CAPITAL UNIVERSITY OF SCIENCE AND TECHNOLOGY, ISLAMABAD

# Cryptanalysis of the Encryption Scheme based on Advanced Hill Cipher Algorithm

by

Tooba Azam

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

in the

Faculty of Computing
Department of Mathematics

2020

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

# CERTIFICATE OF APPROVAL

## Cryptanalysis of the Encryption Scheme based on Advanced Hill Cipher Algorithm

by

Tooba Azam

(MMT181020)

## THESIS EXAMINING COMMITTEE

| S. No. | Examiner | Name | Organization |
|---|---|---|---|
| (a) | External Examiner | Dr. Munazza Naz | FJWU Rawalpindi |
| (b) | Internal Examiner | Dr. Qamar Mahmood | CUST Islamabad |
| (c) | Supervisor | Dr. Rashid Ali | CUST Islamabad |

Dr. Rashid Ali
Thesis Supervisor
May, 2020

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

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

# *Author's Declaration*

I, **Tooba Azam** hereby state that my MPhil thesis titled "**Cryptanalysis of the Encryption Scheme based on Advanced Hill Cipher Algorithm**" 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.

**(Tooba Azam)**

Registration No: MMT181020

# *Plagiarism Undertaking*

I solemnly declare that research work presented in this thesis titled "**Cryptanalysis of the Encryption Scheme based on Advanced Hill Cipher Algorithm**" 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.

**(Tooba Azam)**

Registration No: MMT181020

# *Acknowledgements*

First and foremost I would like to thank **Almighty Allah** the most merciful for all his blessings throughout my life, and for always being my strength and peace. To say that the past period that I have spent working on this thesis is a journey is a true understatement. I could not have achieved this much without the grace of **Almighty Allah**.

I am profoundly grateful to my generous supervisor **Dr. Rashid Ali** for his encouragement. He was always there whenever I found any problem. I really appreciate his efforts and guidance throughout my thesis and proud to be a student of such kind supervisor.

I would like to thank my affectionate teachers, **Dr. Muhammad Sagheer**, **Dr. Abdul Rehman Kashif**, **Dr. Shafqat Hussain**, **Dr. Muhammad Afzal** and **Dr. Rashid Ali** for their excellent teaching and support during these years.

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

I am thankful to all of my family members for becoming a bulwark of patience and support during my research work. However, my deepest gratitude is reserved for my Parents for their earnest prayers, unconditional love and unflinching support in completing my degree program. They supported and encouraged me throughout my life.

I would like to thank all of my friends for motivating me during my degree program. Mostly, I would like to thank Saadia Noor for her guidance during my research work. Also I would like to thank all my seniors for guiding me during my research journey.

Finally, I am obliged to all people who pray for me, share their knowledge during my degree program and support me.

**(Tooba Azam)**

Registration No: MMT181020

# *Abstract*

The Hill cipher algorithm is one of the symmetric key algorithms that have several advantages in data encryption. But, the inverse of the key matrix used for encrypting the plaintext does not always exist. If the key matrix is not invertible, then the encrypted text cannot be decrypted. In the Involutory matrix generation method, the key matrix used for the encryption is it's own inverse. So, at the time of decryption we need not to find the inverse of the key matrix. The article discussed in this thesis is image encryption using Advanced Hill cipher algorithm by Acharya et al. In this thesis we cryptanalyze novel advanced Hill (AdvHill) encryption technique, which uses an involutory key matrix. Our analysis shows that AdvHill technique is insecure. A major drawback of this scheme is, that, it encrypts the identical plaintext with identical ciphertext. The proposed scheme is not resistant against known plaintext attack.

# Contents

# List of Figures

# List of Tables

# Abbreviations

| | |
|---|---|
| **AdvHill** | Advanced Hill Cipher |
| **AES** | Advanced Encryption Standard |
| **DES** | Data Encryption Standard |
| **DSA** | Digital Signature Algorithm |
| **GCD** | Greatest Common Divisor |
| **RSA** | Rivest–Shamir–Adleman |

# Symbols

| | |
|---|---|
| $M$ | Plaintext or Message |
| $C$ | Ciphertext |
| $E$ | Encryption Algorithm |
| $D$ | Decryption Algorithm |
| $K$ | Key |
| $E_k$ | Encryption key |
| $D_k$ | Decryption key |
| $P_R$ | Private Key |
| $P_U$ | Public Key |
| $\mathbb{Z}$ | Set of Integers |
| $\mathbb{R}$ | Set of Real Numbers |
| $\mathbb{Z}_p$ | Finite Field Of Order Prime $p$ |

# Chapter 1

# Introduction

From ancient time to today, the secure transfer of private data over the public network is a big issue. There is a major need of secure channel for wireless networking and secret communication. Roman people knew some cryptographic methods and used the Shift Cipher or Caesar Cipher [1] while communicating with each other. Later, many ciphers were introduced for sending codes or secret messages. For example, monoalphabetical cipher [1, 2], polyalphabetical cipher [3], Playfair cipher, four square cipher, hill ciphers of different orders, etc. In this context, there are many contributions to cryptography.

Due to the advancement in network technology, security of the data is a big challenge. The rapid growth of technology extends to all areas of scientific research including digital image processing and transmission [4]. Popular use of multimedia technologies and enhanced network communication capacity slowly lead us to get clear and direct information through the images. In many fields, such as military, medical, industrial, digital, communication or even personal, millions of images are stored or transmitted every day via the Internet. The need to defend certain photos from unauthorized users has become a problem, depending on the application domain. Data security can be done by following various ways such as cryptography, watermarking and steganography etc [5].

## 1.1 Cryptography

It is a branch of cryptology, a science of secret communication which is used to alter the original message into unreadable form in the presence of a third-party over an insecure channel. The original message is called plaintext and the converted message is called ciphertext. To convert the plaintext into ciphertext an algorithm is needed and this is called an encryption algorithm. The algorithm that converts the ciphertext back into plaintext is called the algorithm for decryption. For encryption and decryption, cryptographic schemes need special information which is shared between sender and receiver, and is called a key. A cryptographic scheme that consists of a message space, a ciphertext space, a key space, an encryption algorithm and decryption algorithm is called a cryptosystem.

Cryptography is an art of transforming the meaningful message (plaintext) into the meaningless material (ciphertext) and then again re-transforming that meaningless message (ciphertext) back to its original meaningful message (plaintext). Modern cryptography is an art of science which is now considered as branch of mathematics and computer science. It uses sophisticated mathematical equations (algorithms) and also provides secrecy and integrity, and both authentication and anonymity to our data [6]. On the basis of keys, cryptography is divided into two main branches: Symmetric (Private) Key Cryptography and Asymmetric (Public) Key Cryptography.

In Symmetric (Private) Key Cryptography, only one key is used for both the data encryption and decryption. Sender and receiver are bound to share the key with each other for encryption and decryption of the data. For example: Data Encryption Standard (DES) [7], Double Data Encryption Standard (2DES), Triple Data Encryption Standard (TDES), Advanced Encryption Standard (AES) [8] and Blowfish [9].

In 1976, Whitfield Diffie and Martin Hellman introduced a new scheme known as asymmetric key cryptography, also known as public key cryptography. In Asymmetric (Public) Key Cryptography [10], two keys are used in which, one is for data encryption and the other is used for decryption. A person generates two keys one is kept secret, called secret key, and the other key is made public, called the public key. Anyone can encrypt data since the encryption key is public but only the person having the decryption key can decrypt the data because decryption key is private. Sender encrypts original text using public key and encryption algorithm to obtain cipher text. The secret key and decryption algorithm are used to obtain original text. Examples are: RSA [11], DSA, ELGamal [12], Diffie-Hellman key exchange [13] and Elliptic curve cryptosystem [14].

## 1.2 Cryptanalysis

There is also another branch of cryptology known as cryptanalysis. Cryptanalysis is an art of breaking a cryptosystem. Code breaking is usually considered to be a crime and there is a consideration that it should not be added as the main class of scientific discipline. Many researchers put their own contribution to the field of cryptanalysis. We may not judge the security of any cryptosystem without any attempt to break the cryptosystem. There are number of cryptographic attacks: Brute force attack [15], a trial-and-error cryptanalytic attack for attempting to decrypt any encrypted data. An attacker tries different usernames and password again and again until it breaks without taking any advantage of other weaknesses in an encryption system. Chosen ciphertext attack [16], attacker tries to unveil the secret key with random ciphertext. Chosen plaintext attack [17], like chosen ciphertext attack attacker chooses random plaintext and recover the key. Known plaintext attack [18], hidden key is retrieved with the information of plaintext and corresponding ciphertext. Ciphertext only attack [19], attacker has information about ciphertext and algorithm. He recovers the key as well as the plaintext. Algebraic attack [20], in this attack, attacker uses his information in algebraic expression and break the scheme to reveal the key. Birthday attack [21] in probability theory is a type of cryptographic attack that belongs to a class of brute force attacks. Birthday attack can even be used to find collisions for hash functions. It exploits the math behind the birthday problem. This assault may be used to exploit contact between two parties or more.

## 1.3 Current Research

In this research, we focused on "Image Encryption Using Advanced Hill Cipher Algorithm" by Acharya et al [22]. They proposed it with Two-level Hill cipher under modular arithmetic. Hill cipher is based on manipulation of the matrix. In this article, they used the arithmetic that satisfies the mathematical operations: the addition, the subtraction, the multiplication and the division. Also,they proposed the involutory key generation algorithm. They used the involutory matrices over $\mathbb{Z}_p$ in their scheme. The use of an involutory matrix makes the decryption process efficient as the inverse of an involutory matrix is the matrix itself. The Hill cipher is vulnerable to a known plaintext attack. Therefore in [22] Acharya et al proposed a new symmetric sncryption scheme called Advanced hill cipher (AdvHill) algorithm using involutory matrices. We mainly focused on working of the encryption scheme and investigating its resistance against known attacks. For this purpose, we have used involutory key generation algorithm and proposed AdvHill technique to cipher and encipher the data. We constructed algebra based structures which have some kind of periodicity and symmetry.
By using known plaintext-ciphertext pairs with an unknown involutory key, a system of non-linear algebraic equation is formulated. The analysis shows that the proposed Advanced Hill encryption scheme has security flaws. In fact, the solution of algebraic system resulted in the recovery of secret key. We have developed codes and algorithms using computer algebra software "ApCoCoA" [23] for effective computations.

## 1.4 Thesis Layout

The thesis is composed as follows:

In *Chapter*1, we have discussed the idea of cryptography, cryptographic background and presented the introduction of the basic terms related to our thesis.

In *Chapter*2, we discussed the fundamental ideas and definition of cryptography and mathematical terms related to our work. In the form of sections, the brief description of the cryptology, cryptography, purpose of cryptography, cryptanalysis, modular arithmetic and Hill cipher is discussed.

In *Chapter*3, we have presented the review of "Image Encryption Using Advanced Hill Cipher Algorithm" by Acharya et al [22]. For that purpose we discussed the concepts of Hill Cipher, Modular Arithmetic, Involutory Matrix and Image Encryption Using AdvHill Technique scheme with the help of examples and the calculation are performed with the help of Computer algebra system "ApCoCoA"[23].

In *Chapter*4, we have presented a cryptanalysis of the "Image Encryption Using Advanced Hill Cipher Algorithm" scheme. Furthermore, we have described the concepts of scheme with the help of examples. All the calculation are performed with the help of Computer Algebra System "ApCoCoA".

