CAPITAL UNIVERSITY OF SCIENCE AND TECHNOLOGY, ISLAMABAD

A Key Recovery Attack on Modified Hill Encryption Scheme

by

Saliha Ameen

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

in the

Faculty of Computing

Department of Mathematics

2023

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

CERTIFICATE OF APPROVAL

A Key Recovery Attack on Modified Hill Encryption Scheme

by

Saliha Ameen

(MMT213034)

THESIS EXAMINING COMMITTEE

S. No.	Examiner	Name	Organization
(a)	External Examiner	Dr. Nasir Siddiqui	UET, Taxila
(b)	Internal Examiner	Dr. Muhammad Afzal	CUST, Islamabad
(c)	Supervisor	Dr. Rashid Ali	CUST, Islamabad

Dr. Rashid Ali
Thesis Supervisor
November, 2023

Dr. Muhammad Sagheer
Head
Dept. of Mathematics
November, 2023

Dr. M. Abdul Qadir
Dean
Faculty of Computing
November, 2023

Author's Declaration

I, **Saliha Ameen** hereby state that my MPhil thesis titled "**A Key Recovery Attack on Modified Hill Encryption Scheme**" 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 MPhil Degree.

Saliha

(Saliha Ameen)

Registration No: MMT213034

Plagiarism Undertaking

I solemnly declare that research work presented in this thesis titled "**A Key Recovery Attack on Modified Hill Encryption Scheme**" is solely my research work with no significant contribution from any other person. Small contribution/help wherever taken has been duly 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 MPhil Degree, the University reserves the right to withdraw/revoke my MPhil 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.

Saliha

(Saliha Ameen)

Registration No: MMT213034

Acknowledgement

I want to thank Allah the most Compassionate and Benevolent, who gave me the strength to keep going through ups and downs and helped me finish my thesis.

I am deeply thankful to **Dr. Rashid Ali**, my supportive supervisor, for his constant inspiration. Whenever I encountered challenges, he was readily available to assist. I truly value his dedication and direction throughout my thesis, and I take pride in being under the guidance of such a compassionate supervisor.

I am thankful to my family specially Grandmother and Phoppu for being patient and supportive during my research. My parents have been a constant source of inspiration in my life. I am forever thankful for their prayers, love, and continuous inspiration throughout my academic career.

Lastly, I am grateful to everyone who has offered prayers for me, shared their knowledge throughout my academic journey, and provided their support.

(Saliha Ameen)

Registration No: MMT213034

Abstract

The Hill Cipher is a cryptographic algorithm based on matrix multiplication and modulo operations to encrypt plaintext into ciphertext. The traditional Hill Cipher uses a square matrix as the encryption key. The square matrix key is randomly generated and shared between the sender and receiver. The modified form of Hill Cipher uses a pseudo invertible rectangular matrix as the shared key for encryption and decryption. The pseduoinverse of this rectangular matrix is used for decryption of the ciphertext. The use of a rectangular key matrix results in a longer and more complex ciphertext compared to a square key matrix. The Playfair Cipher Algorithm is used to generate a rectangular key matrix and this rectangular matrix is used as key in the modified form of Hill Cipher. The Authors claimed that an attack cannot be mounted on their scheme because of the key matrix being rectangular and it is harder to find patterns or apply linear algebraic techniques to break the encryption. The author's claim is wrong. The scheme is successfully cryptanalyzed by mounting a method called Known Plaintext Attack. Using pseudo-invertible rectangular matrices does not protect the Hill Cipher from this attack.

Contents

List of Figures

List of Tables

Symbols

X	Plaintext
Y	Ciphertext
$\mathcal{A}$	Rectangular matrix key
E_k	Encryption key
D_k	Decryption key
K_1	Public key
K_2	Secret key

Chapter 1

Introduction

Mathematics is the mother of all sciences. It is the foundation for everything you can imagine. It is used everywhere, from predicting the weather, in medical, building impressive structures, and managing money matters. Its uses are endless and touch every part of life. Mathematics is like a big tree with many branches, and each branch focuses on a specific part of math. For example Arithmetic, Algebra, Geometry, Trigonometry, Calculus, and Cryptography etc.

Cryptography is one field where mathematics is extremely important. The ancient roots of cryptography date back to approximately 1900 BC, where it was employed in different structure and methods within the Egyptian civilization [1]. Egyptian scribes used hieroglyphic symbols, which were intricate picture symbols representing sounds, objects, actions, or ideas, to hide confidental messages from those who lacked understand the writing system. These hieroglyphic symbols served as a means of securing government and military information and were the most renowned Egyptian scripts used for this purpose.

Later, during the time of the Roman Empire, the famous Caesar cipher was introduced by Julius Caesar. This cipher involved shifting each letter in the plaintext a certain number of positions down the alphabet, and it was used to communicate securely with Caesar's military commanders. As time went on, the practice of cryptography evolved, leading to the development of many other cryptographic ciphers and techniques for transmitting codes and secret messages securely.

Sending communications in a way that only the intended recipients can comprehend is known as cryptography. It involves using mathematical functions to protect data from unauthorized access. Before being sent out over an open network, the starting point of communication, called as plaintext. The plaintext is changed into a message with a code (ciphertext) using an encryption technique. The recipient or another authorized individual then uses a decryption approach which turns the encrypted data into its original plaintext. A hidden item of information, called a key, can be obtained by the sender and the recipient and is used for encryption and decryption. Everything that happens is referred to as a cryptosystem, and the private nature of the key defines how secure the system is. In wireless networking and private communication, there has been significant demand for secure channels for a long time. As communication technology develops, there is an increasing demand for reliable encryption systems that can offer genuine and trustworthy security. For instance, the mono-alphabetical cipher [2], the four-square cipher [2], Playfair cipher [3] the Hill ciphers [4], etc. As time has passed, countermeasures have been introduced against these cryptosystems, and various attacks have been developed to compromise their security. The purpose of cryptography extends beyond encryption and decryption; it is to ensure the safety and protection of data and information. Cryptography provides data with confidentiality, authenticity, availability, and integrity, ensuring its secure handling and usage [5]. The number of people a cryptosystem includes as members affects the integrity of symmetric or private key encryption systems. The encryption and decryption processes in such methods apply the same shared secret key. When only a few interacting parties are involved, maintaining these shared keys becomes manageable. But when the number of conversations between parties increases, it gets harder to manage the shared key.

An identical key can be used for both data encryption and decryption for symmetric or private key cryptography. This key must be exchanged between the two parties before for encryption and decryption to take place. Public key cryptography, a ground-breaking idea in cryptography, was developed by Diffie and Hellman in 1976. Two keys a private key and a public key are used in this idea.

The drawbacks and weaknesses of symmetric key encryption were solved by public key cryptography. As time passed, several cryptographic algorithms came into being, including the Hill cipher. To produce a ciphertext that is challenging to cryptanalysts to crack variants of Known Plaintext Attack,Choosen Plaintext Attack and Choosen Ciphertext Attack etc.

The Hill cipher cryptographic algorithm involves matrix operations and modulo arithmetic. Many data systems that use the Hill cipher algorithm include matrix keys, and a number of ways are used to compute the key matrix, increasing the security of those systems. Alawiyah recommended an update to the encryption procedure in 2017 by adding a binary tree visit operation at the start. A rectangular matrix key was additionally used.

Due to the difficulties in locating the linear equation within the new ciphertext, cryptanalysts have had a tough time unlocking it [6]. Another research proposal combines the Elliptic Curve Cryptosystem with the Hill Cipher (ECCHC) to develop an image encryption technique [7]. Furthermore, there are studies focusing on utilizing a shared matrix as a secret key, where a non-singular matrix G is employed as a public key [8]. The importance to establish key privacy in cryptography can be seen by Kerckhoffs's principle.

This rule states that the encryption technique should not rely on the algorithm's confidentiality. The encryption technique should be created in such a way that it can be openly shared and even come into the hands of the enemy without causing trouble or harming the system's security [9]. Mahendra's research applies the Playfair cipher to figure out the key matrix. The fact that the resulting matrix is square, however, is what characterises it and makes it unique.

This feature is important because it gives the Hill Cipher method a key matrix, which strongly speeds up the encryption and decryption procedures [10].

Current Research

In this thesis, the article "Generation of Rectangular Matrix Key for Hill Cipher Algorithm Using Playfair Cipher" authored by Alawiyah et al [11] is reviewed.

They claimed that used rectangualr matix for key because it can be hard for cryptanalysts to discover their linear equations as the ciphertext generated is longer than the plaintext. The work is based on the following task:

1. The scheme is successfully cryptanalyzed by mounting a method called Known Plaintext attack. Using pseudo-invertible rectangular matrices does not protect the changed Hill Cipher from this attack.

2. Computational example of Known Plaintext Attack on the encryption scheme. This kind of attack succeeded in using the shared secret key in encryption and decryption.

3. Drawback of "Generation of Rectangular Matrix Key for Hill Cipher Algorithm Using Playfair Cipher" authored by Alawiyah et al [11]

Thesis Layout

The other sections of the thesis are as follows:

1. In Chapter 2, the essential concepts and definitions in cryptography that are needed to understand the development of a cryptosystem are covered. This section also explains key terms and give examples that are relevant to the thesis. Additionally, a short review of basic algebra concepts that will be used throughout this thesis is also presented.

2. In Chapter 3, we brefily explain "Generation of Rectangular Matrix Key for Hill Cipher Algorithm Using Playfair Cipher" [11].

3. In Chapter 4, we showed that the Key recover attack attack on the encryption scheme of "Generation of Rectangular Matrix Key for Hill Cipher Algorithm Using Playfair Cipher" [11]. Additionally, we have explained the scheme's concepts using examples.

4. In Chapter 5, we presented conclusion and future work suggestion.

Chapter 2

Preliminaries

The basics concept of cryptography will explain in this chapter and how it is used in various applications. It will also define important terms and provide examples that are relevant to the thesis. Additionally, it will refresh your memory on fundamental algebraic concepts that will be used throughout this thesis.

2.1 Mathematical Background

Here are some important concepts from mathematics that will be used in the thesis.

2.1.1 Modular Arithmetic

The concept of modular arithmetic, that involves working with integers and performing arithmetic operations on them in a way that wraps around at a certain value, called the modulus. In other words, modular arithmetic involves finding the remainder when one integer is divided by another integer. It is represented using the symbol “mod” and must be greater than zero. In modular arithmetic, two numbers are considered congruent if they have the same remainder when divided by the modulus. Let u and v are two integers. When we say "u is congruent to v modulo $\mathtt{m}$", we write it as:

$$u \equiv v \mod \mathtt{m} \tag{2.1}$$

Modular arithmetic is used in various fields[12] including cryptography, because it helps in handling large numbers efficiently and ensures that results stay within a fixed range. In cryptography, this property is crucial for secure encryption and decryption of data to establish a crytosystem based on the term of numbers.

2.1.2 Eucledian Algorithm

Euclidean algorithm [13] is a technique for finding the greatest common divisor (gcd) of two numbers. One of the ancient algorithms that remain in use today, they are named after the Greek mathematician Euclid. The gcd of u and v is the largest positive integer that divides given numbers with no left a remainder r. According to the Euclidean Algorithm

$$\gcd(u, v) = \gcd(v, \mathsf{r}), \text{ where } \mathsf{r} \text{ is the remainder when u is divided by v.}$$

The GCD helps simplify fractions to their lowest terms. This algorithm is widely employed in cryptography and number theory. Moreover, the Euclidean algorithm can also be applied to perform division in modular arithmetic.

Algorithm 2.1.1.

```
1. $A = u$; $B = v$
2. if $B = 0$ return $A = \gcd(u, v)$
3. $R = A \mod B$
4. $A = B$
5. $B = R$
6. goto Step 2
```

The Extended Euclidean Algorithm is an advanced version of the Euclidean algorithm, designed to efficiently find the gcd of both integers u and v, while simultaneously determining the coefficients m and n for Bezout's identity, satisfying the equation:

$$um + vn = \gcd(u, v)$$

In essence, this algorithm not only calculates the gcd of u and v but also reveals the integers m and n that can be used to express the gcd as a linear combination of u and v. It is a powerful tool used in various mathematical applications, including number theory, modular arithmetic, and cryptography.

Algorithm 2.1.2. Extended Inverse Algorithm

Input: An integer $\mathtt{t}$ and modulo $\mathtt{m}$.

Output: $\mathtt{t}^{-1} \mod \mathtt{m}$

```
1. Set up the integers $P_i$ and $Q_i$ for $i$=1,2,3,4,5,6
   $(P_1, P_2, P_3) = (1, 0, \mathtt{m})$
   $(Q_1, Q_2, Q_3) = (0, 1, \mathtt{t})$
2. If $Q_3 = 0$, return $P_3 = \gcd(\mathtt{t}, \mathtt{m})$; no inverse of $\mathtt{t}$ exist in $\mod \mathtt{m}$
3. $Q_3 = 1$, return $Q_3 = \gcd(\mathtt{t}, \mathtt{m})$ and $Q_2 = \mathtt{t}^{-1} \mod \mathtt{m}$
4. Calculate Quotient $q$ and dividing $P_3$ by $Q_3$ .
5. Set $(V_1, V_2, V_3) = (P_1 - qQ_1, P_2 - qQ_2, P_3 - qQ_3)$
6. Set $(P_1, P_2, P_3) = (Q_1, Q_2, Q_3)$
7. Set $(Q_1, Q_2, Q_3) = (V_1, V_2, V_3)$
8. Go to Step 2
```

The following example illustrates the above Extended Euclidean algorithm.

Example 2.1.3.

Compute the $550^{-1} \mod 1759$ by using extended Euclidean Alogorithm?

Solution:

Let $r = 550$ and $m = 1759$. The values of q, P_i and Q_i $(i = 1,2,3)$ after each iteration are given in the table below:

Table 2.1: Extended Euclidean Algorithm

q	P_1	P_2	P_3	Q_1	Q_2	Q_3
-	1	0	1759	0	1	550
3	0	1	550	1	-3	109
5	1	-3	109	-5	16	5
21	-5	16	5	106	-339	4
1	106	-339	4	-111	355	1

The inverse of 550 is 355 under modulo prime 1759.

Definition 2.1.4.

