Applications*, vol. 2, no. 2, pp. 1–12, 2015.

[2] J.-S. Coron, "What is cryptography?" *IEEE security and privacy*, vol. 4, no. 1, pp. 70–73, 2006.

[3] W. Stallings, "Cryptography and network security," *4/E. Pearson Education India, 2006*, vol. 4, pp. 1–457, 2006.

[4] Y. Desmedt and J.-J. Quisquater, "Public-key systems based on the difficulty of tampering (Is there a difference between DES and RSA?)," *Advances in Cryptology CRYPTO 86*, vol. 263, no. 3, pp. 111–117, 1987.

[5] J. Daemen and V. Rijmen, "The design of rijndael: AES-the advanced encryption standard," *Springer Science and Business Media*, vol. 1, no. 2, pp. 23–54, 2013.

[6] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE transactions on Information Theory*, vol. 22, no. 6, pp. 644–654, 1976.

[7] R. Singh and S. Kumar, "Elgamals algorithm in cryptography," *International Journal of Scientific and Engineering Research*, vol. 3, no. 12, pp. 1–4, 2012.

[8] T. K. S. M. M. Rahman and M. A.-A. Bhuiyan, "Implementation of rsa algorithm for speech data encryption and decryption," *International Journal of Computer Science and Network Security (IJCSNS)*, vol. 12, no. 3, pp. 1–74, 2012.

[9] A. J. M. D. Hankerson and S. Vanstone, "Guide to elliptic curve cryptography," *Springer Science and Business Media*, vol. 1, no. 1, pp. 1–149, 2006.

[10] C. W.C.Cheng and L.Golubchik, "Performance of batch-based digital signatures," *10th IEEE International Symposium on Modeling*, 2002.

[11] S. M. S. Goldwasser and R. L. Rivest, "A digital signature scheme secure against adaptive chosen-message attacks," *SIAM Journal on Computing*, vol. 17, no. 2, pp. 281–308, 1998.

[12] O. Goldreich, "Two remarks concerning the goldwasser-micali-rivest signature scheme," *Conference on the Theory and Application of Cryptographic Techniques*, vol. 263, no. 1, pp. 104–110, 1996.

[13] S. H. R. Gennaro and T. Rabin, "Secure hash-and-sign signatures with- out the random oracle," *International Conference on the Theory and Ap- plications of Cryptographic Techniques*, vol. 1592, no. 1, pp. 123–139, 1999.

[14] R. Cramer and V. Shoup, "Signature schemes based on the strong rsa assumption," *ACM Transactions on Information and System Security (TISSEC)*, vol. 3, no. 3, pp. 161–185, 2000.

[15] N. S. P. Kitsos and O. Koufopavlou, "Electronics, circuits and systems," *An efficient implementation of the digital signature algorithm*, vol. 1462, no. 8, pp. 327–337, 2002.

[16] O. G. S. Even and S. Micali, "On-line/off-line digital signatures," *Proceedings of CRYPTO*, 1990.

[17] P. O. A. J. Menezes and S. A. Vanstone, "Handbook of applied cryptography," *CRC Press*, vol. 4, no. 3, pp. 1–176, 1996.

[18] A. Buldas and M. Saarepera, "Electronic signature system with small number of private keys," *presented at 2nd Annual PKI Research Workshop*, vol. 12, no. 7, pp. 96–108, 2003.

[19] Saeednia, "How to make the Hill cipher secure. cryptologia. s., 2000." vol. 24, no. 4, pp. 353–360, 2000.

[20] T. W. W. J. Overbey, J., “On the keyspace of the Hill cipher. cryptologia,” vol. 29, pp. 59–72, 2005.

[21] P. O. A. J. Menezes and S. A. Vanstone, “Handbook of applied cryptography, crc press,” 1996.

[22] Stallings, “W. cryptography and network security.” *4th edition, Prentice Hall.*, 2005.

[23] S. J. O. A. Imai H., Hanaoka G., “Nascimento a.c. 2002. cyptography with information theoretic security. information theory workshop,” *Proceedings of the IEEE*, vol. 5, no. 4-5, pp. 355–380, 2002.

[24] P. K. Perumal, “A new efficent digital signature scheme algorithm based on block chiper,” vol. 7, no. 1, pp. 47–52, 2012.

[25] D. J. Saroj Kumar Panigrahy, Bibhudendra Acharya, “Encryption scheme based on self-invertible Hill cipher,” vol. 1, no. 1, pp. 1–4, 2008.

[26] K. Ruohonen, “Mathematical cryptology,” *Lecture Notes*, vol. 1, no. 1, pp. 1–138, 2010.

[27] K.Jacobs, “A survey of modern mathematical cryptology,” vol. 1, no. 1, pp. 1–13, 2011.

[28] A. J. Menezes, “Handbook of applied cryptography,,” vol. 442, no. 3, pp. 1–794, 1997.

[29] K. A. Sangeeta, “A review on symmetric key cryptography algorithms,” *International Journal of Advanced Research in Computer Science*, vol. 8, no. 4, pp. 358–361, 2017.

[30] N. Koblitz, “Elliptic curve cryptosystems,” *Mathematics of computation*, vol. 48, no. 177, pp. 203–209, 1987.

[31] T. Takagi, “Fast RSA-type cryptosystem modulo p^k q,” vol. 1462, no. 4, pp. 318–326, 1998.

[32] A. D.Hankerson and S.Vanstone, "Guide to elliptic curve cryptography." *Springer Science and Business Media*, vol. 1, no. 3, pp. 1–311, 2006.

[33] D. G. Amalarethinam and J. S. Geetha, "Encryption and decryption in public key cryptography based on MR," vol. 1, no. 4, pp. 133–138, 2015.

[34] M. Matsui, "Linear cryptanalysis method for DES cipher," vol. 765, no. 3, pp. 386–397, 1993.

[35] N. Kumar, "Investigations in brute force attack on cellular security based on DES and AES," *IJCEM Internation Journal of Computational Engineering & Management*, vol. 14, no. 4, pp. 50–52, 2011.

[36] D. S. C.Rackoff, "Non-interactive zero-knowledge proof of knowledge and chosen ciphertext attack," *Annual International Cryptology Conference*, vol. 576, no. 3, pp. 433–444, 1991.

[37] M. Matsui, "Linear cryptanalysis method for des cipher," *Workshop on the Theory and Application of Cryptographic Techniques*, vol. 765, pp. 386–397, 1993.

[38] M. Eisenberg, "Hill ciphers and modular linear algebra," *Mimeographed notes*, vol. 165, no. 9, pp. 1–19, 1999.

[39] R. Lidl and H. Niederreite, "Introduction to finite fields and their applications," vol. 1326, no. 11, pp. 1–416, 1994.

[40] D. A. Wallace, "Groups, rings and fields," *Springer Science and Business Media*, vol. 3423, no. 2, pp. 1–245, 2012.

[41] G. L. Mullen and D. Panario, "Handbook of finite fields," *Chapman and Hall/CRC*, vol. 16, no. 1, pp. 1–1068, 2013.

[42] N. S. P. Kitsos and O. Koufopavlou, "An efficient implementation of the digital signature algorithm, electronics, circuits and systems," vol. 90, no. 6, pp. 969–986, 2002.

[43] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE transactions on information theory*, vol. 31, no. 4, pp. 469–472, 1985.

[44] A. S. R. L. Rivest and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978.

[45] L. S. Hill, "Cryptography in an algebraic alphabet," *The American Mathematical Monthly*, vol. 36, no. 6, pp. 306–312, 1929.