Finally the conclusion is presented in *Chapter*5.

# Chapter 2

# Preliminaries

In this chapter, we will discuss the basic ideas and definitions of cryptography. Introduction of classical cipher and cryptanalysis is briefly described. The mathematical background is also discussed in this chapter.

The word "**cryptology**"[24] is a combination of two Greek words **kryptos** (hidden) and **logos** (words). Cryptology is a mathematical science that secure data for communication. It has further two branches: (1). Cryptography and (2). Cryptanalysis as shown in Figure 2.1.

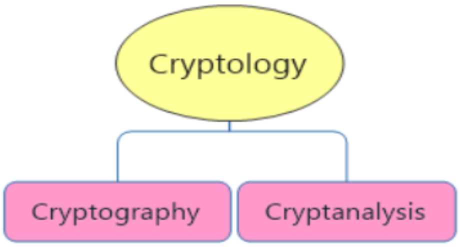

FIGURE 2.1: Types of Cryptology

## 2.1 Cryptography

Cryptography is the branch of cryptology. It is also originated from Greek word **kryptos** (hidden) and **graphein** (to write). Cryptography [7] is a science and secure art which transforms original data into the coded disguise form and only readable for the intended person. It will be very difficult for third person to read or understand the original data. The sender remodels the original data or **Plaintext** $M$ such as messages, audio or video into muddled data or **Ciphertext** $C$. A system in which original data (plaintext) is converted into muddled data (ciphertext) by using encryption algorithm and converting back muddled data (ciphertext) into original data (plaintext) by using decryption algorithm is known as cryptosystem. This encryption and decryption is done by using a secret key $K$ as shown in Figure 2.2. Cryptosystem has five basic components:

1. Plaintext Space $M$
2. Ciphertext Space $C$
3. Encryption algorithm $E$
4. Decryption Algorithm $D$
5. Key $K$

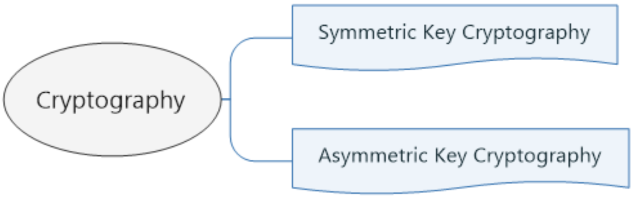

FIGURE 2.2: Cryptography

### 2.1.1 Purpose of Cryptography

In cryptography two parties Bob and Alice have to communicate with each other. Alice as sender sends original data to Bob as ciphertext. Ciphertext is not the original data, it is disguised by the encryption method in the form of ciphertext. Bob, the receiver, receives the encoded data and decode it by decryption method converting back to original plaintext and vice versa. This all process is mainly depends on a key which is kept secret. So the main purposes of cryptography [25] are below:

1. **Confidentiality:** Confidentiality implies the data confidentiality and privacy. The sender and receiver knows the original information about the data and no one can understand the transmitted information. And confidentiality is, if anyone knows the secret information but still unable to get the original data.

2. **Integrity:** It assures the receiver that the information transmitted to him is not changed, either viciously or accidentally. That is, he received the original transmitted information and no one other than sender and receiver can change the data.

3. **Authentication:** Authentication provides:

   ***i.*** **Source Authentication:** It is used to verify the identities of both sender and receiver or of the system which created the information.

   ***ii.*** **Integrity Authentication:** It is used to verify that the communication between sender and receiver is not controlled by any unauthorized person.

4. **Access control:** It is identification authentication and authorization of individual users which communicate with each other and credentials.

5. **Anonymity:** This is the property which secure the identity of users and data from the attackers who are trying to discover the communication data.

6. **Non-Repudiation:** It assures that the communicator (sender or receiver) cannot deny about the delivered information at any stage. It is a legal concept in the world of cryptography which provides the origin and integrity of data. In any cryptosystem, it helps sender and receiver to trust each other.

### 2.1.2 Types of Cryptography

Cryptography is categorized into two major types based on key distribution as shown in Figure 2.3:

- Symmetric Key Cryptography (Secret Key Cryptography)
- Asymmetric Key Cryptography (Public Key Cryptography)

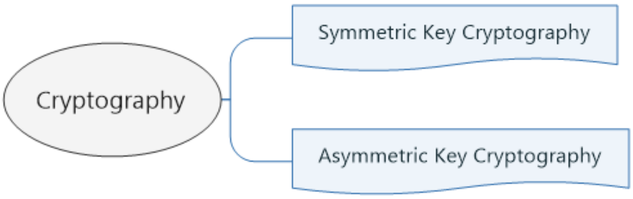

FIGURE 2.3: Types of Cryptography

### 2.1.3 Symmetric Key Cryptography

Symmetric key cryptography (symmetric encryption) [26] is known as secret or private key cryptography. It uses only one key to perform encryption or decryption algorithm as shown in Figure 2.4. In symmetric encryption, a set of information that is used with an algorithm to encrypt and decrypt the data in a symmetric encryption is called secret key. It is also known as **private key**. It can be shared between two parties through secure channel, it is neither shared publicly nor unauthorized channel. The key is private and shrouded from attackers. Examples are: Data Encryption Standard (DES) [7], Double Data Encryption Standard (2DES), Triple Data Encryption Standard (TDES), Advanced Encryption Standard (AES) [8] and Blowfish [9].

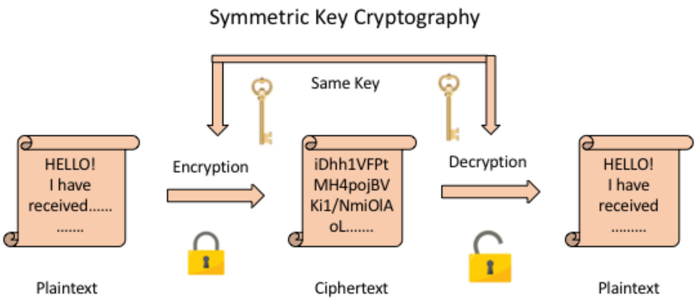

Figure 2.4: Symmetric Key Cryptography

## 2.1.4 Classical Symmetric Cipher

An algorithm used for transforming an original message (intelligible message) into one that is un-understandable (unintelligible) by using different methods. A symmetric cryptographic algorithm used to encrypt the data which operates on a fixed size of $n$-bits of data, as a group, at a time using a shared secret key is known as block cipher. If the data is larger than the fixed size block, it will be further divided into several blocks and encrypted in the same way. Block ciphers is same as polyalphabetic ciphers. Electronic Code Book (ECB) is the easiest algorithm of block cipher. Classical ciphers are cryptographic algorithms that were used in the history and were practically computed and solved by hand, where it was used by bodger. But on other hand, it was also used by armies to secure their top level information and communication. There are two key components of classical ciphers: 1. Transposition cipher and 2. Substitution cipher.

**Definition 2.1.1. (Transposition Cipher)**
Transposition cipher encrypts original plaintext to ciphertext by moving around the letters or symbols of original plaintext [27]. The plaintext letters or symbols are reordered in some way.

**Definition 2.1.2. (Substitution Cipher)**
Substitution cipher encrypts original data to ciphertext by swapping units in data (generally single letters, pairs of letters, triplets of letters, mixtures of the above, and so on) by different units of symbol as directed by the key.

**Definition 2.1.3. (Inverse Substitution)**
The receiver decrypts ciphertext to its original form by following the algorithm. The units of the recovered original text are reserved in the same sequence as in the ciphered data. The process is known as inverse substitution [28].

**Definition 2.1.4. (Monoalphabetic Substitution Cipher)**
Monoalphabetic substitution cipher encrypts original message on a fixed replacement structure/algorithm *i.e* the substitution is fixed for each letter of alphabet. This is also known as simple substitution cipher. One of the popular example of monoalphabetic substitution cipher is the Caesar cipher [1].

**Definition 2.1.5. (Polyalphabetic Substitution Cipher)**
Polyalphabetic Cipher is a substitution cipher that encrypts plaintext to ciphertext by using multiple substitution alphabets. In polyalphabetic substitution Cipher, during encryption process, the cipher alphabet for the plain alphabet, different alphabets are used depending on their position.

**Example 2.1.** An example of polyalphabetic substitution cipher is vigenère cipher. Here we encrypt the word "RIGHT". The letter 'R' in the left column of Table 2.1 is mapped to the next column headed by 'A' which results 'R', second letter 'I' in the left column traced to the next second column headed by 'B' results 'J' and so on. The word "RIGHT"encrypted to "RJIKX".

"

| | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| A | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| B | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A |
| C | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B |
| D | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C |
| E | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D |
| F | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E |
| G | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F |
| H | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G |
| I | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H |
| J | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I |
| K | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J |
| L | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K |
| M | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L |
| N | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M |
| O | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N |
| P | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O |
| Q | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P |
| R | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q |
| S | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R |
| T | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S |
| U | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T |
| V | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U |
| W | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V |
| X | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W |
| Y | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X |
| Z | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y |

Table 2.1: Polyalphabetic substitution cipher:vigenère cipher

”

**Definition 2.1.6. (Homophonic Substitution Cipher)**

A substitution cipher which involves replacing each letter of plaintext with a variety of different ciphertext letters or the symbols. The point of offering number of potential substitutes is proportional to the frequency of the letter or symbols, constitutes roughly about 1% of the ciphertext.

**Example 2.2.** Let the cipher alphabets as in following Table 2.2

Let the plaintext “CHOOSE THE DIFFERENT LETTERS”, to encipher we use the above table. From the above table, we find that ‘*C*’ is replaced by the letter below it *i.e* ‘*F*’. The next letter is ‘*H*’ which will be replaced by the letter choosed randomly as cipher *i.e* ‘*C*’. The third letter, ‘*O*’ is frequently used in English so it provides us several choices in cipher *i.e* ‘0’ or ‘8’. We choose any one from

| | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| *A* | *B* | *C* | *D* | *E* | *F* | *G* | *H* | *I* | *J* | *K* | *L* | *M* | *N* | *O* | *P* | *Q* | *R* | *S* | *T* | *U* | *V* | *W* | *X* | *Y* | *Z* |
| *L* | *X* | *F* | *S* | *Z* | *H* | *E* | *C* | *V* | *T* | *I* | *P* | *G* | *A* | *Q* | *D* | *K* | *J* | *R* | *O* | *W* | *U* | *M* | *Y* | *N* | *B* |
| “9 | | | | 2 | | | | 3 | | | | | 5 | 0 | | | | 4 | 6 | | | | | | ” |
| | | | | 7 | | | | | | | | | | 8 | | | | | | | | | | | |
| | | | | 1 | | | | | | | | | | | | | | | | | | | | | |

TABLE 2.2: Homophonic substitution cipher

these randomly, say ‘8’ similarly for ‘*S*’. But the letter ‘*E*’ has more choices to be replaced as it has ‘*Z*’, ‘7’, ‘2’ or ‘1’ and so on.