A matrix B of order $a \times b$ is said to be a full rank if and only if

$$rank(B) = \min(a, b)$$

Clearly, if B is a square, that is $a = b$, then it is full rank if and only if

$$rank(B) = a = b$$

- If $\min(a, b) = a$ then B will be full row rank and if $\min(a, b) = b$ then B is called full column rank matrix.

Example 2.1.5. Determine the rank of the following matrix A.

$$A = \begin{bmatrix} 2 & 15 & 20 & 4 & 9 & 1 & 8 \\ 17 & 2 & 15 & 13 & 23 & 2 & 13 \end{bmatrix} \quad \text{mod } 26.$$

Solution:

$$A = \begin{bmatrix} 2 & 15 & 20 & 4 & 9 & 1 & 8 \\ 17 & 2 & 15 & 13 & 23 & 2 & 13 \end{bmatrix} \quad \text{mod } 26.$$

Replace the R_1 and R_2

$$A = \begin{bmatrix} 17 & 2 & 15 & 13 & 23 & 2 & 13 \\ 2 & 15 & 20 & 4 & 9 & 1 & 8 \end{bmatrix} \mod 26.$$

Multiplying the first row R_1 by $17^{-1} \mod 26$, then get

$$A = \begin{bmatrix} 1 & 4 & 7 & 1 & 19 & 4 & 1 \\ 2 & 15 & 20 & 4 & 9 & 1 & 8 \end{bmatrix} \mod 26.$$

Subtracting $2R_1$ from R_2, we get

$$A = \begin{bmatrix} 1 & 4 & 14 & 8 & 18 & 2 & 16 \\ 0 & 7 & 6 & 2 & 23 & 19 & 6 \end{bmatrix} \mod 26.$$

The reduced matrix's rank is 2 is determined by the number of greater than zero rows. As rank of $A = 2 = \min(2, 7)$. Therefore A is full row rank matrix.

2.1.3 Pseudoinverse

The concept of Moore-Penrose inverse introduced by E. H. Moore in 1920 [14] who used it to solve systems of linear equations with more equations than unknowns. However it was not the 1950s that the pseduoinverse was more fully developed by servel researchers inclduing Bjerhammar [15] and Penrose [16]. Pensore's work on the pseduoinverse was particularly influential, and he is often credited with developing the modern theory of the pseduoinverses.

In his 1955 paper " A Generalized Inverse For Matrices", Pnerose introduced the four properties that the pseduoinverse must satisfy, which are known as Moore-Penrose conditions. Pseduoinverse is denoted as $\mathcal{P}^{\dagger}$. It a generalization of the inverse matrix for non- square matrices in linear algebra[17].

Notation

The following rules are used in the discussion that follows:

- $\mathbb{F}_{a\times b}$ represents the collection of all $a \times b$ matrices whose entries come from either the real numbers or the complex numbers, depending on whether $\mathbb{F}$ is $\mathbb{R}$ or $\mathbb{C}$ respectively.
- For $\mathcal{P} \in \mathbb{F}_{a\times b}, \mathcal{P}^\intercal$ is called Transpose and $\mathcal{P}^*$ is known as Hermitian transpose. It is also called the Conjugate transpose.
  If $\mathbb{F} = \mathbb{R}$, then $\mathcal{P}^*$=$\mathcal{P}^\intercal$.

Properties:

1. $\mathcal{P}\mathcal{P}^\dagger\mathcal{P} = \mathcal{P}$
2. $\mathcal{P}^\dagger\mathcal{P}\mathcal{P}^\dagger = \mathcal{P}^\dagger$
3. $(\mathcal{P}\mathcal{P}^\dagger)^{-1} = \mathcal{P}\mathcal{P}^\dagger$
4. $(\mathcal{P}^\dagger\mathcal{P})^{-1} = \mathcal{P}^\dagger\mathcal{P}$

Properties Proofs

The proofs of the following properties are given below:

1. $\mathcal{P}\mathcal{P}^\dagger\mathcal{P} = \mathcal{P}$.

$$\begin{aligned} L.H.S &= \mathcal{P}\mathcal{P}^\dagger\mathcal{P} \\ &= \mathcal{P}\mathcal{P}^\intercal(\mathcal{P}\mathcal{P}^\intercal)^{-1}\mathcal{P} \\ &= I.\mathcal{P} \\ &= \mathcal{P} \text{ which is R.H.S.} \end{aligned}$$

2. $\mathcal{P}^\dagger\mathcal{P}\mathcal{P}^\dagger = \mathcal{P}^\dagger$.

$$\begin{aligned} L.H.S &= \mathcal{P}^\dagger\mathcal{P}\mathcal{P}^\dagger \\ &= \mathcal{P}^\intercal(\mathcal{P}\mathcal{P}^\intercal)^{-1}.\mathcal{P}.\mathcal{P}^\intercal(\mathcal{P}\mathcal{P}^\intercal)^{-1} \\ &= \mathcal{P}^\intercal(\mathcal{P}\mathcal{P}^\intercal)^{-1}.I \\ &= \mathcal{P}^\dagger \text{ that is R.H.S.} \end{aligned}$$

3. $(\mathcal{P}\mathcal{P}^{\dagger})^{-1} = \mathcal{P}\mathcal{P}^{\dagger}$.

$$\begin{aligned}
L.H.S &= (\mathcal{P}\mathcal{P}^{\dagger})^{-1}.\\
&= \mathcal{P}(\mathcal{P}^{\intercal}(\mathcal{P}\mathcal{P}^{\intercal})^{-1})^{-1}.\\
&= I^{-1}\\
&= I.\\
R.H.S &= \mathcal{P}\mathcal{P}^{\dagger}\\
&= \mathcal{P}\mathcal{P}^{\intercal}(\mathcal{P}\mathcal{P}^{\intercal})^{-1}\\
&= I.
\end{aligned}$$

4. $(\mathcal{P}^{\dagger}\mathcal{P})^{-1} = \mathcal{P}^{\dagger}\mathcal{P}$.

$$\begin{aligned}
L.H.S &= (\mathcal{P}^{\dagger}\mathcal{P})^{-1}\\
&= (\mathcal{P}^{\intercal}(\mathcal{P}\mathcal{P}^{\intercal})^{-1}\mathcal{P})^{-1}\\
&= I^{-1}\\
&= I.\\
R.H.S &= \mathcal{P}^{\dagger}\mathcal{P}\\
&= \mathcal{P}^{\intercal}(\mathcal{P}\mathcal{P}^{\intercal})^{-1}\mathcal{P}\\
&= I.
\end{aligned}$$

All the proofs are satisfied.

Pseduoinverse is calculated by two different way.

- If $\mathcal{P}$ has columns that are linearly independent and matrix $\mathcal{P}^{\intercal}\mathcal{P}$ is invertible then $\mathcal{P}^{\dagger}$ can be calculated as

$$\mathcal{P}^{\dagger} = (\mathcal{P}^{\intercal}\mathcal{P})^{-1}\mathcal{P}^{\intercal}.$$

  Because in this case number of columns is less than equal to the number of rows.

  The pseudoinverse is a left inverse, $\mathcal{P}^{\dagger}\mathcal{P} = I$.

- If the matrix $\mathcal{P}$ has linearly independent rows and $\mathcal{P}\mathcal{P}^{\intercal}$ is invertible then $\mathcal{P}^{\dagger}$ calculated as

$$\mathcal{P}^{\dagger} = \mathcal{P}^{\intercal}(\mathcal{P}^{\intercal}\mathcal{P})^{-1}.$$

  Because in this case number of rows is less than equal to the number of columns. The pseudoinverse is a right inverse, $\mathcal{P}^{\dagger} = I$.

Basic characteristics

- If $\mathcal{P}$ has real enteries, then $\mathcal{P}^{\dagger}$ also does.
- If $\mathcal{P}$ can be inverted, then its pseudoinverse is also inverse. That is

$$\mathcal{P}^{\dagger} = \mathcal{P}^{-1}.$$

- The initial matrix $\mathcal{P}$ is the pseudoinverse of the pseudoinverse.

$$(\mathcal{P}^{\dagger})^{\dagger} = \mathcal{P}.$$

- Transposition, conjugation, and taking the conjugate transpose commute with pseudoinversion.

$$(\mathcal{P}^{T})^{\dagger} = (\mathcal{P}^{\dagger})^{\intercal}, (\bar{\mathcal{P}})^{\dagger} = \bar{\mathcal{P}}^{\dagger}, (\mathcal{P}^{-1})^{\dagger} = (\mathcal{P}^{\dagger})^{-1}.$$

- The scalar multiple of Pseduoinverse $\mathcal{P}$ is the reciprocal of $\mathcal{P}^{\dagger}$:

$$(\gamma\mathcal{P})^{\dagger} = (\gamma^{-1})\mathcal{P}^{\dagger} for\ \gamma \neq 0.$$

Example 2.1.6. Find the Moore-Penrose pseudoinverse of the following matrix

$$A = \begin{bmatrix} 2 & 15 & 20 & 4 & 9 & 1 & 8 \\ 17 & 2 & 15 & 13 & 23 & 2 & 13 \end{bmatrix} \quad \text{mod } 95.$$

and satisfy the pseduoinverse properties.

Solution:

The pseudoinverse of a matrix A is $A^{\dagger} = A^{\intercal}(AA^{\intercal})^{-1}$. Because the rows of A are linearly independent, the pseduoinverse $A^{\dagger}$ of A is given as

$$A^{\dagger} = A^{\intercal}(AA^{\intercal})^{-1} \mod 95.$$

First, find $A^{\intercal}$

$$A^{\intercal} = \begin{bmatrix} 2 & 15 & 20 & 4 & 9 & 1 & 8 \\ 17 & 2 & 15 & 13 & 23 & 2 & 13 \end{bmatrix}^{\intercal} = \begin{bmatrix} 2 & 17 \\ 15 & 2 \\ 20 & 15 \\ 4 & 13 \\ 9 & 23 \\ 1 & 2 \\ 8 & 13 \end{bmatrix}.$$

Now,

$$AA^{\intercal} = \begin{bmatrix} 2 & 15 & 20 & 4 & 9 & 1 & 8 \\ 17 & 2 & 15 & 13 & 23 & 2 & 13 \end{bmatrix} \begin{bmatrix} 2 & 17 \\ 15 & 2 \\ 20 & 15 \\ 4 & 13 \\ 9 & 23 \\ 1 & 2 \\ 8 & 13 \end{bmatrix} \mod 95.$$

$$= \begin{bmatrix} 791 & 729 \\ 729 & 1389 \end{bmatrix} \mod 95.$$

$$= \begin{bmatrix} 31 & 64 \\ 64 & 59 \end{bmatrix} \mod 95$$

To find $(AA^{\intercal})^{-1}$

$$(AA^{\intercal})^{-1} = \begin{bmatrix} 31 & 64 \\ 64 & 59 \end{bmatrix}^{-1} \quad \text{mod } 95$$

$$= \begin{bmatrix} 63 & 17 \\ 17 & 17 \end{bmatrix} \quad \text{mod } 95.$$

Finally, multiply the matrices $A^{\intercal}(AA^{\intercal})^{-1}$, to get $A^{\dagger}$

$$A^{\dagger} = (AA^{\intercal})^{-1} = \begin{bmatrix} 2 & 17 \\ 15 & 2 \\ 20 & 15 \\ 4 & 13 \\ 9 & 23 \\ 1 & 2 \\ 8 & 13 \end{bmatrix} \begin{bmatrix} 63 & 17 \\ 17 & 17 \end{bmatrix} \quad \text{mod } 95$$

$$A^{\dagger} = \begin{bmatrix} 35 & 38 \\ 29 & 4 \\ 90 & 25 \\ 93 & 4 \\ 8 & 69 \\ 2 & 51 \\ 60 & 72 \end{bmatrix}.$$

The next computations show that the above computated $A^{\dagger}$ satisfies all the four properties.

Property:1

$\mathcal{A}\mathcal{A}^{\dagger}\mathcal{A} = \mathcal{A}$

$$\mathcal{A}\mathcal{A}^{\dagger} = \begin{bmatrix} 2 & 15 & 20 & 4 & 9 & 1 & 8 \\ 17 & 2 & 15 & 13 & 23 & 2 & 13 \end{bmatrix} \begin{bmatrix} 35 & 38 \\ 29 & 4 \\ 90 & 25 \\ 93 & 4 \\ 8 & 69 \\ 2 & 51 \\ 60 & 72 \end{bmatrix} \mod 95.$$

$$= \begin{bmatrix} 3231 & 1900 \\ 4180 & 3706 \end{bmatrix} \mod 95$$

$$\mathcal{A}\mathcal{A}^{\dagger}\mathcal{A} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 2 & 15 & 20 & 4 & 9 & 1 & 8 \\ 17 & 2 & 15 & 13 & 23 & 2 & 13 \end{bmatrix}$$

$$= \begin{bmatrix} 2 & 15 & 20 & 4 & 9 & 1 & 8 \\ 17 & 2 & 15 & 13 & 23 & 2 & 13 \end{bmatrix} = \mathcal{A}.$$

Property:2 $\mathcal{A}^{\dagger}\mathcal{A}\mathcal{A}^{\dagger} = \mathcal{A}^{\dagger}$ that is

$$\mathcal{A}^{\dagger}\mathcal{A}\mathcal{A}^{\dagger} = \begin{bmatrix} 35 & 38 \\ 29 & 4 \\ 90 & 25 \\ 93 & 4 \\ 8 & 69 \\ 2 & 51 \\ 60 & 72 \end{bmatrix} \begin{bmatrix} 2 & 15 & 20 & 4 & 9 & 1 & 8 \\ 17 & 2 & 15 & 13 & 23 & 2 & 13 \end{bmatrix} \begin{bmatrix} 35 & 38 \\ 29 & 4 \\ 90 & 25 \\ 93 & 4 \\ 8 & 69 \\ 2 & 51 \\ 60 & 72 \end{bmatrix} \mod 95$$

$$= \begin{bmatrix} 35 & 38 \\ 29 & 4 \\ 90 & 25 \\ 93 & 4 \\ 8 & 69 \\ 2 & 51 \\ 60 & 72 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} 35 & 38 \\ 29 & 4 \\ 90 & 25 \\ 93 & 4 \\ 8 & 69 \\ 2 & 51 \\ 60 & 72 \end{bmatrix} = \mathcal{A}^{\dagger}.$$

Property:3 $(\mathcal{P}\mathcal{P}^{\dagger})^{-1} = \mathcal{P}\mathcal{P}^{\dagger}$

$$\begin{aligned} (\mathcal{P}\mathcal{P}^{\dagger})^{-1} &= \left(\begin{bmatrix} 2 & 15 & 20 & 4 & 9 & 1 & 8 \\ 17 & 2 & 15 & 13 & 23 & 2 & 13 \end{bmatrix} \begin{bmatrix} 35 & 38 \\ 29 & 4 \\ 90 & 25 \\ 93 & 4 \\ 8 & 69 \\ 2 & 51 \\ 60 & 72 \end{bmatrix} \right)^{-1} \\ &= \left(\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \right)^{-1} \\ &= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}. \end{aligned}$$

Taking R.H.S

$$\mathcal{P}\mathcal{P}^{\dagger} = \begin{bmatrix} 2 & 15 & 20 & 4 & 9 & 1 & 8 \\ 17 & 2 & 15 & 13 & 23 & 2 & 13 \end{bmatrix} \begin{bmatrix} 35 & 38 \\ 29 & 4 \\ 90 & 25 \\ 93 & 4 \\ 8 & 69 \\ 2 & 51 \\ 60 & 72 \end{bmatrix} \mod 95$$

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

Property:4 $(\mathcal{P}^{\dagger}\mathcal{P})^{-1} = \mathcal{P}^{\dagger}\mathcal{P}$

$$(\mathcal{P}^{\dagger}\mathcal{P})^{-1} = \left(\begin{bmatrix} 35 & 38 \\ 29 & 4 \\ 90 & 25 \\ 93 & 4 \\ 8 & 69 \\ 2 & 51 \\ 60 & 72 \end{bmatrix} \begin{bmatrix} 2 & 15 & 20 & 4 & 9 & 1 & 8 \\ 17 & 2 & 15 & 13 & 23 & 2 & 13 \end{bmatrix} \right)^{-1}$$

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

R.H.S

$$\mathcal{P}^{\dagger}\mathcal{P} = \begin{bmatrix} 35 & 38 \\ 29 & 4 \\ 90 & 25 \\ 93 & 4 \\ 8 & 69 \\ 2 & 51 \\ 60 & 72 \end{bmatrix} \begin{bmatrix} 2 & 15 & 20 & 4 & 9 & 1 & 8 \\ 17 & 2 & 15 & 13 & 23 & 2 & 13 \end{bmatrix}$$

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

Hence all the properties are satisfied.

2.2 Cryptography

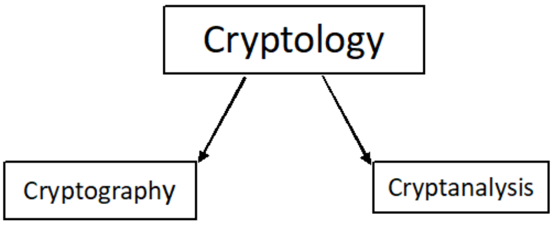

Figure 2.1: Kinds of Cryptology

Cryptography is the branch of Cryptology in which study of secure communication between two parties through a public channel in the presence of third party(e.g hacker) is known as cryptography. Through the use of codes, it is a technique for protecting communication and information. It is used to encode the original data so that it cannot be read by anybody other than the intended recepient. The coded message is referred to as ciphertext, whereas the plaintext is the original message and it is not delivered to the orginal user in its real form; rather, it is first changed into an unreadable form before being sent. The encryption algorithm

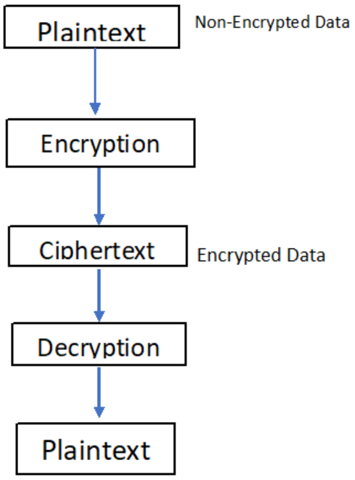

Figure 2.2: Cryptography

transforms the plaintext into ciphertext. The decryption algorithm transforms the ciphertext back into plaintext. For encryption and decryption techniques, both sender and receiver use a secret information (known only to sender and receiver) known as a key. The security of a secure connection depend on the integrity of the encryption key., it should be kept secret at all times. This procedure is known as a cryptosystem. A cryptosystem's security only depends on the security of the key.

Types of key

The cryptography is further separated into the two following major groups based on the design of a cryptosystem:

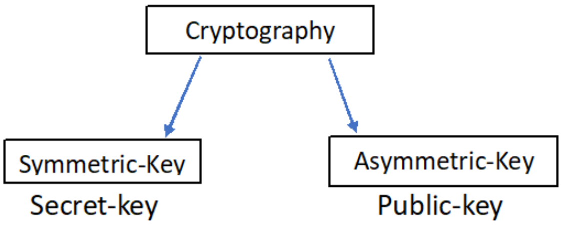

Figure 2.3: Cryptographic Protocols

- Symmetric (secret) key cryptography.
- Asymmetric (public) key cryptography.

2.2.1 Symmetric Key

Symmetric key cryptography, also referred to as secret key cryptography. Symmetric key is a method where two parties utilize a single key to both encrypt and decrypt data. This was the exclusive approach employed for secure communication until 1976. In simple terms, symmetric key cryptography involves using a shared secret key for both encrypting and decrypting information[18].For instance Two persons one is Ayesha and other is Bilal, want to communicate with each other over an insecure channel like the Internet. To ensure the security of their communication, they start by sharing a secret key through a secure channel. This key will be used for both encryption and decryption. **How it works:** Ayesha takes the secret key K and uses it to encrypt the information She wishes to distribute it with Bilal.. She uses an encryption algorithm E_K to transform the message into a secret code called ciphertext. Ayesha then sends this encrypted message to Bilal over the insecure channel. To decrypt the message and retrieve the original information, Bilal needs the secret key. Ayesha securely sends the key to Bilal through a separate, safe channel. When Bilal receives the key K, he can easily use it with the decryption algorithm D_k to convert the ciphertext back into the original message. It is important to note that for this method to work, the party encrypting the message must send the encryption key to the other party. Without the key, the encrypted message cannot be deciphered. Therefore, it is crucial to use a secure channel to send the key to the intended recipient. If the key falls into the wrong hands during transmission, the confidentiality of the message could be compromised. Example of the symmetric key are

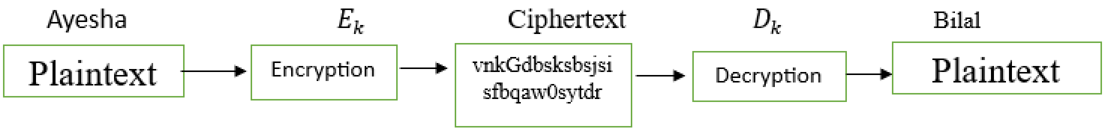

FIGURE 2.4: Symmetric Key

1. AES [19]

2. DES[20]

Symmetric key cryptography has the following drawback

- **Shared keys**: When a group of n people communicates, distributing the encryption key becomes a problem. If just one person shares the key, it puts the entire communication at risk.
- **Authentication:** A significant challenge is authentication, particularly when Ayesha and Bilal communicate. Ayesha needs a way to verify that the received message indeed came from Bilal.

2.2.2 Asymmetric Key

Symmetric key cryptography had some drawbacks. One major issue was the challenge of securely sharing the encryption key between the sender and the receiver. To overcome this problem, Diffie Hellman [21] introduced the idea of public key cryptography. It is also called as asymmetric key cryptography, in 1976. Two unique keys have been used in public key cryptography, a public key that is used for encryption and a private key for decryption. The public key K_1 can be freely shared with anyone, allowing them to encrypt messages and send them to the intended recipient. However, only the owner of the private key K_2, which is kept secret, can decrypt the messages. Diffie-Hellman key exchange protocol [22], RSA [23] are examples of asymmetric key.

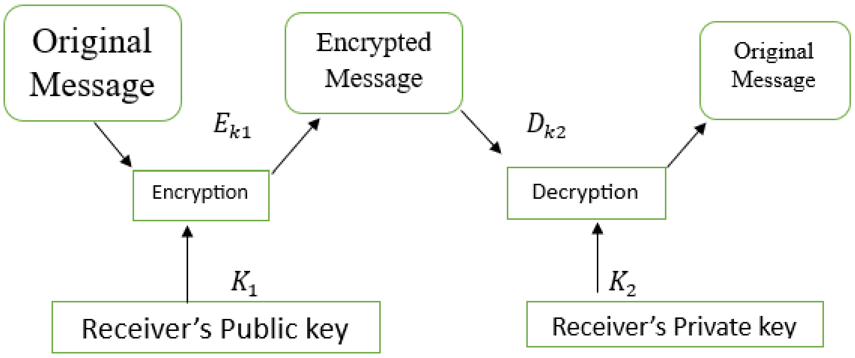

FIGURE 2.5: Asymmetric

2.2.3 Application of cryptography

Cryptography is a foundational technology for ensuring the confidentiality, integrity, and authenticity of information in various domains, and its applications continue to evolve with advances in technology and the increasing need for secure communication and data protection. Several uses for cryptography are given below:[24]

Confidentiality

It is important to keep information private and protect it from unauthorized individuals. For instance, Amna wants to send some personal data to Bilal. If an attacker like Darth intercepts the encrypted data during transmission, and will be unable to read it. The purpose of confidentiality is to ensure that the original information remains a secret.

Integrity

Integrity ensures that the original data remains same during storage or transmission to the intended recipient. It helps Bilal trust that the information he receives from Amna in encrypted form is exactly as it was when it was sent. Integrity provides assurance that the information has not been tampered with along the way.

Non-repudiation

Non-repudiation shows that the information's source cannot later reject it . For instance, there is no way for Bilal to later reject the information if it has been provided by bilal. This makes it easier for the person receiving it to obtain the sender's trust in any cryptographic scheme.

Authentication

It allows possible for the sender and recipient to verify each other's identity. For example Amna and Bilal establish up a secure communication channel. Amna and Bilal must be able to confirm each other's identities in order to share information properly. This characteristic allows users to verify that other users are real not to be criminals. These applications create an effective and secure cryptographic communication protocol that is more dependable and useful, and so enables a better platform that satisfies the fundamental requirements of a safe connection.

2.3 Cryptanalysis

The second branch of cryptography is cryptanalysis. It is the process of recovering the key from the ciphertext or the plaintext without the using of a key. [25]. For the purpose of trying to identify or improve methods for breaking or destroy them, cryptanalysis experts investigate ciphers, cryptosystems, and ciphertext to understand how they work. However, as we're about to learn, it can be used for good or evil purposes. Many different kinds of groups are involved in cryptanalysis, including governments looking for ways to unlock the private communications of other countries, businesses producing safety devices who use cryptanalysts for testing their privacy functions, hackers, crackers, non-governmental organizations, and researchers searching for flaws in cryptographic protocols and methods. The continual struggle between cryptanalysis and cryptographers to unlock cryptosystems and protect data is what improves our understanding of cryptology as a whole. There are exist two different attack.

- Active attack
- Passive attack

1. **Active Attack**

   In the active attack when a "message tampering" occurs. A person with malicious intent interrupts the communication and changes the message's content. This tampering can have harmful effects [5] because it compromises the "integrity" of the message, meaning the message's originality and accuracy are no longer trustworthy. Example of active attack is "man in the middle attack"

2. **Passive Attack**

   In the passive attack, the attacker tries to obtain or use information from the system without causing any noticeable impact on the system's resources [5]. The primary goal of passive attacks is to gather information covertly. An example of this passive attack is the "known plaintext attack."

Depending on the models given above, cryptanalysis has many forms of attacks. The difference between these attacks is based on the level of information available to the attacker.. Somes of attacks are discussed below [26].

1. **Known Plaintext Attack**

   In known-plaintext attacks, the attacker possesses access to both the ciphertext and the corresponding plaintext to some extent. Using this information, he either finds a logical method for cracking several ciphertexts or makes every logical effort to find the key used in the encryption function again. One historical example of a known plaintext attack involves the Enigma machine used by the Germans during World War II.

2. **Choosen Plaintext Attack**

   The attacker select a random plaintext and attempts to decode it. He will now apply the combination of using both the chosen plaintext and the ciphertext that corresponds to it in order to determine the secret key.

3. **Choosen ciphertext attack**

   In choosen plaintext attack, the attacker selects a ciphertext. It makes an effort to figure out the related plaintext or gets as much information as they can in an attempt to unlock the encryption algorithm's shared secret key.

4. **Man in the Middle Attack**

   This attack involves the attacker remaining in the middle of the two parties who are speaking in confidence while attempting to hack both sides of the conversation. For the purpose of attempting to implement a man in the middle attack, the attacker selects two mock-up keys, uses one of them to create a channel of communication with the first party, then receives the text that is encrypted makes an effort to crack it using his own personal keys. Then, using his keys, he encodes or changes the message that was obtained and sends it to the other party. When the other party contacts him and establishes connection, he unlocks their encrypted data using his keys. By hiding their true identity from both ends, one might stop the entire conversation and endanger the system's security.

5. **Brute Force Attack**

   The main objective of a brute force attack is to try every combination until you find the correct one. It is a method where the attacker completely checks every option, like trying every possible password until they discover the right one to gain unauthorized access to a system or decrypt encrypted data. It is a time consuming process, but if the password or encryption key is weak or short, it can be successful.

2.3.1 Playfair Cipher

The Playfair cipher is a type of symmetric polyalphabetic encryption that employs block substitution. Its initial invention can be credited to Charles Wheatstone in 1854, but it gained widespread recognition and popularity through the efforts of Lord Playfair [27].