**Plaintext:** CHOOSE THE DIFFERENT LETTERS

**Ciphertext:** FC80RZ UC7 9VEE1J2A6 P7U6ZJ4

### 2.1.5 Asymmetric Key Cryptography

Asymmetric Key Cryptography (asymmetric encryption) is public key cryptography. This encryption comes out with keys in pair where one is known to everyone(it is publicly available and can be passed over the internet) is called **public key** [13] and other is hidden or kept secret is called **private key**. The private key of one is used for encryption while public key is used for decryption by the other entity as shown in Figure 2.5. The plaintext $(M)$ is encrypted with the help of encryption algorithm $(E)$ and public key $(PU)$ of the receiver and coverted in ciphertext $(C)$, after receiving the ciphertext, receiver will use his own private key $(PR)$ and will decrypt the encoded message via decryption algorithm. The structure is given below:

$$C = E(P_U, M) \tag{2.1}$$

$$M = D(P_R, C). \tag{2.2}$$

Examples for Asymmetric Key Cryptography [10] are: RSA [11], DSA, ELGamal [12], Diffie-Hellman key exchange [13] and Elliptic curve cryptosystem [14].

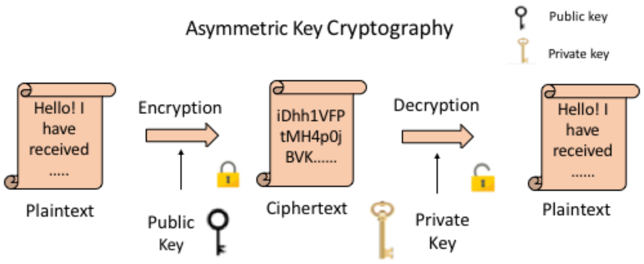
Asymmetric Key Cryptography
Public key
Private key
Hello! I have received ......
Plaintext
Encryption
Public Key
iDhh1VFP tMH4p0j BVK......
Ciphertext
Decryption
Private Key
Hello! I have received ......
Plaintext

Figure 2.5: Asymmetric Key Cryptography

## 2.2 Cryptanalysis

The process of breaking cryptosystem to get forged information out of the encrypted data is called an attack on the system [29]. The main objective of this attack is to encounter the unknown key $K$ and also the hidden original data even if the main algorithm is unable to decipher. The process of attack is known as **cryptanalysis**. And the person who takes out the whole above process is known as **cryptanalyst**. To make a good cryptanalyst it takes a successful blend of persistence, mathematics, intuition, inquisitiveness, and a working computer. When there is any weakness found in cryptosystem, the crypanalyst does his job. Either any of the property is compromised: confidentiality, integrity, authentication, access control, anonymity or non-repudiation [30]. Crypatanalysis is performed by two main attacks, active attack and passive attack. In order to conduct cryptanalysis, cryptanalyst has to defeat some cryptographic mechanism.

1. **Passive Attack**

   In this attack [31], cryptanalyst individually attempts to break the system based on observed data and cannot interact with any of the communicator.

2. **Active Attack**

   In this attack [32], cryptanalyst changes the communication. He tries to uncloak the key and may create, forge, alter, replace, block or reroute communication.

There are many attacks in cryptography, some of them are discussed here.

### 2.2.1 Ciphertext Only Attack

An attacker has the access to ciphertext and the encryption algorithm. He uses the ciphertext to obtain plaintext and secret key. Mostly, the attacker has no information about the original data but he continuously tries to unveil the original data by using ciphertext attack. Frequency analysis is very helpful in ciphertext attack [19].

only.jpg only.jpg only.jpg only.jpg only.jpg only.jpg only.jpg only.jpg only.jpg

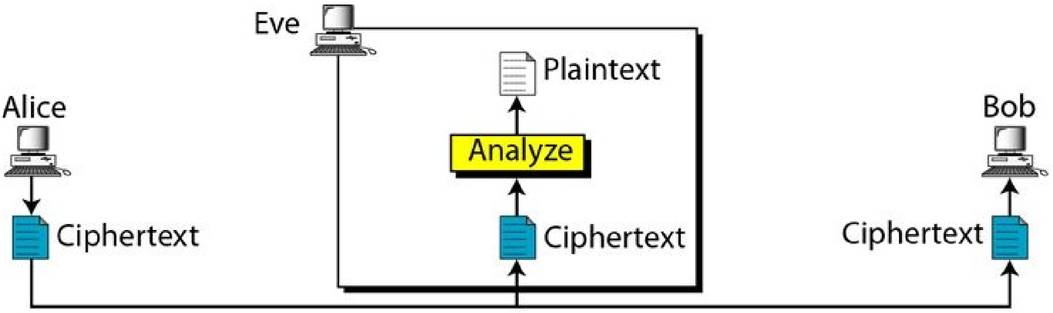

FIGURE 2.6: Ciphertext Only Attack [33]

### 2.2.2 Known Plaintext Attack

Here attacker has some information about the plaintext as well as its corresponding ciphertext. In this case, he tries to recover the key to decipher any further information by using previous information [18].

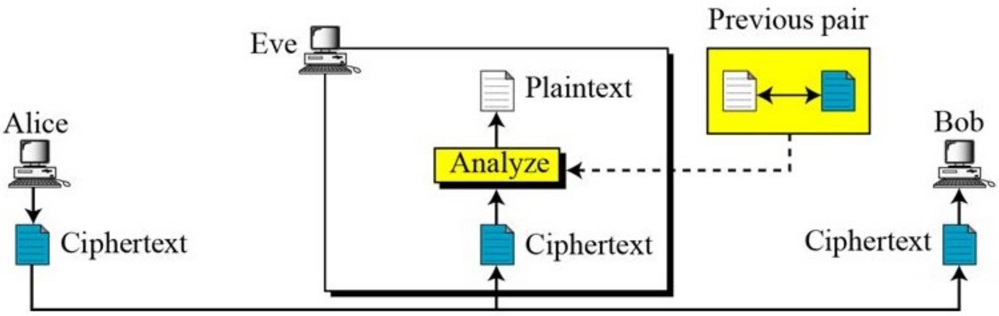

FIGURE 2.7: Known Plaintext Attack [33]

### 2.2.3 Chosen Plaintext Attack

For cryptanalysis, attacker chooses random plaintext to encrypt and tries to obtain corresponding ciphertext. By ciphertext and plaintext information, attacker can regain the key [30]. The goal of such attack is to obtain more information about cryptosystem which reduces the security of encryption scheme.

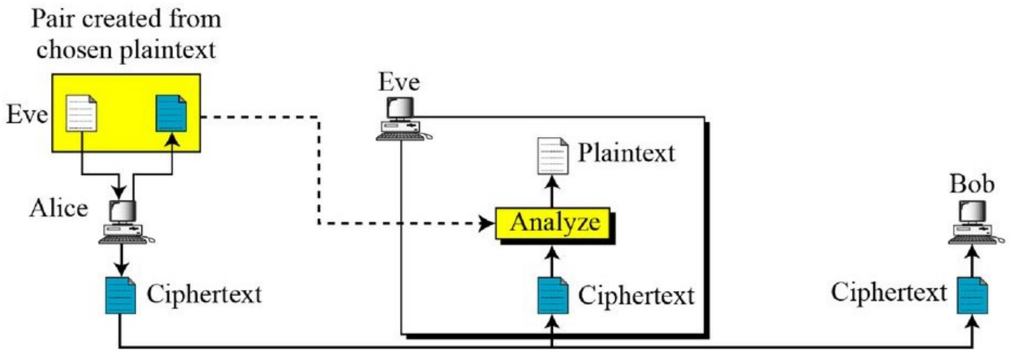

FIGURE 2.8: Chosen Plaintext Attack [33]

### 2.2.4 Chosen Ciphertext Attack

For cryptanalysis, cryptanalyst chooses random ciphertext [17], same as chosen plaintext, to decrypt and tries to obtain plaintext. He tries to recover the secret key from the obtained information [16].

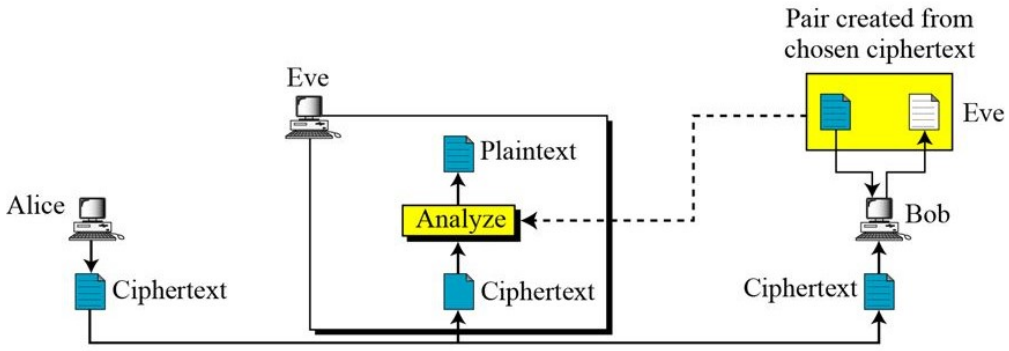

FIGURE 2.9: Chosen Ciphertext Attack [33]

### 2.2.5 Brute Force Attack

The attacker tries to reveal original data from ciphertext by trying all the possible keys. Larger the key size, harder to attempt this attack [15].

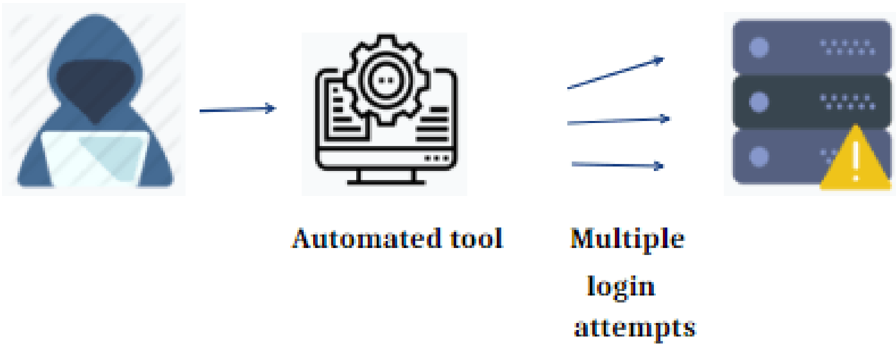

FIGURE 2.10: Brute Force Attack [34]

### 2.2.6 Algebraic Attack

If the attacker has information about ciphertext and plaintext then he can break the cipher to unveil the secret key. In this attack, attacker expresses the cipher operation mode as a set of equations then solve it to obtain the key [20] or some information regarding plaintext.

## 2.3 Mathematical Background

In this section, we will discuss some mathematical definitions that will be used throughout the thesis.

**Definition 2.3.1. (Algorithm)**
Algorithm is a finite sequence of well-defined set of instructions designed to perform specific task. Following the algorithm, step by step, the recurrent problem can be solved.

**Definition 2.3.2.** $\big($**Euclidean Algorithm**$\big)$

An algorithm used to find the greatest common divisor (gcd) of two integers $a$ and $b$. The greatest common divisor (gcd) is the largest possible number that completely divides both numbers without leaving any remainder. Euclidean algorithm is based on the fact *i.e.*

$$gcd(a, b) = gcd(b, r)$$

**Definition 2.3.3.** $\big($**Extended Euclidean Algorithm**$\big)$

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

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

**Algorithm 2.3.4.** $\big($**Extended Euclidean Inverse Algorithm**$\big)$

**Input:** An integer $r$ and modulo $m$.

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

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

**Definition 2.3.5.** **(Involutory Matrix)**

"Matrix $A$ is called involutory matrix if the matrix $A$ is it's own inverse. The multiplication by matrix $A$ is an involution iff $A^2 = I$."