Encryption Method

To construct the square table 5×5 for the playfair cipher, begin with a chosen keyword, removing any duplicate characters. The unique characters are then placed in the matrix. Any remaining empty spaces in the matrix are filled with the remaining characters in alphabetic order.

$$\begin{bmatrix} K & E & Y & W & O \\ R & D & A & B & C \\ F & G & H & I/J & L \\ M & N & P & Q & S \\ T & U & V & X & Z \end{bmatrix}$$

In the Playfair cipher, the English alphabet is represented in pairs of letters, traditionally using "I" and"J" together in a single entry. The plaintext is viewed as a series of two-character blocks. If the plaintext has an odd length, a filler is added at the end to create a complete two-character block for encryption. Whenever a letter in a pair is repeated, insert the filler X in the pair to break the repetition. In simple terms, the substitution rules for the blocks are as follows:

1. If two characters are on the same row, replace each character with the next one in that row, wrapping around to the first element if needed.

2. If two characters are on the same column, replace each character with the one below it, wrapping around to the top element if needed.

3. If two characters are neither on the same row nor the same column, replace each character with the one on its row that aligns with the other character vertically (same column).

Decryption

To decrypt the message, the receiver needs the same key used during encryption to create the key table. Having the correct key allows the receiver to easily reverse the encryption process and read the original message.

Example 2.3.1. Encrypt a message GIRL'S HOSTEL using playfair cipher using keyword INSTRUNMENT and also perform decryption.

Encryption:

Using keyword create the matrix for encryption and decryption as given below.

$$\begin{bmatrix} I/J & N & S & T & R \\ U & M & E & A & B \\ C & D & F & G & H \\ K & L & O & P & Q \\ V & W & X & Y & Z \end{bmatrix}$$

Spilt the plaintext in the pairs as GI, RL, SH, OS, TE, LX. Add a X with L because L has no any pair. Now, encrypt the GI, RL, SH, OS, TE, LX

$$\text{GI} \rightarrow \text{CT}$$
$$\text{RL} \rightarrow \text{NQ}$$
$$\text{SH} \rightarrow \text{RF}$$
$$\text{OS} \rightarrow \text{XE}$$
$$\text{TE} \rightarrow \text{SA}$$
$$\text{LX} \rightarrow \text{OW}$$

Therefore, the resultant ciphertext is “CTNQRFXESAOW”.

Decryption

Now, decrypt the ciphertext “CTNQRFXESAOW”. Spilt the given ciphertext in the pairs CT, NQ, RF, XE, SA, OW.

$$\begin{aligned} \text{CT} &\rightarrow \text{GI} \\ \text{NQ} &\rightarrow \text{RL} \\ \text{RF} &\rightarrow \text{SH} \\ \text{XE} &\rightarrow \text{OS} \\ \text{SA} &\rightarrow \text{TE} \\ \text{OW} &\rightarrow \text{LX} \end{aligned}$$

Hence, the resulting plaintext is “GIRLS HOSTELX”. Now, by inserting approprite space and removing the filler the crossponding message is “GIRLS HOSTEL”.

2.3.2 Hill Cipher

Lester S. Hill created the Hill Cipher in 1929 [28]. It had been first practical polygraphic cipher, capable of operating on more than three symbols at once. The Hill Cipher is an encryption algorithm that uses linear algebra concepts, where each letter is represented by a number (e.g., A=0, B=1, C=2, ..., Z=25 for English). The message to be encrypted or decrypted is divided into blocks of n letters and multiplied by a non singular square matrix using modulo arithmetic based on the size of the alphabet being used [29].

Key Generation

Hill cipher is a cryptographic algorithm that uses matrix as a key by utilizing modulo operations. The key matrix used is usually made randomly as a square matrix that must be invertible. The order of the matrix is determined by the block size of the cipher. That is, for a block size of n, the key matrix is of order $n \times n$.

Ecryption process

The plaintext message is divided into blocks of fixed size, usually the same size as the key matrix. Each block is then converted to a vector of numerical values based on a mapping of the plaintext characters to integers (usually A = 0, B = 1, ..., Z = 25 for the English alphabet). The key matrix is multiplied with each vector of plaintext characters to get a new vector representing the encrypted characters. The new vector is converted back to characters using the reverse mapping, generating the ciphertext. The following formula is used in Hill cipher for encryption process

$$Y = E(\mathcal{K}, X) = X\mathcal{K} \mod n$$

where $\mathcal{K}$ is Key martix, X is Plaintext and Y is Ciphertext.

Decryption process

To decrypt the ciphertext, the recipient should have the same key matrix used for encryption, but with the inverse matrix calculated using modular arithmetic. The encrypted message is divided into blocks of the same size as the key matrix. Each block is converted to a vector of numerical values, similar to the encryption process. The inverse of the key matrix is multiplied with each vector of ciphertext characters to obtain a new vector representing the decrypted characters. The new vector is converted back to characters using the reverse mapping, recovering the original plaintext. The following formula is used for decryption process

$$X = D(\mathcal{K}, Y) = Y\mathcal{K}^{-1} \mod n$$

Where, $\mathcal{K}^{-1} = Adj\mathcal{K} \cdot (Det\mathcal{K})^{-1} \mod n$

Example 2.3.2.

Consider the encoding table given below.

TABLE 2.2: Numerical equivalent to each letter

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

Encrypt the message “PAY MORE MONEY” using Hill cipher with encryption key and show the decryption of the ciphertext to recover the original plaintext.

$$\mathcal{K} = \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix}$$

Solution:

As the order of $\mathcal{K}$ is 3×3. Spilt plaintext in blocks of 3 characters as:

Plaintext = PAY, MOR, EMO, NEY

Using the encoding table (2.3)

The numerical form of plaintext =

$$\begin{bmatrix} 15 & 0 & 24 \end{bmatrix}, \begin{bmatrix} 12 & 14 & 17 \end{bmatrix}$$

$$\begin{bmatrix} 4 & 12 & 14 \end{bmatrix} and \begin{bmatrix} 13 & 4 & 24 \end{bmatrix}$$

Encryption

Now, encrypting PAY

$$\begin{bmatrix} Y_1 & Y_2 & Y_3 \end{bmatrix} = \begin{bmatrix} X_1 & X_2 & X_3 \end{bmatrix} \begin{bmatrix} K_{11} & K_{12} & K_{13} \\ K_{21} & K_{22} & K_{23} \\ K_{31} & K_{32} & K_{33} \end{bmatrix} \quad \text{mod } 26.$$

Encrypt PAY

$$\begin{bmatrix} Y_1 & Y_2 & Y_3 \end{bmatrix} = \begin{bmatrix} 15 & 0 & 24 \end{bmatrix} \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix} \quad \text{mod } 26$$

$$= \begin{bmatrix} 303 & 303 & 531 \end{bmatrix} \quad \text{mod } 26$$

$$= \begin{bmatrix} 17 & 17 & 11 \end{bmatrix} \quad \text{mod } 26$$

$$= \begin{bmatrix} R & R & L \end{bmatrix} \text{From table (2.3).}$$

Now, encrypting MOR

$$
\begin{aligned}
\begin{bmatrix} Y_4 & Y_5 & Y_6 \end{bmatrix} &= \begin{bmatrix} 12 & 14 & 17 \end{bmatrix} \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix} \\
&= \begin{bmatrix} 532 & 490 & 677 \end{bmatrix} \mod 26 \\
&= \begin{bmatrix} 12 & 22 & 1 \end{bmatrix} \mod 26 \\
&= \begin{bmatrix} M & W & B \end{bmatrix}.
\end{aligned}
$$

The encrypt of EMO is given below:

$$
\begin{aligned}
\begin{bmatrix} Y_7 & Y_8 & Y_9 \end{bmatrix} &= \begin{bmatrix} 14 & 12 & 14 \end{bmatrix} \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix} \mod 26 \\
&= \begin{bmatrix} 348 & 312 & 538 \end{bmatrix} \mod 26 \\
&= \begin{bmatrix} 10 & 0 & 18 \end{bmatrix} \mod 26 \\
&= \begin{bmatrix} K & A & S \end{bmatrix}.
\end{aligned}
$$

Finally, NEY is encrypted as:

$$
\begin{aligned}
\begin{bmatrix} Y_{10} & Y_{11} & Y_{12} \end{bmatrix} &= \begin{bmatrix} 13 & 4 & 24 \end{bmatrix} \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix} \mod 26 \\
&= \begin{bmatrix} 761 & 341 & 605 \end{bmatrix} \mod 26 \\
&= \begin{bmatrix} 15 & 3 & 7 \end{bmatrix} \mod 26 \\
&= \begin{bmatrix} P & D & H \end{bmatrix}.
\end{aligned}
$$

Combining all the ciphertext vectors, are the resulting ciphertext is RRLMWBKASPDH.

Decryption:

As we known the formula for decryption is

$$X = D(\mathcal{K}, Y) = Y\mathcal{K}^{-1} \mod n.$$

So, first we will find out the $\mathcal{K}^{-1}$ and the formula of $\mathcal{K}^{-1} = Adj\mathcal{K} \cdot (Det\mathcal{K})^{-1} \mod 26$.

$$\mathcal{K} = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \mod 26.$$

Therefore,

$$\begin{aligned} Det(\mathcal{K}) =& 17(18 \times 19 - 2 \times 21) - 17(19 \times 21 - 2 \times 21) + \\ & 5(2 \times 21 - 2 \times 18) \mod 26 \\ =& 5100 - 6069 + 30 \mod 26 \\ =& -939 \mod 26 \\ =& 23. \end{aligned}$$

Now, find the $Adj(\mathcal{K})$. The cofactor matrix consists of all cofactor of the given matrix, which are calculated according to the formula $C_{ij} = (-1)^{i+j} M_{ij}$, where M_{ij} is the minor. For example, the determinant of the submatrix formed by deleting row i and column j from the given matrix. Calculate all factors:

$$\begin{aligned} C_{11} &= (-1)^{1+1} \begin{vmatrix} 18 & 21 \\ 2 & 19 \end{vmatrix} \mod 26 \\ &= 300 \mod 26 \\ &= 14 \mod 26. \\ C_{12} &= (-1)^{1+2} \begin{vmatrix} 21 & 21 \\ 2 & 19 \end{vmatrix} \mod 26 \\ &= -357 \mod 26 \end{aligned}$$

$$= 7 \mod 26.$$

$$C_{13} = (-1)^{1+3} \begin{vmatrix} 21 & 18 \\ 2 & 2 \end{vmatrix} \mod 26$$

$$= 6 \mod 26.$$

$$C_{21} = (-1)^{2+1} \begin{vmatrix} 17 & 5 \\ 2 & 19 \end{vmatrix} \mod 26$$

$$= -313 \mod 26$$

$$= 25 \mod 26.$$

$$C_{22} = (-1)^{2+2} \begin{vmatrix} 17 & 5 \\ 2 & 19 \end{vmatrix} \mod 26$$

$$= 313 \mod 26$$

$$= 1 \mod 26.$$

$$C_{23} = (-1)^{2+3} \begin{vmatrix} 17 & 5 \\ 2 & 19 \end{vmatrix} \mod 26$$

$$= 0 \mod 26.$$

$$C_{31} = (-1)^{3+1} \begin{vmatrix} 17 & 5 \\ 18 & 21 \end{vmatrix} \mod 26$$

$$= 7 \mod 26.$$

$$C_{32} = (-1)^{3+2} \begin{vmatrix} 17 & 5 \\ 21 & 21 \end{vmatrix} \mod 26$$

$$= -252 \mod 26$$

$$= 8 \mod 26.$$

$$C_{33} = (-1)^{3+3} \begin{vmatrix} 17 & 17 \\ 21 & 18 \end{vmatrix} \mod 26$$

$$= 1 \mod 26.$$

Thus, the cofactor matrix of $\mathcal{K}$ is

$$= \begin{bmatrix} 14 & 7 & 6 \\ 25 & 1 & 0 \\ 7 & 8 & 1 \end{bmatrix} \mod 26.$$

Transpose of the above matrix $\mathcal{K}$ is Adj$\mathcal{K}$ given below.

$$Adj\mathcal{K} = \begin{bmatrix} 14 & 25 & 7 \\ 7 & 1 & 8 \\ 6 & 0 & 1 \end{bmatrix} \mod 26.$$

Now,

$$\mathcal{K}^{-1} = Adj\mathcal{K} \cdot (Det\mathcal{K})^{-1} \mod 26$$

$$=\frac{1}{23} \begin{bmatrix} 14 & 25 & 7 \\ 7 & 1 & 8 \\ 6 & 0 & 1 \end{bmatrix} \mod 26$$

$$\mathcal{K}^{-1} =17 \times \begin{bmatrix} 14 & 25 & 7 \\ 7 & 1 & 8 \\ 6 & 0 & 1 \end{bmatrix} \mod 26$$

$$= \begin{bmatrix} 238 & 425 & 119 \\ 119 & 17 & 136 \\ 102 & 0 & 17 \end{bmatrix} \mod 26$$

$$= \begin{bmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{bmatrix} \mod 26.$$

Now,we will use the formula of decryption

$$X = D(\mathcal{K}, Y) = X\mathcal{K}^{-1} \mod 26.$$

The ciphertext vectors crossponding to ciphertext RRL,MWB,KAS,PDH are

$$\begin{bmatrix} 17 & 17 & 11 \end{bmatrix}, \begin{bmatrix} 12 & 22 & 1 \end{bmatrix}, \begin{bmatrix} 10 & 0 & 18 \end{bmatrix} \, and \begin{bmatrix} 15 & 3 & 7 \end{bmatrix}$$

R	R	L	M	W	B	K	A	S	P	D	H
17	17	11	12	22	1	10	0	18	15	3	7

.