**Definition 2.3.6.** **(Ring)**

The **Ring** [35] denoted by $(R, +, .)$ is the set of elements embedded with two binary operations addition "+" and multiplication "·" that satisfies the following axioms:

1. $(R, +)$ is an abelian group.
2. $(R, \cdot)$ is monoid.
3. Left and right distributive laws of multiplication with respect to addition hold in $R$.

**Example 2.3.** Some examples of ring are given below.

***i.*** Set of integers $\mathbb{Z}$ under addition " + " and multiplication " · " is a ring.

***ii.*** Let $\mathbb{Z}_p = \{0, 1, 2, ...p - 1\}$ and $p > 0$ and $p \in \mathbb{Z}$ is a ring under addition and multiplication modulo $p$.

***iii.*** The set of all $n \times n$ matrices with real entries under the usual matrix addition and multiplication forms a ring.

## 2.4 Modular Arithmetic

Modulus (abbreviated as "*mod*") is originated from the Latin word *modulus* means "remainder, residue"or more in "what is left after parts of the whole are taken". Thus, "modular"or "mod arithmetic" is really "remainder arithmetic". Modular arithmetic is the mathematical concept which plays a central role in cryptography. Almost all cipher from the Caesar Cipher to the RSA Cipher used it. A system of arithmetic for integers, where numbers "wrap" around when reaching a certain value, the modulus. Modular arithmetic is widely used in computer science and cryptography [36]. “Let $p$, $x$ and $y$ be integers. $a$ is congruent to $b \mod p$ if $p \mid a - b$”[37].

The following are some statements which equates the term $p \mid a - b$:

- $p \mid b - a$
- $a - b = kp$ for some $k \in \mathbb{Z}$

The set of the integers congruent to $a \quad modulo \quad p$, is called the congruence class. Here are some operations of Modular Arithmetic: “

1. $a \equiv b \mod p$
2. $a \equiv a \mod p$ **(Reflexivity)**
3. $a \equiv b \mod p \implies b \equiv a \mod p$ **(Symmetry)**
4. $a \equiv b \mod p \quad and \quad b \equiv c \mod p \implies a \equiv c \mod p$ **(Transitivity)**

”Here are the arithmetic operations addition, subtraction, unary, multiplication and division described under the modular. “Let $\mathbb{Z}_p = [0, 1, ..., p - 1]$ the set of residue modulo $p$. If the modular arithmetic is performed within the set $\mathbb{Z}_p$, the following arithmetic operations will occur:

1. **Addition:**

$$(a + b) \mod p \equiv [a \mod p + b \mod p] \mod p$$

2. **Negation:**

$$-a \mod p \equiv p - (a \mod p)$$

3. **Subtraction:**

$$(a - b) \mod p \equiv [a \mod p - b \mod p] \mod p$$

4. **Multiplication:**

$$(a * b) \mod p \equiv [a \mod p * b \mod p] \mod p$$

5. **Division:**

$$(a/b) \mod p \equiv c \quad when \quad a \equiv (b * c) \mod p$$

The following represents the properties of modular arithmetic:

- **Commutative Law:**

$$(w + x) \mod p = (x + w) \mod p$$

$$(w * x) \mod p = (x * w) \mod p$$

- **Associative Law:**

$$[(w + x) + y] \mod p = [w + (x + y)] \mod p$$

- **Distribution Law:**

$$[w * (x + y)] \mod p = [(w * x) \mod p * (w * y) \mod p] \mod p$$

- **Identities:**

$$(0 + a) \mod p = a \mod p$$

and

$$(1 * a) \mod p = a \mod p$$

- **Inverses:**

For apiece $x \in \mathbb{Z}_p, \exists y$ such that
$(x + y) \mod p = 0 then y = -x$

For apiece $x \in \mathbb{Z}_p, \exists y$ such that
$(x * y) \mod p = 1$

”

## 2.5 Hill Cipher

In 1929, the mathematician Lester S. Hill invented Hill Cipher. The basic and most important part of Hill cipher is matrix management. Hill cipher operates on groups of symbols like the digraphic ciphers. It is extended to work on different size of blocks of symbols and technically polygraphic substitution cipher. The Hill cipher is a monoalphabetic polygraphic substitution cipher, it was the first monoalphabetic polygraphic cipher which operates on more than three symbols simultaneously. Hill cipher, a blocked cipher, uses a main area of mathematics which is called **Linear Algebra** and the user must have elementary knowledge of matrices. It also uses mathematical area **Modular Arithmetic**. From the areas used by Hill cipher, it has substantially more mathematical nature than any other. For encryption or decryption, algorithm takes $m$ successive letters as input and substitutes $m$ ciphered or deciphered letters as output. In Hill cipher, all 26 alphabets are assigned a numerical value from 0 to 25[7, 38].

“ Hill cipher represents the encryption by

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

”

Table 2.3: Encoding Scheme

$$C = KP \qquad \mod 26$$

where $C$ represents ciphertext, $P$ represents plaintext and both are column vector of length $m$. And $K$ represents the key used for encryption which is a square matrix of order $m \times m$. All operations of the algorithm are performed modulo 26. For $m = 3$, the plaintext letters $P_1, P_2, P_3$, the corresponding ciphertext letters $C_1, C_2, C_3$ and $3 \times 3$ key can be depicted as follows:

$$\begin{pmatrix} C_1 \\ C_2 \\ C_3 \end{pmatrix} = \begin{pmatrix} K_{11} & K_{12} & K_{13} \\ K_{21} & K_{22} & K_{23} \\ K_{31} & K_{32} & K_{33} \end{pmatrix} \begin{pmatrix} P_1 \\ P_2 \\ P_3 \end{pmatrix} \qquad \mod 26$$

The plaintext letters corresponding to the ciphertext letters result in 3 linear equations.

$$C_1 = (K_{11}P_1 + K_{12}P_2 + K_{13}P_3) \qquad \text{mod } 26$$

$$C_2 = (K_{21}P_1 + K_{22}P_2 + K_{23}P_3) \qquad \text{mod } 26$$

$$C_3 = (K_{31}P_1 + K_{32}P_2 + K_{33}P_3) \qquad \text{mod } 26$$

For decryption, the inverse of key matrix $K$ is required [39]. The inverse matrix $K^{-1}$ of a key matrix $K$ is defined by the following equation

$$KK^{-1} = K^{-1}K = I \quad \text{mod } 26$$

where $I$ represents the identity matrix. Still and all the inverse matrix of the key doesn't always exit. But when exists, it conforms to the equation $KK^{-1} = K^{-1}K = I$. As $K$ is operated on plaintext to find the cipher, in the same way $K^{-1}$ is multiplied with the ciphertext to recover the plaintext. We can write the generalized form of the encryption and decryption as following:

For encryption

$$C = E_k(P) = KP \qquad \text{mod } 26$$

For decryption

$$D = D_k(C) = K^{-1}C = K^{-1}KP = P \qquad \text{mod } 26$$

The possible letters blocks vary with the length of block, if the block length is $m$ then there may be $26^m$ possible and different $m$ block letters. Each of them can be viewed as a letter present in a $26^m$-letter alphabet. Hill cipher's polygraphic substitution method add up to monoalphabetic substitution on $26^m$-letter alphabet.

**Example 2.4.** Let the plaintext **P** be given as

$$P = SHORTS$$

and a $3 \times 3$ encryption key $\mathbf{K}$ be given as

$$K = \begin{pmatrix} 6 & 4 & 1 \\ 13 & 16 & 10 \\ 2 & 17 & 5 \end{pmatrix} \quad \mod 26.$$

To encrypt the plaintext by hill cipher algorithm, first $\mathbf{P}$ is encoded by using Table 2.3 as

$$P = SHORTS = 18 \quad 7 \quad 14 \quad 17 \quad 19 \quad 18$$

Since $m = 3$, we split $\mathbf{P}$ as block of 3 integers as following

$$P_\alpha = \begin{pmatrix} 18 \\ 7 \\ 14 \end{pmatrix}, \quad P_\beta = \begin{pmatrix} 17 \\ 19 \\ 18 \end{pmatrix}$$

Using encryption algorithm $\mathbf{C} = K\mathbf{P} \mod 26$ we get

$$C_\alpha = KP_\alpha \quad \mod 26$$

$$\begin{pmatrix} C_1 \\ C_2 \\ C_3 \end{pmatrix} = \begin{pmatrix} K_{11} & K_{12} & K_{13} \\ K_{21} & K_{22} & K_{23} \\ K_{31} & K_{32} & K_{33} \end{pmatrix} \begin{pmatrix} P_1 \\ P_2 \\ P_3 \end{pmatrix} \quad \mod 26$$

$$\begin{pmatrix} C_1 \\ C_2 \\ C_3 \end{pmatrix} = \begin{pmatrix} 6 & 4 & 1 \\ 13 & 16 & 10 \\ 2 & 17 & 5 \end{pmatrix} \begin{pmatrix} 18 \\ 7 \\ 14 \end{pmatrix} \quad \mod 26$$

$$\begin{pmatrix} C_1 \\ C_2 \\ C_3 \end{pmatrix} = \begin{pmatrix} (6)(18)+(4)(7)+(1)(14) \\ (13)(18)+(16)(7)+(10)(14) \\ (2)(18)+(17)(7)+(5)(14) \end{pmatrix} \mod 26$$

$$\begin{pmatrix} C_1 \\ C_2 \\ C_3 \end{pmatrix} = \begin{pmatrix} 20 \\ 18 \\ 17 \end{pmatrix} \mod 26$$

Similarly,

$$C_\beta = KP_\beta \qquad \mod 26$$

$$\begin{pmatrix} C_4 \\ C_5 \\ C_6 \end{pmatrix} = \begin{pmatrix} K_{11} & K_{12} & K_{13} \\ K_{21} & K_{22} & K_{23} \\ K_{31} & K_{32} & K_{33} \end{pmatrix} \begin{pmatrix} P_4 \\ P_5 \\ P_6 \end{pmatrix} \mod 26$$

$$\begin{pmatrix} C_4 \\ C_5 \\ C_6 \end{pmatrix} = \begin{pmatrix} 6 & 4 & 1 \\ 13 & 16 & 10 \\ 2 & 17 & 5 \end{pmatrix} \begin{pmatrix} 17 \\ 19 \\ 18 \end{pmatrix} \mod 26$$

$$\begin{pmatrix} C_4 \\ C_5 \\ C_6 \end{pmatrix} = \begin{pmatrix} (6)(17)+(4)(19)+(1)(18) \\ (13)(17)+(16)(19)+(10)(18) \\ (2)(17)+(17)(19)+(5)(18) \end{pmatrix} \mod 26$$

$$\begin{pmatrix} C_4 \\ C_5 \\ C_6 \end{pmatrix} = \begin{pmatrix} 14 \\ 03 \\ 05 \end{pmatrix} \qquad \mod 26$$

So, the encrypted text **C** is

$$C = 20 \quad 18 \quad 17 \quad 14 \quad 03 \quad 05$$

Now place back the numbers above to alphabets by using Table 2.3 as

$$C = USRODF$$

Hence, the plaintext "**SHORTS**"is encoded to "**USRODF**".