Decrypt "RRL"

$$\begin{bmatrix} X_1 & X_2 & X_3 \end{bmatrix} = \begin{bmatrix} R & R & L \end{bmatrix} \begin{bmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{bmatrix} \mod 26$$

$$= \begin{bmatrix} 17 & 17 & 14 \end{bmatrix} \begin{bmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{bmatrix} \mod 26$$

$$= \begin{bmatrix} 587 & 442 & 544 \end{bmatrix} \mod 26$$

$$= \begin{bmatrix} 15 & 0 & 24 \end{bmatrix}$$

$$\begin{bmatrix} X_1 & X_2 & X_3 \end{bmatrix} = \begin{bmatrix} P & A & Y \end{bmatrix}.$$

Decrypt "MWB"

$$\begin{aligned}\begin{bmatrix}X_4 & X_5 & X_6\end{bmatrix} &= \begin{bmatrix}M & W & B\end{bmatrix}\begin{bmatrix}4 & 9 & 15\\ 15 & 17 & 6\\ 24 & 0 & 17\end{bmatrix} \mod 26\\ &= \begin{bmatrix}12 & 22 & 1\end{bmatrix}\begin{bmatrix}4 & 9 & 15\\ 15 & 17 & 6\\ 24 & 0 & 17\end{bmatrix} \mod 26\\ &= \begin{bmatrix}402 & 482 & 329\end{bmatrix} \mod 26\\ &= \begin{bmatrix}12 & 14 & 17\end{bmatrix}\end{aligned}$$

$$\begin{bmatrix}X_4 & X_5 & X_6\end{bmatrix} = \begin{bmatrix}M & O & R\end{bmatrix}.$$

Decrypt "KAS"

$$\begin{aligned}\begin{bmatrix}X_7 & X_8 & X_9\end{bmatrix} &= \begin{bmatrix}K & A & S\end{bmatrix}\begin{bmatrix}4 & 9 & 15\\ 15 & 17 & 6\\ 24 & 0 & 17\end{bmatrix} \mod 26\\ &= \begin{bmatrix}10 & 0 & 18\end{bmatrix}\begin{bmatrix}4 & 9 & 15\\ 15 & 17 & 6\\ 24 & 0 & 17\end{bmatrix} \mod 26\\ &= \begin{bmatrix}472 & 90 & 456\end{bmatrix} \mod 26\\ &= \begin{bmatrix}4 & 12 & 14\end{bmatrix} \mod 26\end{aligned}$$

$$\begin{bmatrix}X_7 & X_8 & X_9\end{bmatrix} = \begin{bmatrix}E & M & O\end{bmatrix}.$$

Decrypt “PDH”

$$\begin{bmatrix} X_{10} & X_{11} & X_{12} \end{bmatrix} = \begin{bmatrix} P & D & H \end{bmatrix} \begin{bmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{bmatrix} \mod 26$$

$$= \begin{bmatrix} 15 & 3 & 7 \end{bmatrix} \begin{bmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{bmatrix} \mod 26$$

$$= \begin{bmatrix} 273 & 186 & 362 \end{bmatrix} \mod 26$$

$$= \begin{bmatrix} 13 & 4 & 24 \end{bmatrix}$$

$$\begin{bmatrix} X_{10} & X_{11} & X_{12} \end{bmatrix} = \begin{bmatrix} N & E & Y \end{bmatrix}.$$

So, the resulting plaintext is“PAY” “MOR” “EMO“NEY”
that is “Pay more money”.

Chapter 3

The Encryption Scheme based on Modified Hill Cipher Algorithm

In this chapter, a detailed work on "Generation of Rectangular Matrix for Hill Cipher Algorithm Using Playfair Cipher" by Alawiyah et al [11]. The focus of the paper is on a cryptographic approach to produce a rectangular matrix key within the Hill cipher framework.

Based on the the findings of Hidayat [30] and Alawiyah et al [11] the Playfair cipher will be used to establish a rectangular matrix key. The research suggests that using a rectangular matrix key in a Hill cipher scheme is more secure compared to a square matrix. This security arises from the fact that the resulting ciphertext is longer than the plaintext. As a result, cryptanalysts face increased challenges in attempting to see any linear equations, thus enhancing the overall security of the encryption.

3.1 Modified Hill Cipher

In traditional Hill cipher square key matrix is used in the encryption scheme but rectangular key matrix is used in the encryption scheme based on Hill cipher algorithm. The key generation, encryption and decryption are discussed given below. In below subsections X is plaintext, Y is ciphertet, $\mathcal{A}$ is key and m is modolu.

3.1.1 Key Generation

Alawiyah et al [11] used two methods to make messages secure: the Playfair cipher 2.3.1 and the Hill Cipher 2.3.2. In the Hill Cipher method, usually start by creating a random key matrix. But in this study, the key matrix using the encrypted result of the Playfair Cipher. For creating the key matrix, first made a secret key. Keywords are arrange in a table format by using the letters of the alphabet that have not be included in the kerword yet. Encrypted the plaintext and obtained ciphertext. This ciphertext changed into the numerical values under arithmetic modulo. This unique matrix becomes the key for the Hill Cipher. This method ensures the creation of a specific key matrix that derives its structure from the Playfair Cipher encryption, enhancing the security and distinctiveness of the cryptographic scheme. Consider rectangular matrix $\mathcal{A}$ which is key. The shape of the rectangular matrix key plays a crucial role. If the key matrix has a full column rank, the encryption is performed using the equations

$$Y = X\mathcal{A} \mod m.$$

On the other hand, if the key matrix has a full row rank, the encryption process utilizes the equations.

$$Y = \mathcal{A}X \mod m.$$

If the choosen rectangular matrix does not possess a pseudo-inverse, the process involves exploring other dimensions of rectangular matrices until one with a pseudo-inverse is obtained. This search aims to find a suitable rectangular matrix that fulfills the requirements for a pseudo-inverse.

$$\mathcal{A}^{\dagger} = A^{\intercal}(\mathcal{A}\mathcal{A}^{\intercal})^{-1}.$$

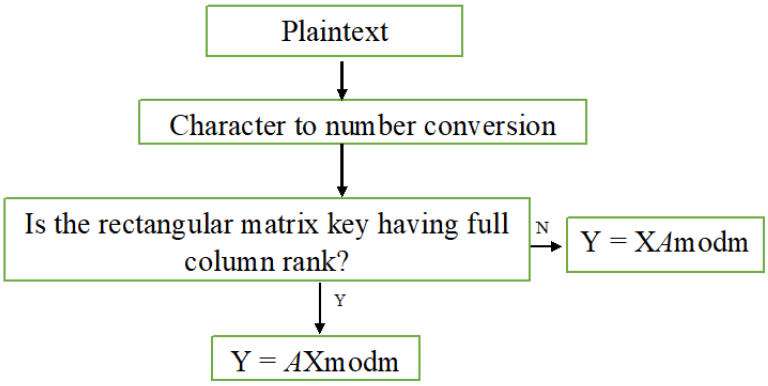
Plaintext
Character to number conversion
Is the rectangular matrix key having full column rank?
N
Y = X𝐴modm
Y
Y = 𝐴Xmodm

FIGURE 3.1: Full row rank or Full column rank

Once a rectangular matrix with a valid pseudo-inverse is identified, it can be used as the rectangular matrix key $\mathcal{A}$ for the Hill cipher algorithm.

3.1.2 Encryption

The Pseduo rectangular matrix $\mathcal{A}$ is multiply from the right side of plaintext because pseduo rectangular matrix is full row rank. So, the following formula is used in the encryption of Modified Hill cipher. X is plaintext and Y is ciphertext.

$$Y = X\mathcal{A} \mod m.$$

3.1.3 Decryption

Pseduoinverse $\mathcal{A}^{\dagger}$ is used in decryption of Modified Hill cipher because

$$\mathcal{A}^{\dagger} = \mathcal{A}^{-1}$$

as given in chapter (2) 2.1.3 Basics characteristics (point 2). So, the following formula is used in decryption of Modified Hill cipher

$$X = Y\mathcal{A}^{-1} \mod m.$$

The working of complete scheme is shown in the figure 3.2

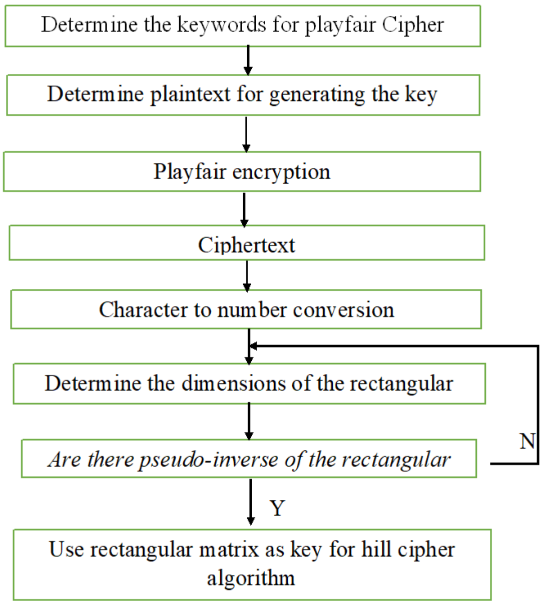
Determine the keywords for playfair Cipher
Determine plaintext for generating the key
Playfair encryption
Ciphertext
Character to number conversion
Determine the dimensions of the rectangular
Are there pseudo-inverse of the rectangular
N
Y
Use rectangular matrix as key for hill cipher algorithm

FIGURE 3.2: Rectangular matrix key for hill cipher

Example 3.1.1. The message “Research report”, keyword is“Rainbow” for key and also determine the encryption using plaintext “Secret Message” and decryption of the ciphertext to recover the original plaintext. A numerical equivalent to each letter is given in the table under modolu 95.

Char	Value	Char	Value	Char	Value	Char	Value	Char	Value
A	0	T	19	m	38	5	57	}	76
B	1	U	20	n	39	6	58	\	77
C	2	V	21	o	40	7	59	|	78
D	3	W	22	p	41	8	60	‘	79
E	4	X	23	q	42	9	61	~	80
F	5	Y	24	r	43	space	62	!	81
G	6	Z	25	t	44	,	63	@	82
H	7	a	26	u	45	<	64	#	83
I	8	b	27	v	46	.	65	$	84
J	9	c	28	w	47	>	66	%	85
K	10	d	29	x	48	/	67	∧	86
L	11	e	30	y	49	?	68	&	87
M	12	f	31	z	50	;	69	*	88
N	13	g	32	0	51	:	70	(	89
O	14	h	33	1	52	’	71	)	90
P	15	i	34	2	53	”	72	-	91
Q	16	j	35	3	54	[	73	_	92
R	17	k	36	4	55	{	74	=	93
S	18	l	37	5	56	]	75	+	94

Solution:

Playfair cipher are used to finding the key. The Keyword is “Rainbow”. So, the keyword are arranged in a matrix.

$$\begin{bmatrix} R & A & I & N & B \\ O & W & C & D & E \\ F & G & H & K & L \\ M & P & Q & S & T \\ U & V & X & Y & Z \end{bmatrix}$$

Now, encrypt the plaintext “Research report” in table 3.1. Spilt it into the pairs “RE” “SE” “AR” “CH” “RE” “PO” “RT” and get the result

$$\begin{gathered} \text{RE} \rightarrow \text{BO} \\ \text{SE} \rightarrow \text{TD} \\ \text{AR} \rightarrow \text{IA} \\ \text{CH} \rightarrow \text{HQ} \\ \text{RE} \rightarrow \text{BO} \\ \text{PO} \rightarrow \text{MW} \\ \text{RT} \rightarrow \text{BM}. \end{gathered}$$

The resulting cipertext is “BOTDIAHQBOMWBM” and it has following numerical values : $1, 14, 19, 3, 8, 0, 7, 16, 1, 14, 12, 22, 1, 12$. These numerical values are used to get of rectangular matrix $\mathcal{A}_{2\times 7}$ of order 2×7.

$$\mathcal{A} = \begin{bmatrix} 1 & 14 & 19 & 3 & 8 & 0 & 7 \\ 16 & 1 & 14 & 12 & 22 & 1 & 12 \end{bmatrix}$$

If $\mathcal{A}$ does not possess a pseduo-inverse than rectangular matrix $\mathcal{A}$ will take another dimension until one with a pseduo-inverse is obtained. Now, check whether $\mathcal{A}$ has a pseudoinverse or not. Since the number of rows is less than the number of columns in matrix $\mathcal{A}$, then

$$\mathcal{A}^{\dagger} = \mathcal{A}^{\intercal}(\mathcal{A}\mathcal{A}^{\intercal})^{-1}.$$

used for pseduoinverse. From $\mathcal{A}$, the transpose $\mathcal{A}^{\intercal}$ is given below

$$\mathcal{A}^{\intercal} = \begin{bmatrix} 1 & 16 \\ 14 & 1 \\ 19 & 14 \\ 3 & 12 \\ 8 & 22 \\ 0 & 1 \\ 7 & 12 \end{bmatrix}.$$

Multiplying $\mathcal{A}$ with $\mathcal{A}^{\intercal}$ then we get,

$$\mathcal{A}\mathcal{A}^{\intercal} = \begin{bmatrix} 1 & 14 & 19 & 3 & 8 & 0 & 7 \\ 16 & 1 & 14 & 12 & 22 & 1 & 12 \end{bmatrix} \begin{bmatrix} 1 & 16 \\ 14 & 1 \\ 19 & 14 \\ 3 & 12 \\ 8 & 22 \\ 0 & 1 \\ 7 & 12 \end{bmatrix}$$

$$\begin{aligned} \mathcal{A}\mathcal{A}^{\intercal} &= \begin{bmatrix} 680 & 592 \\ 592 & 1226 \end{bmatrix} \mod 95 \\ \mathcal{A}\mathcal{A}^{\intercal} &= \begin{bmatrix} 15 & 22 \\ 22 & 86 \end{bmatrix} \mod 95. \end{aligned}$$

As Det$(\mathcal{A}) = 46$ coprime with $95 \neq 0 \mod 95$ and therefore, $(\mathcal{A}\mathcal{A}^{\intercal})^{-1}$ and hence $\mathcal{A}$ is pseduoinverse. Now,

$$\begin{aligned} (\mathcal{A}\mathcal{A}^{\intercal})^{-1} =& (Det((\mathcal{A}\mathcal{A}^{\intercal}))^{-1} Adj(AA^{\intercal}) \mod 95 \\ =& 46^{-1} \begin{bmatrix} 86 & -22 \\ -22 & 15 \end{bmatrix} \mod 95 \end{aligned}$$

$$(\mathcal{A}\mathcal{A}^{\intercal})^{-1} = \begin{bmatrix} 6 & 78 \\ 78 & 85 \end{bmatrix} \mod 95.$$

Finally to get Pseduoinverse $A^{\dagger}$, multiplying $\mathcal{A}^{\intercal}$ and $(\mathcal{A}\mathcal{A}^{\intercal})^{-1}$ that is

$$A^{\dagger} = A^{\intercal}(\mathcal{A}\mathcal{A}^{\intercal})^{-1} = \begin{bmatrix} 1254 & 1438 \\ 162 & 1177 \\ 1206 & 2672 \\ 954 & 1254 \\ 1764 & 2494 \\ 78 & 85 \\ 978 & 1566 \end{bmatrix} \mod 95$$

$$\mathcal{A}^{\dagger} = \begin{bmatrix} 19 & 13 \\ 67 & 37 \\ 66 & 12 \\ 4 & 19 \\ 54 & 24 \\ 78 & 85 \\ 28 & 46 \end{bmatrix} \mod 95.$$

Since $\mathcal{A}$ is pseduoinverse, it can be used as the recatngular matrix key for the Hill cipher algorithm. This ensures that the key matrix $\mathcal{A}$ is appropriate and facilitates secure encryption and decryption in the Modified Hill cipher algorithm.