Now we decode the ciphertext "**USRODF**" to its original form by using the following equation.

$$P = K^{-1}C \qquad \mod 26$$

In order to do this, we must consider the inverse key $K^{-1}$ by using **ApCoCoA** *i.e*

$$K^{-1} = \begin{pmatrix} 20 & 5 & 12 \\ 23 & 14 & 9 \\ 23 & 18 & 22 \end{pmatrix} \qquad \mod 26$$

The ciphertext **C** is given below:

$$C = USRODF$$

First **C** is encoded by using Table 2.3 as

$$C = 20 \quad 18 \quad 17 \quad 14 \quad 03 \quad 05$$

Since $m = 3$, we split $\mathbf{C}$ as block of 3 integers as following

$$C_\alpha = \begin{pmatrix} 20 \\ 18 \\ 17 \end{pmatrix}, \quad C_\beta = \begin{pmatrix} 14 \\ 03 \\ 05 \end{pmatrix}$$

Using decryption algorithm $\mathbf{P} = K^{-1}\mathbf{C} \mod 26$ we get

$$P_\alpha = K^{-1}C_\alpha \qquad \text{mod } 26$$

$$\begin{pmatrix} P_1 \\ P_2 \\ P_3 \end{pmatrix} = \begin{pmatrix} K_{11} & K_{12} & K_{13} \\ K_{21} & K_{22} & K_{23} \\ K_{31} & K_{32} & K_{33} \end{pmatrix}^{-1} \begin{pmatrix} C_1 \\ C_2 \\ C_3 \end{pmatrix} \qquad \text{mod } 26$$

$$\begin{pmatrix} P_1 \\ P_2 \\ P_3 \end{pmatrix} = \begin{pmatrix} 20 & 5 & 12 \\ 23 & 14 & 9 \\ 23 & 18 & 22 \end{pmatrix} \begin{pmatrix} 20 \\ 18 \\ 17 \end{pmatrix} \qquad \text{mod } 26$$

$$\begin{pmatrix} P_1 \\ P_2 \\ P_3 \end{pmatrix} = \begin{pmatrix} (20)(20) + (5)(18) + (12)(17) \\ (23)(20) + (14)(18) + (9)(17) \\ (23)(20) + (18)(18) + (22)(17) \end{pmatrix} \qquad \text{mod } 26$$

$$\begin{pmatrix} P_1 \\ P_2 \\ P_3 \end{pmatrix} = \begin{pmatrix} 18 \\ 07 \\ 14 \end{pmatrix} \qquad \text{mod } 26$$

Similarly,

$$P_\beta = K^{-1}C_\beta \qquad \text{mod } 26$$

$$\begin{pmatrix} P_4 \\ P_5 \\ P_6 \end{pmatrix} = \begin{pmatrix} K_{11} & K_{12} & K_{13} \\ K_{21} & K_{22} & K_{23} \\ K_{31} & K_{32} & K_{33} \end{pmatrix}^{-1} \begin{pmatrix} C_4 \\ C_5 \\ C_6 \end{pmatrix} \qquad \text{mod } 26$$

$$\begin{pmatrix} P_4 \\ P_5 \\ P_6 \end{pmatrix} = \begin{pmatrix} 20 & 5 & 12 \\ 23 & 14 & 9 \\ 23 & 18 & 22 \end{pmatrix} \begin{pmatrix} 14 \\ 03 \\ 05 \end{pmatrix} \qquad \text{mod } 26$$

$$\begin{pmatrix} P_4 \\ P_5 \\ P_6 \end{pmatrix} = \begin{pmatrix} (20)(14) + (5)(03) + (12)(05) \\ (23)(14) + (14)(03) + (9)(05) \\ (23)(14) + (18)(03) + (22)(05) \end{pmatrix} \qquad \text{mod } 26$$

$$\begin{pmatrix} P_4 \\ P_5 \\ P_6 \end{pmatrix} = \begin{pmatrix} 17 \\ 19 \\ 18 \end{pmatrix} \qquad \text{mod } 26$$

So, the decrypted text **P** is

$$P = 18 \quad 7 \quad 14 \quad 17 \quad 19 \quad 18$$

Now place back the numbers above to alphabets by using Table 2.3 as

$$P = SHORTS$$

## Cryptanalysis

The basic Hill cipher is vulnerable to a known plaintext attack because it is completely linear. An adversary who retrieves multiple pairs of plaintext / ciphertext symbols can set up a linear structure that can be easily solved. If this scheme is indeterminate, then only a few more plaintext / ciphertext pairs need to be added. Hill cipher represents the encryption by

$$C = KP \qquad \text{mod } 26$$

where $C$ represents ciphertext, $P$ represents plaintext and both are column vector of length $m$. And $K$ represents the key used for encryption which is a square matrix of order $m \times m$. All operations of the algorithm are performed modulo 26. The known plaintext $P$ is **SHORTSXYZ** and the corresponding ciphertext $C$ is **USRODFZXH**. The unknown key of order $3 \times 3$ is

$$K = \begin{pmatrix} K_{11} & K_{12} & K_{13} \\ K_{21} & K_{22} & K_{23} \\ K_{31} & K_{32} & K_{33} \end{pmatrix}$$

First of all, encode plaintext $P$ and ciphertext $C$ by using Table 2.3 as

$$P = SHORTSXYZ = 18 \quad 7 \quad 14 \quad 17 \quad 19 \quad 18 \quad 23 \quad 24 \quad 25$$

$$C = USRODFZXH = 20 \quad 18 \quad 17 \quad 14 \quad 03 \quad 05 \quad 25 \quad 23 \quad 7$$

Split the plaintext $P$ as block of 3 integers as following

$$P_\alpha = \begin{pmatrix} 18 \\ 7 \\ 14 \end{pmatrix}, \quad P_\beta = \begin{pmatrix} 17 \\ 19 \\ 18 \end{pmatrix}, \quad P_\gamma = \begin{pmatrix} 23 \\ 24 \\ 25 \end{pmatrix}.$$

Now split the ciphertext $c$ as block of 3 integers as following

$$C_\alpha = \begin{pmatrix} 20 \\ 18 \\ 17 \end{pmatrix}, \quad C_\beta = \begin{pmatrix} 14 \\ 3 \\ 5 \end{pmatrix}, \quad C_\gamma = \begin{pmatrix} 25 \\ 23 \\ 7 \end{pmatrix}.$$

Now for $P_\alpha$, $C_\alpha$ and unknown $K$, we have

$$C_\alpha = K * P_\alpha \mod 26$$

$$\begin{pmatrix} 20 \\ 18 \\ 17 \end{pmatrix} = \begin{pmatrix} K_{11} & K_{12} & K_{13} \\ K_{21} & K_{22} & K_{23} \\ K_{31} & K_{32} & K_{33} \end{pmatrix} \begin{pmatrix} 18 \\ 7 \\ 14 \end{pmatrix} \mod 26$$

This gives 3 linear system of equations:

$$\begin{aligned} 20 &= 18K_{11} + 7K_{12} + 14K_{13} \mod 26 \\ 18 &= 18K_{21} + 7K_{22} + 14K_{23} \mod 26 \\ 17 &= 18K_{31} + 7K_{32} + 14K_{33} \mod 26 \end{aligned}$$

Now for $P_\beta$, $C_\beta$ and unknown $K$, we have

$$C_\beta = K * P_\beta \mod 26$$

$$\begin{pmatrix} 14 \\ 3 \\ 5 \end{pmatrix} = \begin{pmatrix} K_{11} & K_{12} & K_{13} \\ K_{21} & K_{22} & K_{23} \\ K_{31} & K_{32} & K_{33} \end{pmatrix} \begin{pmatrix} 17 \\ 19 \\ 18 \end{pmatrix} \mod 26.$$

This gives 3 linear system of equations:

$$\begin{aligned} 14 &= 17K_{11} + 19K_{12} + 18K_{13} \mod 26 \\ 3 &= 17K_{21} + 19K_{22} + 18K_{23} \mod 26 \\ 5 &= 17K_{31} + 19K_{32} + 18K_{33} \mod 26 \end{aligned}$$

Now for $P_\gamma$, $C_\gamma$ and unknown $K$, we have

$$C_\gamma = K * P_\gamma \mod 26$$

$$\begin{pmatrix} 25 \\ 23 \\ 7 \end{pmatrix} = \begin{pmatrix} K_{11} & K_{12} & K_{13} \\ K_{21} & K_{22} & K_{23} \\ K_{31} & K_{32} & K_{33} \end{pmatrix} \begin{pmatrix} 23 \\ 24 \\ 25 \end{pmatrix} \mod 26.$$

This gives 3 linear system of equations:

$$\begin{aligned} 25 &= 23K_{11} + 24K_{12} + 25K_{13} \mod 26 \\ 23 &= 23K_{21} + 24K_{22} + 25K_{23} \mod 26 \\ 7 &= 23K_{31} + 24K_{32} + 25K_{33} \mod 26 \end{aligned}$$

System of linear algebraic equations:

$$20 = 18K_{11} + 7K_{12} + 14K_{13} \mod 26 \tag{2.3}$$

$$18 = 18K_{21} + 7K_{22} + 14K_{23} \mod 26 \tag{2.4}$$

$$17 = 18K_{31} + 7K_{32} + 14K_{33} \mod 26 \tag{2.5}$$

$$14 = 17K_{11} + 19K_{12} + 18K_{13} \mod 26 \tag{2.6}$$

$$3 = 17K_{21} + 19K_{22} + 18K_{23} \mod 26 \tag{2.7}$$

$$5 = 17K_{31} + 19K_{32} + 18K_{33} \mod 26 \tag{2.8}$$

$$25 = 23K_{11} + 24K_{12} + 25K_{13} \mod 26 \tag{2.9}$$

$$23 = 23K_{21} + 24K_{22} + 25K_{23} \mod 26 \tag{2.10}$$

$$7 = 23K_{31} + 24K_{32} + 25K_{33} \mod 26 \tag{2.11}$$

There are nine unknowns and nine linear equations. Solving Equations 2.4, 2.7 and 2.10 by Gauss Jordan Elimination method, we get:

$$K_{11} = 6 \mod 26 \tag{2.12}$$

$$K_{12} = 4 \mod 26 \tag{2.13}$$

$$K_{13} = 1 \mod 26 \tag{2.14}$$

Solving Equations 2.5, 2.8 and 2.11 by Gauss Jordan Elimination method, we get:

$$K_{21} = 13 \mod 26 \tag{2.15}$$

$$K_{22} = 16 \mod 26 \tag{2.16}$$

$$K_{23} = 10 \mod 26 \tag{2.17}$$

Solving Equations 2.6, 2.9 and 2.11 by Gauss Jordan Elimination method, we get:

$$K_{31} = 2 \mod 26 \tag{2.18}$$

$$K_{32} = 17 \mod 26 \tag{2.19}$$

$$K_{33} = 5 \mod 26 \tag{2.20}$$

From Equation 2.13-2.20, we get the unknown key $K$ which satisfies the Hill cipher encryption process *i.e.*

$$K = \begin{pmatrix} K_{11} & K_{12} & K_{13} \\ K_{21} & K_{22} & K_{23} \\ K_{31} & K_{32} & K_{33} \end{pmatrix} \mod 26$$

$$K = \begin{pmatrix} 6 & 4 & 1 \\ 13 & 16 & 10 \\ 2 & 17 & 5 \end{pmatrix} \mod 26.$$

# Chapter 3

# The Encryption Scheme based on Advanced Hill Cipher Algorithm

In this chapter we will review the article entitled “Image Encryption Using Advanced Hill Cipher Algorithm” presented by Acharya et al [22]. Here we will present their proposed advanced Hill Cipher and encryption/decryption algorithm. This article describes the cryptographic scheme for Hill cipher to generate an involutory key matrix. At the end, we will discuss the encryption/decryption algorithm using the advanced Hill cipher technique.