Encryption

Since the rectangular matrix key $\mathcal{A}$ is guaranteed to have full row ranks, we can now proceed with the encryption process using the Hill cipher. To encrypt the plaintext X using the key matrix $\mathcal{A}$ in the equation $Y = X\mathcal{A} \mod 95$, we need to divide the plaintext X into multiple matrices. Each of these matrices will contain the same number of elements as the number of rows in the rectangular key matrix $\mathcal{A}$. So, two elements will be in each rectangular matrix. The plaintext X is “Secret message” and their crossponding numerical codes given below.

S	E	C	R	E	T	$Space$	M	E	S	S	A	G	E
18	30	28	43	30	45	62	38	30	44	44	26	32	30

$$Y_1 = X_1\mathcal{A} \mod m$$

$$Y_1 = \begin{bmatrix} 18 & 30 \end{bmatrix} \begin{bmatrix} 1 & 14 & 19 & 3 & 8 & 0 & 7 \\ 16 & 1 & 14 & 12 & 22 & 1 & 12 \end{bmatrix} \mod 95$$

$$= \begin{bmatrix} 498 & 282 & 762 & 414 & 804 & 30 & 486 \end{bmatrix} \mod 95$$

$$= \begin{bmatrix} 23 & 92 & 2 & 34 & 44 & 30 & 11 \end{bmatrix} \mod 95.$$

$$Y_2 = \begin{bmatrix} 28 & 43 \end{bmatrix} \begin{bmatrix} 1 & 14 & 19 & 3 & 8 & 0 & 7 \\ 16 & 1 & 14 & 12 & 22 & 1 & 12 \end{bmatrix} \mod 95$$

$$= \begin{bmatrix} 716 & 435 & 1134 & 600 & 1170 & 43 & 712 \end{bmatrix} \mod 95$$

$$= \begin{bmatrix} 51 & 55 & 89 & 30 & 30 & 43 & 47 \end{bmatrix} \mod 95.$$

$$Y_3 = \begin{bmatrix} 30 & 45 \end{bmatrix} \begin{bmatrix} 1 & 14 & 19 & 3 & 8 & 0 & 7 \\ 16 & 1 & 14 & 12 & 22 & 1 & 12 \end{bmatrix} \mod 95$$

$$= \begin{bmatrix} 750 & 465 & 1200 & 630 & 1230 & 45 & 750 \end{bmatrix} \mod 95$$

$$= \begin{bmatrix} 85 & 85 & 60 & 60 & 90 & 45 & 85 \end{bmatrix} \mod 95.$$

$$Y_4 = \begin{bmatrix} 62 & 38 \end{bmatrix} \begin{bmatrix} 1 & 14 & 19 & 3 & 8 & 0 & 7 \\ 16 & 1 & 14 & 12 & 22 & 1 & 12 \end{bmatrix}$$

$$= \begin{bmatrix} 670 & 906 & 1710 & 642 & 1332 & 38 & 890 \end{bmatrix} \mod 95$$

$$= \begin{bmatrix} 5 & 51 & 0 & 72 & 2 & 38 & 35 \end{bmatrix} \mod 95.$$

$$Y_5 = \begin{bmatrix} 30 & 44 \end{bmatrix} \begin{bmatrix} 1 & 14 & 19 & 3 & 8 & 0 & 7 \\ 16 & 1 & 14 & 12 & 22 & 1 & 12 \end{bmatrix} \mod 95$$

$$= \begin{bmatrix} 734 & 464 & 1186 & 618 & 1208 & 44 & 738 \end{bmatrix} \mod 95$$

$$= \begin{bmatrix} 69 & 84 & 46 & 48 & 68 & 44 & 73 \end{bmatrix} \mod 95.$$

$$Y_6 = \begin{bmatrix} 44 & 26 \end{bmatrix} \begin{bmatrix} 1 & 14 & 19 & 3 & 8 & 0 & 7 \\ 16 & 1 & 14 & 12 & 22 & 1 & 12 \end{bmatrix} \mod 95$$

$$= \begin{bmatrix} 460 & 642 & 1200 & 444 & 924 & 26 & 620 \end{bmatrix} \mod 95$$

$$= \begin{bmatrix} 80 & 72 & 60 & 64 & 69 & 26 & 50 \end{bmatrix} \mod 95.$$

$$Y_7 = \begin{bmatrix} 32 & 30 \end{bmatrix} \begin{bmatrix} 1 & 14 & 19 & 3 & 8 & 0 & 7 \\ 16 & 1 & 14 & 12 & 22 & 1 & 12 \end{bmatrix} \mod 95$$

$$= \begin{bmatrix} 512 & 478 & 1028 & 456 & 916 & 30 & 584 \end{bmatrix} \mod 95$$

$$= \begin{bmatrix} 37 & 3 & 78 & 76 & 61 & 30 & 14 \end{bmatrix} \mod 95.$$

So, the Cipher text Y is

23 92 2 34 44 30 11 51 55 89 30 30 43 47 85 85 60 60 90 45 85 5 51 0 72 2 38 35 69 84 46 48 68 44 73 80 72 60 64 69 26 50 37 3 78 76 61 30 14 and its value is X_ CiseLz3(eerv%%88)t%FzA”Cmj;$uw?s[∼”8<;aylD|}9es.

Decryption

To decrypt Y using

$$Y = X\mathcal{A}^{-1} \mod 95.$$

We need to divide the ciphertext Y into multiple matrices. Each of these matrices will contain the same number of elements as the number of coloumn in the rectangular key matrix $\mathcal{A}$. So, seven elements will be in each rectangular matrix.

$$\mathcal{A}^{-1} = \begin{bmatrix} 19 & 13 \\ 67 & 37 \\ 66 & 12 \\ 4 & 19 \\ 54 & 24 \\ 78 & 85 \\ 28 & 46 \end{bmatrix}.$$

$$\begin{aligned} X_1 &= \begin{bmatrix} 23 & 92 & 2 & 34 & 44 & 30 & 11 \end{bmatrix} \begin{bmatrix} 19 & 13 \\ 67 & 37 \\ 66 & 12 \\ 4 & 19 \\ 54 & 24 \\ 78 & 85 \\ 28 & 46 \end{bmatrix} \mod 95 \\ &= \begin{bmatrix} 11893 & 8485 \end{bmatrix} \mod 95 \\ &= \begin{bmatrix} 18 & 30 \end{bmatrix}. \end{aligned}$$

$$\begin{aligned} X_2 &= \begin{bmatrix} 51 & 55 & 89 & 30 & 30 & 43 & 47 \end{bmatrix} \begin{bmatrix} 19 & 13 \\ 67 & 37 \\ 66 & 12 \\ 4 & 19 \\ 54 & 24 \\ 78 & 85 \\ 28 & 46 \end{bmatrix} \mod 95 \\ &= \begin{bmatrix} 16938 & 10873 \end{bmatrix} \mod 95 \\ &= \begin{bmatrix} 28 & 43 \end{bmatrix}. \end{aligned}$$

$$X_3 = \begin{bmatrix}85 & 85 & 60 & 60 & 90 & 45 & 85\end{bmatrix} \begin{bmatrix}19 & 13\\ 67 & 37\\ 66 & 12\\ 4 & 19\\ 54 & 24\\ 78 & 85\\ 28 & 46\end{bmatrix} \mod 95$$

$$= \begin{bmatrix}22260 & 16005\end{bmatrix} \mod 95$$

$$= \begin{bmatrix}30 & 45\end{bmatrix}.$$

$$X_4 = \begin{bmatrix}5 & 51 & 0 & 72 & 2 & 38 & 35\end{bmatrix} \begin{bmatrix}19 & 13\\ 67 & 37\\ 66 & 12\\ 4 & 19\\ 54 & 24\\ 78 & 85\\ 28 & 46\end{bmatrix} \mod 95$$

$$= \begin{bmatrix}7852 & 8208\end{bmatrix} \mod 95$$

$$= \begin{bmatrix}62 & 38\end{bmatrix}.$$

$$X_5 = \begin{bmatrix}69 & 84 & 46 & 48 & 68 & 44 & 73\end{bmatrix} \begin{bmatrix}19 & 13\\ 67 & 37\\ 66 & 12\\ 4 & 19\\ 54 & 24\\ 78 & 85\\ 28 & 46\end{bmatrix} \mod 95$$

$$= \begin{bmatrix}19315 & 14199\end{bmatrix} \mod 95$$

$$= \begin{bmatrix}30 & 44\end{bmatrix}.$$

$$\begin{aligned}X_6 &= \begin{bmatrix}80 & 72 & 60 & 64 & 69 & 26 & 50\end{bmatrix}\begin{bmatrix}19 & 13\\67 & 37\\66 & 12\\4 & 19\\54 & 24\\78 & 85\\28 & 46\end{bmatrix} \mod 95\\ &= \begin{bmatrix}17714 & 11806\end{bmatrix} \mod 95\\ &= \begin{bmatrix}44 & 26\end{bmatrix}.\end{aligned}$$

$$\begin{aligned}X_7 &= \begin{bmatrix}37 & 3 & 78 & 76 & 61 & 30 & 14\end{bmatrix}\begin{bmatrix}19 & 13\\67 & 37\\66 & 12\\4 & 19\\54 & 24\\78 & 85\\28 & 46\end{bmatrix} \mod 95\\ &= \begin{bmatrix}12382 & 7630\end{bmatrix} \mod 95\\ &= \begin{bmatrix}32 & 30\end{bmatrix}.\end{aligned}$$

So, the plaintext is $X = 18, 30, 28, 43, 30, 45, 62, 38, 30, 44, 44, 26, 32, 30$ crossponding with “Secret message”.

Chapter 4

Cryptanalysis Attack on the Hill Cipher Algorithm

The Modified Hill Cipher Algorithm by Alawiyah et al [11] uses a rectangular pseduoinvertible key matrix $\mathcal{A}$ for encryption and decryption. We observed that the scheme has serval security issues. Our study revealed that the scheme can be easily attacked using a known plaintext method.

The authors of "Generation of Rectangular Matrix for Hill Cipher Algorithm Using Playfair Cipher" claimed that such an attack cannot be mounted on their scheme because of the key matrix being rectangular. In this chapter a successful cryptanalysis is performed to break the scheme of Alawiyah et al [11].

4.1 General Model of the Attack

A known plaintext attack is mouted to recover the key used to encrypt the plaintext. This attack assumes that the attacker knows one or more pairs of plaintext and ciphertext pairs like

$$X_1, Y_1), (X_2, Y_2), (X_3, Y_3)...(X_k, Y_k). \tag{4.1}$$

To execute the attack, the attacker would first need to represent the plaintext and ciphertext pairs as matrices. Then, they would use linear equations to solve for the key matrix $\mathcal{A}$ that was used to encrypt the plaintext. The pseduoinverse $\mathcal{A}^{\dagger}$ is used to recover the plaintext X. Specifically, if the attacker has one plaintext-ciphertext pair, they can solve for the key matrix directly using matrix multiplication and modular arithmetic.

$$Y = \mathcal{A}X \mod m.$$

Because of known pairs, in (4.1), the attackers knowns Y and X and the only unknown is the matrix $\mathcal{A} = (a_{ij})$, $i = 1, ...n_1$ and $j = 1, ...n_2$ with unknowns $n_1 n_2$ unknowns (a_{ij}). Since the order of $\mathcal{A}$ is $n_1 \times n_2$, then the order of X must be $1 \times n_1$ and that of Y is $1 \times n_2$. So, equation (4.1) gives n_2 linear equations in $n_1 \times n_2$ unknowns. An other pair will result is more equations in the same unknowns. We continues with using known pairs to create enough linear equation to solve for all unknowns.

Attack 4.1.1. Key Recovery Attack

Input : Plaintext ciphertext pairs (X_k, Y_k).

Output : Rectangular key matrix $\mathcal{A}$

1. In a matrix based encryption scheme, the plaintext is divided into blocks, which are represented as matrices. The encryption process involves multiplying these plaintext with a key matrix to produced the crossponding ciphertext.

2. Gathering known plaintext-ciphertext pairs is a crucial step in preparing for a known plaintext attack. The attacker collects the pairs of original plaintext(unercypted message) along with their corresponding ciphertext resulting from the encryption algorithm.

3. The attacker needs to understand the encryption algorithm being used, specifically how the plaintext matrices are transformed into ciphertext matrices using the cryptographic key matrix. This could involve matrix multiplication, addition, modular arithmetic, and other mathematical operations.

4. The attacker attempts to derive equations based on the known plaintext-ciphertext pairs and the encryption algorithm.

5. Using the derived equations, the attacker aims to solve for the elements of the cryptographic key matrix.

6. Once the attacker successfully solves for the key matrix, they can use this key to decrypt other ciphertexts encrypted with the same key.

The attack is illustrated to follows by example.