## 3.1 Generation of Involutory Key Matrix

For encryption technique an involutory key matrix is used in the AdvHill algorithm. Several suggested methods can be found in the literature [40].
“Matrix $A$ is called involutory matrix if the matrix $A$ is it’s own inverse. The multiplication by matrix $A$ is an involution iff $A^2 = I$”.
The following are the properties of involutory matrix:

1. $A = A^{-1}/A^2 = I$.

2. $\det(A) = \pm 1$.

3. $A$ is involutory iff $\frac{1}{2}\left(A+I\right)$ is idempotent.

4. $A$ is involutory, $B$ is involutory then $AB$ is involutory.

5. For $n = even$ $A^n = I$ and for $n = odd$ $A^n = A$.

6. A matrix of period 2 is involutory.

7. $A$ is involutory iff $a_{11} + a_{22} \equiv 0$.

8. $|A| = -1$ iff $a_{11} + a_{22} \equiv 0$

9. $\det(I) = 1 \implies \det(A)$ must be a number whose square must be 1.

The seminal study given here for the production output of involutory key matrix is true for positive integer matrix with modular arithmetic residues of a number. This algorithm produces involutory square matrices of order $n \times n$, where $n$ is even.

Let

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} & \cdots & \cdots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \cdots & \cdots & a_{2n} \\ a_{31} & a_{32} & a_{33} & \cdots & \cdots & a_{3n} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & a_{n3} & \cdots & \cdots & a_{nn} \end{pmatrix}$$

be an $n \times n$ involutory matrix split to

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

where $n$ is even and $A_{11}, A_{12}, A_{21}$ and $A_{22}$ are all matrices of $\frac{n}{2} \times \frac{n}{2}$ order.

From Property 3.1

$$A_{12}A_{21} = I - A_{11}^2 = (I - A_{11})(I + A_{11})$$

The terms $A_{12}$ & $A_{21}$ are the corresponding factors of $I - A_{11}^2$. Then solve the second matrix equation whose resultant is $A_{11}+A_{22} = \mathbf{0}$ then an involutory matrix is formed.

**Algorithm 3.1.1.** (**An Involutory Key Matrix**)
**Input:** $\frac{n}{2} \times \frac{n}{2}$ random matrix over $\mathbb{Z}_p$, $n$ is even.
**Output:** $n \times n$ involutory key matrix.

1. Choose a matrix $A_{22}$ randomly of order $\frac{n}{2} \times \frac{n}{2}$.
2. Get the matrix $A_{11}$ from $A_{22}$ *i.e* $A_{11} = -\, A_{22}$.
3. Select a number $k$ randomly which is a scalar constant.
4. Now calculate $A_{12}$ such that $A_{12} = k(I - A_{11})$ or $A_{12} = k(I + A_{11})$.
5. Similarly, calculate $A_{21}$ such that $A_{21} = \frac{1}{k}(I + A_{11}) \quad or \quad A_{12} = \frac{1}{k}(I - A_{11})$.
6. $n \times n$ involutory key matrix is generated completely.

**Example 3.1.** Let the finite field be $\mathbb{Z}_{31}$ and $n = 2$. To form a $2 \times 2$ involutory matrix, we randomly choose $A_{22}$ as

$$A_{22} = \begin{pmatrix} 20 \end{pmatrix} \mod 31.$$

Get $A_{11}$ by $A_{11} = -A_{22} \qquad \mod 31$,

$$A_{11} = -\begin{pmatrix} 20 \end{pmatrix} = \begin{pmatrix} 11 \end{pmatrix} \mod 31.$$

Now select $k$ randomly, $k = 16$, and calculate $A_{12}$ as $A_{12} = k(I - A_{11}) \qquad \mod 31$,

$$A_{12} = 16\left(\begin{pmatrix} 1 \end{pmatrix} - \begin{pmatrix} 11 \end{pmatrix}\right) = \begin{pmatrix} 26 \end{pmatrix} \mod 31.$$

Similarly, we calculate $A_{21}$ by $\frac{1}{k}(I + A_{11})$, we first calculate $k^{-1}$ by Extended Euclidean Algorithm 2.3.4

$$k = 16 \implies k^{-1} = 2 \qquad \mod 31$$

$$A_{21} = 2\left(\begin{pmatrix}1\end{pmatrix} + \begin{pmatrix}11\end{pmatrix}\right) = \begin{pmatrix}24\end{pmatrix} \quad \text{mod } 31,$$

$$\implies \mathbf{A} = \begin{pmatrix}11 & 26\\ 24 & 20\end{pmatrix} \quad \text{mod } 31.$$

As

$$\det(A) = -1 \implies \det(A) = 30 \qquad \text{mod } 31.$$

Using Extended Euclidean algorithm 2.3.4

$$\det(A)^{-1} = 30 \qquad \text{mod } 31.$$

Also

$$adj(A) = \begin{pmatrix}20 & -26\\ -24 & 11\end{pmatrix} = \begin{pmatrix}20 & 5\\ 7 & 11\end{pmatrix} \qquad \text{mod } 31.$$

So

$$A^{-1} = \det(A)^{-1} adj(A) \qquad \text{mod } 31.$$

$$A^{-1} = 30\left(\begin{pmatrix}20 & 5\\ 7 & 11\end{pmatrix}\right) = \begin{pmatrix}600 & 150\\ 210 & 330\end{pmatrix} \qquad \text{mod } 31$$

$$A^{-1} = \begin{pmatrix}11 & 26\\ 24 & 20\end{pmatrix} \qquad \text{mod } 31.$$

Thus $A^{-1} = A \implies \mathbf{A}$ is involutory.

**Example 3.2.** Consider a non-singular matrix $A_{22}$ randomly of order $2 \times 2$ over $\mathbb{Z}_{31}$

$$A_{22} = \begin{pmatrix} 6 & 19 \\ 20 & 11 \end{pmatrix} \quad \mod 31.$$

compute $A_{11}$ by $A_{11} = -A_{22} \mod 31$,

$$A_{11} = -\begin{pmatrix} 6 & 19 \\ 20 & 11 \end{pmatrix} = \begin{pmatrix} 25 & 12 \\ 11 & 20 \end{pmatrix} \quad \mod 31.$$

Now select $k$ randomly, $k = 2$, and calculate $A_{12}$ as $A_{12} = k(I - A_{11}) \mod 31$

$$A_{12} = 2\left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} - \begin{pmatrix} 25 & 12 \\ 11 & 20 \end{pmatrix}\right) = \begin{pmatrix} 14 & 7 \\ 9 & 24 \end{pmatrix} \quad \mod 31.$$

Similarly, we calculate $A_{21}$ by $\frac{1}{k}(I + A_{11})$. We first calculate $k^{-1} \mod 31$ by Extended Euclidean Algorithm 2.3.4

$$k = 2 \quad \Longrightarrow \quad k^{-1} = 16 \quad \mod 31$$

$$A_{21} = 16\left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} 25 & 12 \\ 11 & 20 \end{pmatrix}\right) \quad \mod 31,$$

$$A_{21} = \begin{pmatrix} 13 & 6 \\ 21 & 26 \end{pmatrix} \quad \mod 31,$$

$$\implies \mathbf{A} = \begin{pmatrix} 25 & 12 & 14 & 7 \\ 11 & 20 & 9 & 24 \\ 13 & 6 & 6 & 19 \\ 21 & 26 & 20 & 11 \end{pmatrix} \mod 31.$$

As

$$\det(A) = 1 \implies \det(A)^{-1} = 1 \qquad \mod 31.$$

Also

$$adj(A) = \begin{pmatrix} 25 & 12 & 14 & 7 \\ 11 & 20 & 9 & 24 \\ 13 & 6 & 6 & 19 \\ 21 & 26 & 20 & 11 \end{pmatrix} \mod 31.$$

So

$$A^{-1} = \det(A)^{-1} adj(A) \qquad \mod 31.$$

$$A^{-1} = 1\left(\begin{pmatrix} 25 & 12 & 14 & 7 \\ 11 & 20 & 9 & 24 \\ 13 & 6 & 6 & 19 \\ 21 & 26 & 20 & 11 \end{pmatrix}\right) \qquad \mod 31$$

$$A^{-1} = \begin{pmatrix} 25 & 12 & 14 & 7 \\ 11 & 20 & 9 & 24 \\ 13 & 6 & 6 & 19 \\ 21 & 26 & 20 & 11 \end{pmatrix} \mod 31.$$

Thus $A^{-1} = A \implies \mathbf{A}$ is involutory.

## 3.2 Encryption Using AdvHill Technique

Acharya et al [22], proposed an image encryption scheme by introducing Advanced Hill cipher encryption scheme. They claim that Advanced Hill cipher is more secure as compared with original Hill cipher.

In this section our focus is study Advanced Hill cipher scheme to check its security against known attack. Our analysis shows that the proposed Advanced Hill cipher technique is vulnerable to known-plaintext attack. That is, an attacker can recover the involutory matrix used as the secret key. We first describe the Advanced Hill cipher algorithm and then illustrate the scheme by an example.

**Algorithm 3.2.1.** (**Algorithm AdvHill**)

**Input:** Original plaintext message and $n \times n$ involutory key matrix over $\mathbb{Z}_p$ where $n$ is even.

**Output:** An encrypted message.

1. $n \times n$ involutory key matrix is generated (using Algorithm 3.1.1).
2. Divide the original plaintext message symmetrically into $n \times n$ blocks.
3. To create a fleeting block, pick $ij$-element of each symmetric block and assemble them together as matrix of order $n \times n$. $(i, j = 1 \ldots n)$
4. Apply Hill cipher technique over the fleeting block.
5. Take the transpose of matrix after Hill cipher technique applied.
6. Apply technique of hill cipher over the transposed resulting matrix again.
7. The ciphertext block matrix is obtained by placing in th $ij$-block oh ciphertext message.

The mathematical illustration of the above algorithm for $n = 2$ and $m = 4$ is given below.