For instance, of $n_1 = 2$ and $n_2 = 7$. The order of unknown matrix $\mathcal{A}$ will be 2×7

$$\mathcal{A} = \begin{bmatrix} a_{11} & a_{12} & a_{13} & a_{14} & a_{15} & a_{16} & a_{17} \\ a_{21} & a_{22} & a_{23} & a_{24} & a_{25} & a_{26} & a_{27} \end{bmatrix} \mod m$$

Every pair (X_1, Y_1) known $X_1 = (x_{11}...x_{17})$ and $y_{11}...y_{17}$ 3.1.1 to Chapter 3 . In each plaintext-ciphertext pairs (X_k, Y_k), one pair of X_k which has a order 1×2, $\mathcal{A} = 2 \times 7$ and one pair of Y_k which has a order 1×7.

$$Y = \begin{bmatrix} y_{11} & y_{12} & y_{13} & y_{14} & y_{15} & y_{16} & y_{17} \\ y_{21} & y_{22} & y_{23} & y_{24} & y_{25} & y_{26} & y_{27} \\ y_{31} & y_{32} & y_{33} & y_{34} & y_{35} & y_{36} & y_{37} \\ y_{41} & y_{42} & y_{43} & y_{44} & y_{45} & y_{46} & y_{47} \\ y_{51} & y_{52} & y_{53} & y_{54} & y_{55} & y_{56} & y_{57} \\ y_{61} & y_{62} & y_{63} & y_{64} & y_{65} & y_{66} & y_{67} \\ y_{71} & y_{72} & y_{73} & y_{74} & y_{75} & y_{76} & y_{77} \end{bmatrix}, X = \begin{bmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \\ x_{31} & x_{32} \\ x_{41} & x_{42} \\ x_{51} & x_{52} \\ x_{61} & x_{62} \\ x_{71} & x_{72} \end{bmatrix}$$

Divide the plaintext 1×2 each block and divide the ciphertext 1×7 each block. Multiplying the known plaintext with unknown key that is equal to ciphertext. Use the equation of Hill cipher algorithm.

$$Y = X\mathcal{A} \mod m$$

$$\begin{bmatrix} x_{11} & x_{12} \end{bmatrix} \begin{bmatrix} a_{11} & a_{12} & a_{13} & a_{14} & a_{15} & a_{16} & a_{17} \\ a_{21} & a_{22} & a_{23} & a_{24} & a_{25} & a_{26} & a_{27} \end{bmatrix} = \begin{bmatrix} y_{11} & y_{12} & y_{13} & y_{14} & y_{15} & y_{16} & y_{17} \end{bmatrix}$$

After multiplcation we get the linear equations that is

$$\begin{aligned}
x_{11}a_{11} + x_{12}a_{21} &= y_{11} \mod m \\
x_{11}a_{12} + x_{12}a_{22} &= y_{12} \mod m \\
x_{11}a_{13} + x_{12}a_{23} &= y_{13} \mod m \\
x_{11}a_{14} + x_{12}a_{24} &= y_{14} \mod m \\
x_{11}a_{15} + x_{12}a_{25} &= y_{15} \mod m \\
x_{11}a_{16} + x_{12}a_{26} &= y_{16} \mod m \\
x_{11}a_{17} + x_{12}a_{27} &= y_{17} \mod m \\
&\vdots
\end{aligned}$$

$$\begin{bmatrix} x_{71} & x_{72} \end{bmatrix} \begin{bmatrix} a_{11} & a_{12} & a_{13} & a_{14} & a_{15} & a_{16} & a_{17} \\ a_{21} & a_{22} & a_{23} & a_{24} & a_{25} & a_{26} & a_{27} \end{bmatrix} = \begin{bmatrix} y_{71} & y_{72} & y_{73} & y_{74} & y_{75} & y_{76} & y_{77} \end{bmatrix}$$

Mutiplying the both matrix then gets linear equations

$$\begin{aligned}
x_{71}a_{11} + x_{12}a_{21} &= y_{71} \mod m \\
x_{71}a_{12} + x_{12}a_{22} &= y_{72} \mod m \\
x_{71}a_{13} + x_{12}a_{23} &= y_{73} \mod m \\
x_{71}a_{14} + x_{12}a_{24} &= y_{74} \mod m \\
x_{71}a_{15} + x_{12}a_{25} &= y_{75} \mod m \\
x_{71}a_{16} + x_{12}a_{26} &= y_{76} \mod m \\
x_{71}a_{17} + x_{12}a_{27} &= y_{77} \mod m
\end{aligned}$$

Now, solve the linear equations and gets the values of unknown variables. On the encryption scheme, we use the Known Plaintext Attack On the encryption scheme, we use the known plaintext attack in the following way.

The computation example is illustrated is given below.

Example 4.1.2. The matrices of the plaintext and ciphertext are of the order 7×2 and 7×7 . Suppose the known X and Y matrices are as given below:

$$X = \begin{bmatrix} 18 & 30 \\ 28 & 43 \\ 30 & 45 \\ 62 & 38 \\ 30 & 44 \\ 44 & 26 \\ 32 & 30 \end{bmatrix}, Y = \begin{bmatrix} 23 & 92 & 2 & 34 & 44 & 30 & 11 \\ 51 & 55 & 89 & 30 & 30 & 43 & 47 \\ 85 & 85 & 60 & 60 & 90 & 45 & 85 \\ 5 & 51 & 0 & 72 & 2 & 38 & 35 \\ 69 & 84 & 46 & 48 & 68 & 44 & 73 \\ 80 & 72 & 60 & 64 & 69 & 26 & 50 \\ 37 & 3 & 78 & 76 & 61 & 30 & 15 \end{bmatrix}$$

Let the unknown key $\mathcal{A}$ of order 2×7 is given as

$$\begin{bmatrix} \mathcal{A}_1 & \mathcal{A}_2 & \mathcal{A}_3 & \mathcal{A}_4 & \mathcal{A}_5 & \mathcal{A}_6 & \mathcal{A}_7 \\ \mathcal{A}_8 & \mathcal{A}_9 & \mathcal{A}_{10} & \mathcal{A}_{11} & \mathcal{A}_{12} & \mathcal{A}_{13} & \mathcal{A}_{14} \end{bmatrix}$$

under arthematic modular 95.

Solution:

The Plaintext of order 7×2 are divided into different matrices which has the same order of all matrices that is 1×2 and the ciphertext of order 7×7 are divided into different matrices which has the same order of all matrices that is 1×7. Now , we are used some matrices of plaintext and ciphertext to find out the unknown key $\mathcal{A}$ by using known plaintext attack.

$$Y = X\mathcal{A} \mod 95$$

$$\begin{bmatrix} 23 & 92 & 2 & 34 & 44 & 30 & 11 \end{bmatrix} = \begin{bmatrix} 18 & 30 \end{bmatrix} \begin{bmatrix} \mathcal{A}_1 & \mathcal{A}_2 & \mathcal{A}_3 & \mathcal{A}_4 & \mathcal{A}_5 & \mathcal{A}_6 & \mathcal{A}_7 \\ \mathcal{A}_8 & \mathcal{A}_9 & \mathcal{A}_{10} & \mathcal{A}_{11} & \mathcal{A}_{12} & \mathcal{A}_{13} & \mathcal{A}_{14} \end{bmatrix}.$$

Multiplying the both matrix and we will get the linear equations.

$$18\mathcal{A}_1 + 30\mathcal{A}_8 = 23 \mod 95 \tag{4.2}$$

$$18\mathcal{A}_2 + 30\mathcal{A}_9 = 92 \mod 95 \tag{4.3}$$

$$18\mathcal{A}_3 + 30\mathcal{A}_{10} = 2 \mod 95 \tag{4.4}$$

$$18\mathcal{A}_4 + 30\mathcal{A}_{11} = 34 \mod 95 \tag{4.5}$$

$$18\mathcal{A}_5 + 30\mathcal{A}_{12} = 44 \mod 95 \tag{4.6}$$

$$18\mathcal{A}_6 + 30\mathcal{A}_{13} = 30 \mod 95 \tag{4.7}$$

$$18\mathcal{A}_7 + 30\mathcal{A}_{14} = 11 \mod 95. \tag{4.8}$$

$$\begin{bmatrix} 51 & 55 & 89 & 30 & 30 & 43 & 47 \end{bmatrix} = \begin{bmatrix} 28 & 43 \end{bmatrix} \begin{bmatrix} \mathcal{A}_1 & \mathcal{A}_2 & \mathcal{A}_3 & \mathcal{A}_4 & \mathcal{A}_5 & \mathcal{A}_6 & \mathcal{A}_7 \\ \mathcal{A}_8 & \mathcal{A}_9 & \mathcal{A}_{10} & \mathcal{A}_{11} & \mathcal{A}_{12} & \mathcal{A}_{13} & \mathcal{A}_{14} \end{bmatrix}$$

$$28\mathcal{A}_1 + 43\mathcal{A}_8 = 51 \mod 95 \tag{4.9}$$

$$28\mathcal{A}_2 + 43\mathcal{A}_9 = 55 \mod 95 \tag{4.10}$$

$$28\mathcal{A}_3 + 43\mathcal{A}_{10} = 89 \mod 95 \tag{4.11}$$

$$28\mathcal{A}_4 + 43\mathcal{A}_{11} = 30 \mod 95 \tag{4.12}$$

$$28\mathcal{A}_5 + 43\mathcal{A}_{12} = 30 \mod 95 \tag{4.13}$$

$$28\mathcal{A}_6 + 43\mathcal{A}_{13} = 43 \mod 95 \tag{4.14}$$

$$28\mathcal{A}_7 + 43\mathcal{A}_{14} = 47 \mod 95. \tag{4.15}$$

Now we will use the equation (4.2) and equation (4.9) and solve simultaneously and then get the $\mathcal{A}_1$ and $\mathcal{A}_8$. Multilying the equation 4.2 with 28 and multiplying equation (4.9) with 18 then we will obtain

$$504\mathcal{A}_1 + 840\mathcal{A}_8 = 644 \tag{4.16}$$

$$504\mathcal{A}_2 + 774\mathcal{A}_8 = 918 \tag{4.17}$$

Subtract the equations (4.16) from (4.17) and we get

$$66\mathcal{A}_8 = -274$$

$$\mathcal{A}_8 = 66^{-1}(-274) \mod 95$$

$$= 396 \mod 95$$

$$\mathcal{A}_8 = 16$$

Put the $\mathcal{A}_8$ in the equation (4.2)

$$\begin{aligned} 18\mathcal{A}_1 + 30(16) &= 23 \\ \mathcal{A}_1 &= 18^{-1}(-457) \\ \mathcal{A}_1 &= 1 \mod 95 \end{aligned}$$

Now we will use the equations (4.3) and (4.10) and find out the $\mathcal{A}_2$ and $\mathcal{A}_9$. First we will multiply equation (4.3) with 28 and equation (4.10) with 18 then gets the equations

$$504\mathcal{A}_2 + 840\mathcal{A}_9 = 2576 \tag{4.18}$$

$$504\mathcal{A}_2 + 774\mathcal{A}_9 = 990 \tag{4.19}$$

Subtract the equations (4.18) from (4.19) and we get

$$66\mathcal{A}_9 = 1586$$

$$\mathcal{A}_9 = 66^{-1}(1586) \mod 95$$

$$= 2376 \mod 95$$

$$\mathcal{A}_9 = 1$$

Put the $\mathcal{A}_9$ in the equation (4.3)

$$\begin{aligned}18\mathcal{A}_2 + 30(1) &= 92\\ \mathcal{A}_2 &= 18^{-1}(62)\\ &= 2294 \mod 95\\ \mathcal{A}_2 &= 14 \mod 95\end{aligned}$$

Now we will use the equations (4.4) and (4.11) and find out the $\mathcal{A}_3$ and $\mathcal{A}_{10}$. First we will multiply equation (4.3) with 28 and equation (4.10) with 18 then gets the equations

$$504\mathcal{A}_3 + 840\mathcal{A}_{10} = 56 \tag{4.20}$$

$$504\mathcal{A}_3 + 774\mathcal{A}_{10} = 89 \tag{4.21}$$

Subtract the equations (4.20) and (4.21) and we get

$$\begin{aligned}66\mathcal{A}_{10} &= -1546\\ \mathcal{A}_{10} &= 66^{-1}(69) \mod 95\\ &= 2484 \mod 95\\ \mathcal{A}_{10} &= 14\end{aligned}$$

Put the $\mathcal{A}_{10}$ in the equation (4.4)

$$\begin{aligned}18\mathcal{A}_3 + 30(14) &= 2\\ \mathcal{A}_3 &= 18^{-1}(-418)\\ &= 2109 \mod 95\\ \mathcal{A}_3 &= 19 \mod 95\end{aligned}$$

Now we will use the equation (4.5) and (4.12) and find out the $\mathcal{A}_4$ and $\mathcal{A}_{11}$. First we will multiply equation (4.5) with 28 and equation (4.12) with 18 then gets the equations

$$504\mathcal{A}_4 + 840\mathcal{A}_{11} = 952 \tag{4.22}$$

$$504\mathcal{A}_4 + 774\mathcal{A}_{11} = 540 \tag{4.23}$$

Subtract the equations (4.22) from (4.23) and we get

$$\begin{aligned} 66\mathcal{A}_{11} &= 412 \\ \mathcal{A}_{11} &= 66^{-1}(32) \mod 95 \\ &= 1152 \mod 95 \end{aligned}$$

$$\mathcal{A}_{11} = 12$$

Put the $\mathcal{A}_{11}$ in the equation (4.5)

$$18\mathcal{A}_4 + 30(12) = 34$$

$$\mathcal{A}_4 = 18^{-1}(-326)$$

$$\begin{aligned} &= 1998 \mod 95 \\ \mathcal{A}_4 &= 3 \mod 95 \end{aligned}$$

Now we will use the equation (4.6) and (4.13) and find out the $\mathcal{A}_5$ and $\mathcal{A}_{12}$. First we will multiply equation (4.6) with 28 and equation (4.13) with 18 then gets the equations.

$$504\mathcal{A}_5 + 840\mathcal{A}_{12} = 1232 \tag{4.24}$$

$$504\mathcal{A}_5 + 774\mathcal{A}_{12} = 540 \tag{4.25}$$

Subtract the equations (4.24) from (4.25) and we get

$$\begin{aligned}
66\mathcal{A}_{12} &= 692 \\
\mathcal{A}_{12} &= 66^{-1}(27) \mod 95 \\
&= 972 \mod 95 \\
\mathcal{A}_{12} &= 22
\end{aligned}$$

Put the $\mathcal{A}_{12}$ in the equation (4.6)

$$\begin{aligned}
18\mathcal{A}_5 + 30(12) &= 44 \\
\mathcal{A}_5 &= 18^{-1}(-326) \\
&= 1813 \mod 95 \\
\mathcal{A}_5 &= 8 \mod 95
\end{aligned}$$