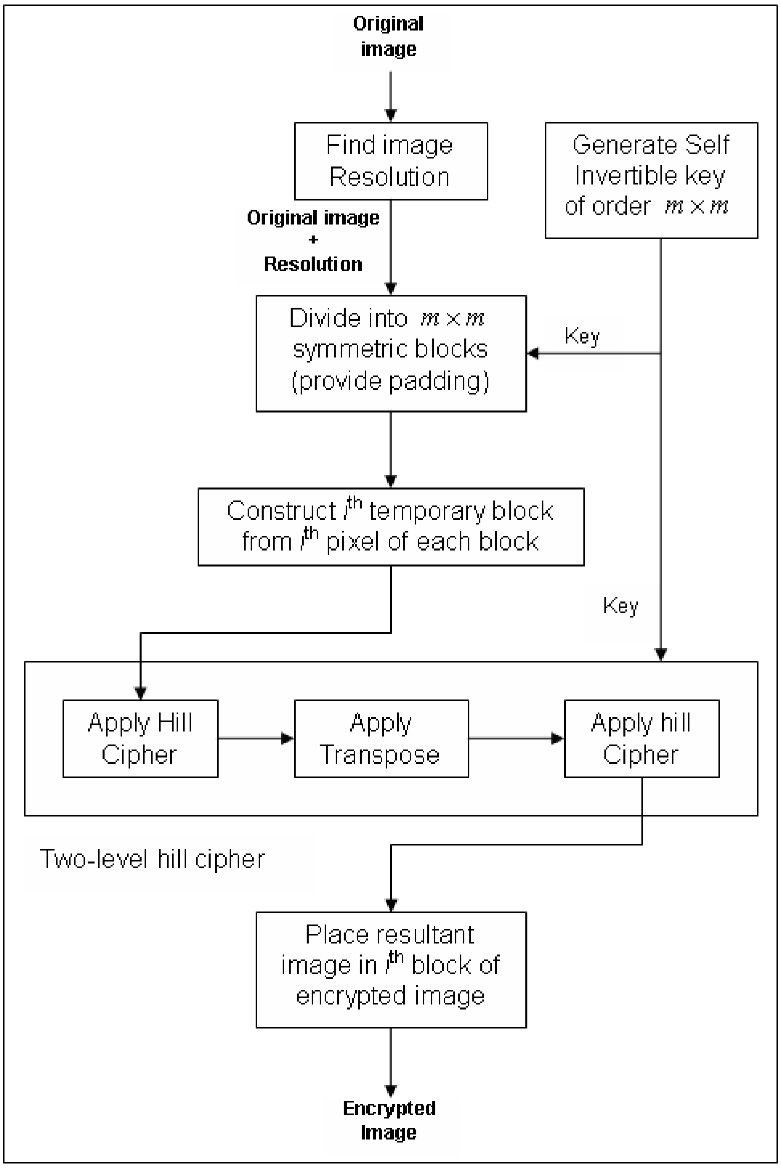
Original image
Find image Resolution
Generate Self Invertible key of order $m \times m$
Original image + Resolution
Divide into $m \times m$ symmetric blocks (provide padding)
Key
Construct $i^{th}$ temporary block from $i^{th}$ pixel of each block
Key
Apply Hill Cipher
Apply Transpose
Apply hill Cipher
Two-level hill cipher
Place resultant image in $i^{th}$ block of encrypted image
Encrypted Image

Figure 3.1: AdvHill Algorithm [22]

**Example 3.3.** Suppose that Algorithm 3.1.1 generates the following $2 \times 2$ matrix over $\mathbb{Z}_p$.

$$A = \begin{pmatrix} \beta & \gamma \\ \chi & \alpha \end{pmatrix} \mod p$$

Let **P** be the plaintext matrix of order 4 × 4. That is,

$$P = \begin{pmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{pmatrix} \mod p.$$

As the order of constructed involutory key is 2 × 2, so we will divide the plaintext into 2 × 2 symmetric blocks *i.e*

$$P = \left(\begin{array}{cc|cc} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ \hline a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{array}\right) \mod p \tag{3.1}$$

As $i = 1, 2$ and $j = 1, 2$. Select 11-element of each block in 3.3 to construct a temporary block $P_1$:

$$P_1 = \begin{pmatrix} a_{11} & a_{13} \\ a_{31} & a_{33} \end{pmatrix} \mod p. \tag{3.2}$$

Similarly $P_2$ is constructed by choosing 12-element of each block. That is

$$P_2 = \begin{pmatrix} a_{12} & a_{14} \\ a_{32} & a_{34} \end{pmatrix} \mod p. \tag{3.3}$$

Continuing this way $P_3$ and $P_4$ are also constructed.

$$P_3 = \begin{pmatrix} a_{31} & a_{23} \\ a_{41} & a_{43} \end{pmatrix}, \quad P_4 = \begin{pmatrix} a_{22} & a_{24} \\ a_{42} & a_{44} \end{pmatrix}.$$

Step 4 of Algorithm 3.2.1 says that apply Hill cipher algorithm on each temporary block to get corresponding cipher blocks $C_1, C_2, C_3$ and $C_4$. For $P_1$ we have

$$C_1 = AP_1 \mod p$$

$$C_1 = \begin{pmatrix} \beta & \gamma \\ \chi & \alpha \end{pmatrix} \begin{pmatrix} a_{11} & a_{13} \\ a_{31} & a_{33} \end{pmatrix} = \begin{pmatrix} a_{11}\beta + a_{31}\gamma & a_{13}\beta + a_{33}\gamma \\ a_{11}\chi + a_{31}\alpha & a_{13}\chi + a_{33}\alpha \end{pmatrix} \mod p$$

Apply Step 5 to replace$C_1$ by $C_1^T$. That is $C_1 \mapsto C_1^T$

$$C_1 \mapsto C_1^T = \begin{pmatrix} a_{11}\beta + a_{31}\gamma & a_{11}\chi + a_{31}\alpha \\ a_{13}\beta + a_{33}\gamma & a_{13}\chi + a_{33}\alpha \end{pmatrix} \mod p$$

The output of Step 6 will results

$$C_1 \mapsto A(AC_1)^T \mod p$$

$$C_1 \mapsto A(AC_1)^T = \begin{pmatrix} \beta & \gamma \\ \chi & \alpha \end{pmatrix} \begin{pmatrix} a_{11}\beta + a_{31}\gamma & a_{11}\chi + a_{31}\alpha \\ a_{13}\beta + a_{33}\gamma & a_{13}\chi + a_{33}\alpha \end{pmatrix} = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} \mod p.$$

Similarly,

$$C_2 \mapsto A(AC_2)^T = \begin{pmatrix} \beta & \gamma \\ \chi & \alpha \end{pmatrix} \begin{pmatrix} a_{12}\beta + a_{32}\gamma & a_{12}\chi + a_{32}\alpha \\ a_{14}\beta + a_{34}\gamma & a_{14}\chi + a_{34}\alpha \end{pmatrix} = \begin{pmatrix} b_{13} & b_{14} \\ b_{23} & b_{24} \end{pmatrix} \mod p.$$

$$C_3 \mapsto A(AC_3)^T = \begin{pmatrix} \beta & \gamma \\ \chi & \alpha \end{pmatrix} \begin{pmatrix} a_{31}\beta + a_{41}\gamma & a_{31}\chi + a_{41}\alpha \\ a_{23}\beta + a_{43}\gamma & a_{23}\chi + a_{43}\alpha \end{pmatrix} = \begin{pmatrix} b_{31} & b_{32} \\ b_{41} & b_{42} \end{pmatrix} \mod p.$$

$$C_4 \mapsto A(AC_4)^T = \begin{pmatrix} \beta & \gamma \\ \chi & \alpha \end{pmatrix} \begin{pmatrix} a_{22}\beta + a_{42}\gamma & a_{22}\chi + a_{42}\alpha \\ a_{24}\beta + a_{44}\gamma & a_{24}\chi + a_{44}\alpha \end{pmatrix} = \begin{pmatrix} b_{33} & b_{34} \\ b_{43} & b_{44} \end{pmatrix} \mod p.$$

Finally combining each computed cipher block $C_1, C_2, C_3$ and $C_4$ obtain the ciphertext matrix **C** of order $4 \times 4$ as:

$$C = \begin{pmatrix} C_1 & C_2 \\ C_3 & C_4 \end{pmatrix}$$

$$C = \begin{pmatrix} b_{11} & b_{12} & b_{13} & b_{14} \\ b_{21} & b_{22} & b_{23} & b_{24} \\ b_{31} & b_{32} & b_{33} & b_{34} \\ b_{41} & b_{42} & b_{43} & b_{44} \end{pmatrix} \mod p.$$

The following example illustrate the computation.

**Example 3.4.** Let **A** be involutory matrix $2 \times 2$ constructed in Example 3.1 by following Algorithm 3.1.1. That is

$$A = \begin{pmatrix} 11 & 26 \\ 14 & 20 \end{pmatrix} \qquad \mod 31.$$

Let the plaintext matrix **P** of order $4 \times 4$ over $\mathbb{Z}_{31}$ by given as

$$P = \begin{pmatrix} 11 & 4 & 11 & 15 \\ 4 & 17 & 11 & 7 \\ 18 & 7 & 2 & 4 \\ 19 & 8 & 8 & 17 \end{pmatrix} \mod 31.$$

As the order of constructed involutory key is 2 × 2, so we will divide the plaintext into 2 × 2 symmetric blocks *i.e*

$$P = \left(\begin{array}{cc|cc} 11 & 4 & 11 & 15 \\ 4 & 17 & 11 & 7 \\ \hline 18 & 7 & 2 & 4 \\ 19 & 8 & 8 & 17 \end{array}\right) \mod 31 \tag{3.4}$$

As $i = 1, 2$ and $j = 1, 2$. Select 11-element of each block in 3.4 to construct a temporary block $P_1$:

$$P_1 = \begin{pmatrix} 11 & 18 \\ 11 & 2 \end{pmatrix} \mod 31. \tag{3.5}$$

Similarly $P_2$ is constructed by choosing 12-element of each block. That is

$$P_2 = \begin{pmatrix} 4 & 7 \\ 15 & 4 \end{pmatrix} \mod 31. \tag{3.6}$$

Continuing this way $P_3$ and $P_4$ are also constructed.

$$P_3 = \begin{pmatrix} 4 & 19 \\ 11 & 8 \end{pmatrix}, \quad P_4 = \begin{pmatrix} 17 & 8 \\ 7 & 17 \end{pmatrix}.$$

Step 4 of Algorithm 3.2.1 says that apply Hill cipher algorithm on each temporary block to get corresponding cipher blocks $C_1, C_2, C_3$ and $C_4$. For $P_1$ we have

$$C_1 = AP_1 \mod 31$$

$$C_1 = \begin{pmatrix} 11 & 26 \\ 24 & 20 \end{pmatrix} \begin{pmatrix} 11 & 18 \\ 11 & 2 \end{pmatrix} = \begin{pmatrix} 4 & 2 \\ 19 & 7 \end{pmatrix} \mod 31$$

Apply Step 5 to replace $C_1$ by $C_1^T$. That is $C_1 \mapsto C_1^T$

$$C_1 \mapsto C_1^T = \begin{pmatrix} 4 & 19 \\ 2 & 7 \end{pmatrix} \mod 31$$

The output of Step 6 will results

$$C_1 \mapsto A(AP_1)^T \mod 31$$

$$C_1 \mapsto A(AP_1)^T = \begin{pmatrix} 11 & 26 \\ 24 & 20 \end{pmatrix} \begin{pmatrix} 4 & 19 \\ 2 & 7 \end{pmatrix} = \begin{pmatrix} 3 & 19 \\ 12 & 7 \end{pmatrix} \mod 31.$$

Similarly,

$$C_2 = AP_2 \qquad \mod 31$$

$$C_2 = \begin{pmatrix} 11 & 26 \\ 24 & 20 \end{pmatrix} \begin{pmatrix} 4 & 7 \\ 15 & 4 \end{pmatrix} = \begin{pmatrix} 0 & 26 \\ 24 & 0 \end{pmatrix} \mod 31$$

Apply Step 5 to replace$C_2$ by $C_2^T$. That is $C_1 \mapsto C_2^T$

$$C_2 \mapsto C_2^T = \begin{pmatrix} 0 & 24 \\ 26 & 0 \end{pmatrix} \mod 31$$

The output of Step 6 will results

$$C_2 \mapsto AC_2^T \qquad \mod 31$$

$$C_2 \mapsto A(AP_2)^T = \begin{pmatrix} 11 & 26 \\ 14 & 20 \end{pmatrix} \begin{pmatrix} 0 & 24 \\ 26 & 0 \end{pmatrix} = \begin{pmatrix} 25 & 16 \\ 24 & 18 \end{pmatrix} \mod 31$$

$$C_3 \mapsto A(AP_3)^T = \qquad \mod 31$$

$$C_3 \mapsto A(AP_3)^T = \begin{pmatrix} 26 & 24 \\ 16 & 2 \end{pmatrix} \mod 31$$

$$C_4 \mapsto A(AP_4)^T \qquad \mod 31$$

$$C_4 \mapsto A(AP_4)^T = \begin{pmatrix} 14 & 20 \\ 19 & 15 \end{pmatrix} \mod 31$$

Finally combining each computed cipher block $C_1, C_2, C_3$ and $C_4$ obtain the ciphertext matrix **C** of order $4 \times 4$ as:

$$C = \begin{pmatrix} C_1 & C_2 \\ C_3 & C_4 \end{pmatrix}$$

$$C = \begin{pmatrix} 3 & 19 & 25 & 16 \\ 12 & 7 & 24 & 18 \\ 26 & 24 & 14 & 20 \\ 16 & 2 & 19 & 15 \end{pmatrix} \mod 31.$$

For decryption, we reverse the Algorithm 3.2.1. The following example illustrates the decryption of Example 3.4.