Now we will use the equations (4.7) and (4.14) and find out the $\mathcal{A}_6$ and $\mathcal{A}_{13}$. First we will multiply equation (4.7) with 28 and equation (4.13) with 18 then gets the equations

$$504\mathcal{A}_6 + 840\mathcal{A}_{13} = 840 \tag{4.26}$$

$$504\mathcal{A}_6 + 774\mathcal{A}_{13} = 774 \tag{4.27}$$

Subtract the equations (4.26) and (4.27) and we get

$$\begin{aligned}
66\mathcal{A}_{13} &= 66 \\
\mathcal{A}_{13} &= 1 \mod 95
\end{aligned}$$

Put the $\mathcal{A}_{13}$ in the equation (4.7)

$$\begin{aligned}
18\mathcal{A}_6 + 30(1) &= 30 \\
18\mathcal{A}_6 &= 30 - 30 \\
\mathcal{A}_6 &= 0
\end{aligned}$$

Now we will use the equations (4.8) and (4.15) and find out the $\mathcal{A}_7$ and $\mathcal{A}_{14}$. First we will multiply equation (4.8) with 28 and equation (4.15) with 18 then gets the equations

$$504\mathcal{A}_7 + 840\mathcal{A}_{14} = 308 \tag{4.28}$$

$$504\mathcal{A}_7 + 774\mathcal{A}_{14} = 846 \tag{4.29}$$

Subtract the equations (4.28) from (4.29) and we get

$$\begin{aligned}
66\mathcal{A}_{14} &= -538 \\
\mathcal{A}_{14} &= 66^{-1}(32) \mod 95 \\
&= 36(32) \mod 95 \\
&= 1152 \mod 95 \\
\mathcal{A}_{14} &= 12
\end{aligned}$$

Put the $\mathcal{A}_{14}$ in the equation (4.8)

$$\begin{aligned}
18\mathcal{A}_7 + 30(12) &= 11 \\
\mathcal{A}_7 &= 18^{-1}(-349) \\
\mathcal{A}_7 &= 37(31) \\
&= 1147 \mod 95 \\
\mathcal{A}_7 &= 7 \mod 95
\end{aligned}$$

By using some part of plaintext “se” “cr” and and some part ciphertext “X _ C i s e L” “z 3 (e e r v” we find out the key($\mathcal{A}_1$ *to* $\mathcal{A}_{14}$)

$$\begin{bmatrix} \mathcal{A}_1 & \mathcal{A}_2 & \mathcal{A}_3 & \mathcal{A}_4 & \mathcal{A}_5 & \mathcal{A}_6 & \mathcal{A}_7 \\ \mathcal{A}_8 & \mathcal{A}_9 & \mathcal{A}_{10} & \mathcal{A}_{11} & \mathcal{A}_{12} & \mathcal{A}_{13} & \mathcal{A}_{14} \end{bmatrix} = \begin{bmatrix} 1 & 14 & 19 & 3 & 8 & 0 & 7 \\ 16 & 1 & 14 & 12 & 22 & 1 & 12 \end{bmatrix}$$

4.2 Drawback of Generation Rectangular Matrix

In the research “Generation of Recatngular Matrix Key for Hill Cipher Algorithm Using Playfair Cipher”[11] by Alawiyah et al, first the playfair algorithm is used to construct a rectangular matrix. This rectangular matrix is then used as rectangular pseduoinvertible key matrix for the proposed Modified Hill Cipher encryption scheme. However, the used of Hill Cipher is not necessary, as it adds nothing to the additional security of the scheme. If they had made the rectangular matrix randomly, it would still have the pseudoinverse-like properties that are useful for the Hill cipher. This means that using Playfair cipher is not required and can be seen as a disadvantage.

Chapter 5

Conclusion and Future Work Suggestion

5.1 Conclusion

In this section, we disscus the positive aspects and drawbacks of using the Hill cipher technique for encryption. The work of Alawiyah et al [11] generating a rectangular matrix key for the Hill cipher algorithm using the Playfair cipher using a simple and effective approach. The Playfair cipher can help with creating rectangular matrix keys more easily. This makes it simpler to remember and share the keys needed for the Hill cipher. When we use a rectangular matrix key, it makes the encoded message appear longer and more random, which helps hide the real message. As per author's claim, this extra randomness makes it harder for someone trying to crack the code to figure out the mathematical relationship between the encoded message and its matrix key. The resulting key matrix has desirable properties, such as its pseudoinverse and full row rank, which make it suitable for use in the Hill cipher.

In short, the Playfair cipher simplifies key creation the rectangular matrix key adds complexity to the encoded message, and this combination makes it tough for attackers to decipher the message's hidden patterns.

In **C**hapter 4, we dicussed a cryptanalysis of the given encryption scheme, which is $Y = \mathcal{A}X \mod 95$. It was observed that, the scheme is despite using a rectangular pseduoinverse key matrix attackable to known plaintext attacks. That is, an attacker who has access to some plaintext-ciphertext pairs can easily deduce the key matrix $\mathcal{A}$ using linear algebra.

It should also be noted that only plaintext-ciphertext pairs are be used for which the resulting system of equations could be solved modulo m. Recall that inverse of an integer $z \mod m$ is possible only $(z, m) = 1$.

In the next section of the paper, that we have suggest future work that could be done to improve the level of security of the encryption scheme against known plaintext attacks. One possible approach would be to use Key matrix modification. This would make it more difficult for an attacker to deduce the key matrix even if they have access to some plaintext-ciphertext pairs. Overall, we have recognize the limitations of the given encryption scheme and suggest that future work should focus on improving its security against known plaintext attacks.

5.2 Future Work

The present form of Modefied Hill cipher is still attackable to known plaintext attack. One possible improvement could be to improve. The encryption scheme in such way that the resulting equation become nonlinear in unknowns. Another approach could be the use of different algebraic structure like Galois field [31] or Tropical algebras [32]

Bibliography

[1] T. M. Damico, "A brief history of cryptography," *Inquiries Journal*, vol. 1, no. 11, 2009.

[2] C. J. Monico, *Semirings and semigroup actions in public-key cryptography.* University of Notre Dame, 2002.

[3] T. Satoh and K. Araki, "On construction of signature scheme over a certain non-commutative ring," *IEICE transactions on fundamentals of electronics, communications and computer sciences*, vol. 80, no. 1, pp. 40–45, 1997.

[4] B. Acharya, S. K. Panigrahy, S. K. Patra, and G. Panda, "Image encryption using advanced hill cipher algorithm," *International Journal of Recent Trends in Engineering*, vol. 1, no. 1, pp. 663–667, 2009.

[5] W. Stallings, *Cryptography and network security, 4/E.* Pearson Education India, 2006.

[6] T. Alawiyah, "Pemanfaatan kunjungan pohon biner pada kriptografi hill cipher kunci matriks persegi panjang," *IJCIT (Indonesian Journal on Computer and Information Technology)*, vol. 2, no. 1, 2017.

[7] Z. E. Dawahdeh, S. N. Yaakob, and R. R. bin Othman, "A new image encryption technique combining elliptic curve cryptosystem with hill cipher," *Journal of King Saud University-Computer and Information Sciences*, vol. 30, no. 3, pp. 349–355, 2018.

[8] K. A. Reddy, B. Vishnuvardhan, A. Krishna, *et al.*, "A modified hill cipher based on circulant matrices," *Procedia Technology*, vol. 4, pp. 114–118, 2012.

[9] A. Shostack, *Threat modeling: Designing for security.* John Wiley & Sons, 2014.

[10] R. Mahendran and K. Mani, "Generation of key matrix for hill cipher encryption using classical cipher," in *2017 World congress on computing and communication technologies (WCCCT)*, pp. 51–54, IEEE, 2017.

[11] T. Alawiyah, A. B. Hikmah, W. Wiguna, M. Kusmira, H. Sutisna, and B. K. Simpony, "Generation of rectangular matrix key for hill cipher algorithm using playfair cipher," vol. 1641, IOP Publishing, 2020.

[12] M. Müller-Olm and H. Seidl, "Analysis of modular arithmetic," in *Programming Languages and Systems: 14th European Symposium on Programming, ESOP 2005, Held as Part of the Joint European Conferences on Theory and Practice of Software, ETAPS 2005, Edinburgh, UK, April 4-8, 2005. Proceedings 14*, pp. 46–60, Springer, 2005.

[13] C. Kimberling, "A visual euclidean algorithm," *The Mathematics Teacher*, vol. 76, no. 2, pp. 108–109, 1983.

[14] C. A. Klein and C.-H. Huang, "Review of pseudoinverse control for use with kinematically redundant manipulators," *IEEE Transactions on Systems, Man, and Cybernetics*, no. 2, pp. 245–250, 1983.

[15] A. Bjerhammar, *Application of Calculus of Matrices to Method of Least Squares with Special Reference to Geodetic Calculations.* Kungl. tekniska högskolans handlingar, Lindståhl, 1951.

[16] R. Penrose, " gnralizd invr for matri," *Cambridg Philophial Soity Proding*, vol. 51, pp. 406–413, 1955.

[17] A. Ben-Israel and T. Greville, "General inverses 2nd ed. isbn: 0-387-00293-6," 2003.

[18] M. S. Iqbal, S. Singh, and A. Jaiswal, "Symmetric key cryptography: Technological developments in the field," *International Journal of Computer Applications*, vol. 117, no. 15, 2015.

[19] W. Stallings, “The advanced encryption standard,” *Cryptologia*, vol. 26, no. 3, pp. 165–188, 2002.

[20] S. William, *Cryptography and network security: For VTU.* Pearson education india, 2006.

[21] N. Bisht and S. Singh, “A comparative study of some symmetric and asymmetric key cryptography algorithms,” *International Journal of Innovative Research in Science, Engineering and Technology*, vol. 4, no. 3, pp. 1028–1031, 2015.

[22] W. Diffie and M. E. Hellman, “New directions in cryptography,” in *Democratizing Cryptography: The Work of Whitfield Diffie and Martin Hellman*, pp. 365–390, 2022.

[23] R. L. Rivest, A. Shamir, 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.

[24] A. Menezes, “Oorschot van, p. and vanstone, s.(1996)handbook of applied cryptography,” 1997.

[25] V. Pachghare, *Cryptography and information security.* PHI Learning Pvt. Ltd., 2019.

[26] C. Christensen, “Review of cryptography and network security: Principles and practice,” *Cryptologia*, vol. 35, no. 1, pp. 97–99, 2010.

[27] M. A. T. Shakil and M. R. Islam, “An efficient modification to playfair cipher,” *ULAB Journal of Science and Engineering*, vol. 5, no. 1, pp. 26–30, 2014.

[28] A. P. U. Siahaan, “Application of hill cipher algorithm in securing text messages,” 2018.

[29] M. S. Negron and P. U. O. P. R. S. JUAN, “Study of the hill cipher encryption/decryption algorithm,” 2012.

[30] A. Hidayat and T. Alawiyah, "Enkripsi dan dekripsi teks menggunakan algoritma hill cipher dengan kunci matriks persegi panjang," *Jurnal Matematika Integratif ISSN*, vol. 1412, p. 6184, 2013.

[31] C. Paar and J. Pelzl, *Understanding cryptography: a textbook for students and practitioners.* Springer Science & Business Media, 2009.

[32] S. T. Tesfay, "A glance at tropical operations and tropical linear algebra," 2015.

Turnitin Originality Report

A Key Recovery Attack on Modified Hill Encryption Scheme by Saliha Ameen

turnitin

From Ms Theses (CUST Library)

- Processed on 16-Nov-2023 12:35 PKT
- ID: 2229906525
- Word Count: 11497

Similarity Index
11%
Similarity by Source

Internet Sources:
8%
Publications:
6%
Student Papers:
5%

sources:

1 1% match (Internet from 20-Oct-2022)
https://repository.bsi.ac.id/index.php/unduh/item/331104/Merged-1-5.pdf

2 1% match (student papers from 16-Jan-2022)
Submitted to Higher Education Commission Pakistan on 2022-01-16

3 1% match (Damian Vizár, Serge Vaudenay. "Cryptanalysis of chosen symmetric homomorphic schemes", Studia Scientiarum Mathematicarum Hungarica, 2015)
Damian Vizár, Serge Vaudenay. "Cryptanalysis of chosen symmetric homomorphic schemes", Studia Scientiarum Mathematicarum Hungarica, 2015

4 1% match (Internet from 07-Feb-2023)
https://bibis.ir/science-books/information-technology/security/2022/Cryptography-and-Network-Security-Principles-and-Practice-Global-Edition-by-William-Stallings_bibis.ir.pdf

5 < 1% match (student papers from 04-Jun-2014)
Submitted to Higher Education Commission Pakistan on 2014-06-04

6 < 1% match (Internet from 03-Oct-2022)
https://dokumen.pub/cryptography-and-network-security-principles-and-practice-global-edition-7nbsped-1292158581-978-1292158587.html

7 < 1% match (Internet from 21-Mar-2023)
https://dokumen.pub/interference-management-in-wireless-networks-fundamental-bounds-and-the-role-of-cooperation-1107165008-9781107165007.html

8 < 1% match (student papers from 28-Apr-2023)
Submitted to University of West London on 2023-04-28

9 < 1% match (student papers from 01-May-2023)
Submitted to University of West London on 2023-05-01

10 < 1% match (student papers from 13-Nov-2015)
Submitted to KTH - The Royal Institute of Technology on 2015-11-13

11 < 1% match (Internet from 04-Feb-2023)
https://thesis.cust.edu.pk/UploadedFiles/Mariam%20Shoukat-MMT173026.pdf

12 < 1% match (student papers from 03-May-2023)
Submitted to American University of the Middle East on 2023-05-03

13 < 1% match (Internet from 16-Sep-2023)
https://ebin.pub/advances-in-cognitive-science-and-communications-selected-articles-from-the-5th-international-conference-on-communications-and-cyber-physical-engineering-iccce-2022-hyderabad-india-9811980853-9789811980855.html

14 < 1% match (Internet from 27-Oct-2021)
https://ebin.pub/cryptography-and-network-security-principles-and-practice-6thnbsped-0133354695-9780133354690.html