**Example 3.5.** Let the cipher $C$ from Example 3.4 that is

$$C = \begin{pmatrix} 3 & 19 & 25 & 16 \\ 12 & 7 & 24 & 18 \\ 26 & 24 & 14 & 20 \\ 16 & 2 & 19 & 15 \end{pmatrix},$$

and involutory key matrix from Example 3.4 that is:

$$A = \begin{pmatrix} 11 & 26 \\ 14 & 20 \end{pmatrix} \mod 31.$$

Partition the cipher matrix in symmetric blocks

$$C = \left(\begin{array}{cc|cc} 3 & 19 & 25 & 16 \\ 12 & 7 & 24 & 18 \\ \hline 26 & 24 & 14 & 20 \\ 16 & 2 & 19 & 15 \end{array}\right) \mod 31 \tag{3.7}$$

Pick the temporary $ij$-block, here we pick up the 11-block from 3.5 $i.e$

$$C_1 = \begin{pmatrix} 3 & 19 \\ 12 & 7 \end{pmatrix} \mod 31.$$

Similarly, pick 12, 21, 22 blocks:

$$C_2 = \begin{pmatrix} 25 & 16 \\ 24 & 18 \end{pmatrix}, C_3 = \begin{pmatrix} 24 & 26 \\ 16 & 2 \end{pmatrix} \text{and} C_4 = \begin{pmatrix} 14 & 20 \\ 19 & 15 \end{pmatrix}.$$

Step 4 of Algorithm 3.2.1 says that apply Hill cipher algorithm on each block to get corresponding plain blocks $P_1, P_2, P_3$ and $P_4$.

$$P = A^{-1}C \implies P = AC \mod 31 \quad \text{Example 3.1}$$

For $C_1$ we have

$$P_1 = AC_1 \qquad \mod 31$$

$$P_1 = \begin{pmatrix} 11 & 26 \\ 14 & 20 \end{pmatrix} \begin{pmatrix} 3 & 19 \\ 12 & 7 \end{pmatrix} = \begin{pmatrix} 4 & 19 \\ 2 & 7 \end{pmatrix} \mod 31$$

Apply Step 5 to replace$P_1$ by $P_1^T$. That is $P_1 \mapsto P_1^T$

$$P_1 \mapsto P_1^T = \begin{pmatrix} 4 & 2 \\ 19 & 7 \end{pmatrix} \mod 31.$$

The output of Step 6 will results

$$P_1 \mapsto A(AC_1)^T \mod 31$$

$$P_1 \mapsto A(AC_1)^T = \begin{pmatrix} 11 & 26 \\ 24 & 20 \end{pmatrix} \begin{pmatrix} 4 & 2 \\ 19 & 7 \end{pmatrix} = \begin{pmatrix} 11 & 18 \\ 11 & 2 \end{pmatrix} \mod 31$$

Similarly,

$$P_2 = AC_2 \qquad \mod 31$$

$$P_2 = \begin{pmatrix} 11 & 26 \\ 14 & 20 \end{pmatrix} \begin{pmatrix} 25 & 16 \\ 24 & 18 \end{pmatrix} = \begin{pmatrix} 0 & 24 \\ 26 & 0 \end{pmatrix} \mod 31$$

Apply Step 5 to replace$P_2$ by $P_2^T$. That is $P_2 \mapsto P_2^T$

$$P_2 \mapsto P_2^T = \begin{pmatrix} 0 & 26 \\ 24 & 0 \end{pmatrix} \mod 31.$$

The output of Step 6 will results

$$P_2 \mapsto AP_2^T \qquad \mod 31$$

$$P_2 \mapsto AP_2^T = \begin{pmatrix} 11 & 26 \\ 24 & 20 \end{pmatrix} \begin{pmatrix} 0 & 26 \\ 24 & 0 \end{pmatrix} = \begin{pmatrix} 4 & 7 \\ 15 & 4 \end{pmatrix} \mod 31$$

$$P_3 = AC_3 \qquad \mod 31$$

$$P_3 = \begin{pmatrix} 11 & 26 \\ 14 & 20 \end{pmatrix} \begin{pmatrix} 24 & 26 \\ 16 & 2 \end{pmatrix} = \begin{pmatrix} 20 & 6 \\ 14 & 27 \end{pmatrix} \mod 31$$

$$P_3 \mapsto AP_3^T \qquad \mod 31$$

$$P_3 \mapsto AP_3^T = \begin{pmatrix} 11 & 26 \\ 24 & 20 \end{pmatrix} \begin{pmatrix} 20 & 14 \\ 6 & 27 \end{pmatrix} = \begin{pmatrix} 4 & 19 \\ 11 & 8 \end{pmatrix} \mod 31$$

$$P_4 = AC_4 \qquad \mod 31$$

$$P_4 = \begin{pmatrix} 11 & 26 \\ 14 & 20 \end{pmatrix} \begin{pmatrix} 14 & 20 \\ 19 & 15 \end{pmatrix} = \begin{pmatrix} 28 & 21 \\ 3 & 5 \end{pmatrix} \mod 31$$

$$P_4 \mapsto AP_4^T \qquad \mod 31$$

$$P_4 \mapsto AP_4^T = \begin{pmatrix} 11 & 26 \\ 24 & 20 \end{pmatrix} \begin{pmatrix} 28 & 3 \\ 21 & 5 \end{pmatrix} = \begin{pmatrix} 17 & 8 \\ 7 & 17 \end{pmatrix} \mod 31$$

Place $ij$-element of each block $P_1, P_2, P_3$ and $P_4$ at $ij$-element of each symmetric block in 3.5. Plaintext message is recovered.

$$P = \begin{pmatrix} \mathbf{11} & \mathbf{4} & \mathbf{11} & \mathbf{15} \\ \mathbf{4} & \mathbf{17} & \mathbf{11} & \mathbf{7} \\ \mathbf{18} & \mathbf{7} & \mathbf{2} & \mathbf{4} \\ \mathbf{19} & \mathbf{8} & \mathbf{8} & \mathbf{17} \end{pmatrix}$$

# Chapter 4

# Cryptanalysis of Advanced Hill Cipher Algorithm

In this chapter, we discussed the encryption scheme based on Advanced Hill cipher algorithm presented by Acharya et al [22]. The analysis of the scheme shows that it has many security flaws. In this chapter, it is shown that the scheme is vulnerable to a known plaintext attack.

## 4.1 Cryptanalysis

In this section we have shown that the encryption/decryption scheme of Acharya et al, is susceptible to known plaintext attack. The main goal of the attack on "Image Encryption Using Advanced Hill Cipher Algorithm"is to identify all $n \times n$ entries in $A$, where $n$ is even and $A$ is unknown key. We can then eavesdrop on any case of single-pass protocol to obtain encrypted plaintext *E(P)*. In a known plaintext attack, we assume that an attacker has the knowledge of plaintext and ciphertext pairs like $(P_1, C_1), (P_2, C_2), \dots, (P_n, C_n)$. Note that the ciphertext $C_i$ for the plaintext $P_i$ is given by

$$C_i = A(AP_i)^T \mod p \tag{4.1}$$

The cryptanalysis shows that if an attacker has the knowledge of both $P$ and $C$ then the scheme will not be secure for any subsequent encryption. Before describing the method of attack, note that an attacker has following information

1. The key $A$ is an $n \times n$ involutory matrix over $\mathbb{Z}_p$, where $p$ is prime.
2. Encryption and decryption are done with the AdvHill cipher algorithm.

The following example illustrates the attack when $n = 2$.

**Example 4.1.** The palintext and ciphertext are the matrices of order $2n \times 2n = 4 \times 4$. Suppose that known $P$ and $C$ are as given below:

$$P = \begin{pmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{pmatrix} \quad \text{and} \quad C = \begin{pmatrix} b_{11} & b_{12} & b_{13} & b_{14} \\ b_{21} & b_{22} & b_{23} & b_{24} \\ b_{31} & b_{32} & b_{33} & b_{34} \\ b_{41} & b_{42} & b_{43} & b_{44} \end{pmatrix} \mod p.$$

Let the unknown key $A$ is an involutory matrix of order $2 \times 2$ and the entries from $\mathbb{Z}_p$, $A$ is given as:

$$A = \begin{pmatrix} x & y \\ z & w \end{pmatrix} \mod p$$

where $x, y, z$ and $w$ are four unknowns. By Step 2 of Algorithm 3.2.1, symmetrically divide the plaintext $P$ and ciphertext $C$ into $n \times n \quad (2 \times 2)$ equal blocks

$$P = \left(\begin{array}{cc|cc} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ \hline a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{array}\right) \mod p \tag{4.2}$$

$$C = \left(\begin{array}{cc|cc} b_{11} & b_{12} & b_{13} & b_{14} \\ b_{21} & b_{22} & b_{23} & b_{24} \\ \hline b_{31} & b_{32} & b_{33} & b_{34} \\ b_{41} & b_{42} & b_{43} & b_{44} \end{array}\right) \mod p. \tag{4.3}$$

Step 3 of Algorithm 3.2.1 says pick $ij$-element of each symmetric block 4.1 and assemble together to create fleeting blocks $i.e$ 11-element to construct $P_1$, similarly 12-element → $P_2$, 13-element → $P_3$ and 14-element → $P_4$

$$P_1 = \begin{pmatrix} a_{11} & a_{13} \\ a_{31} & a_{33} \end{pmatrix}, \qquad P_2 = \begin{pmatrix} a_{12} & a_{14} \\ a_{32} & a_{34} \end{pmatrix},$$
$$P_3 = \begin{pmatrix} a_{21} & a_{23} \\ a_{41} & a_{43} \end{pmatrix} \quad \text{and} \quad P_4 = \begin{pmatrix} a_{22} & a_{24} \\ a_{42} & a_{44} \end{pmatrix}.$$

From Step 7 of Algorithm 3.2.1, select $ij$-block of ciphertext $\mathbf{C}$ 4.1. 11-block → $C_1$, 12-block → $C_2$, 21-block → $C_3$ and 22-block → $C_4$.

$$C_1 = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix}, \quad C_2 = \begin{pmatrix} b_{13} & b_{14} \\ b_{23} & b_{24} \end{pmatrix}$$
$$C_3 = \begin{pmatrix} b_{31} & b_{32} \\ b_{41} & b_{42} \end{pmatrix} \quad \text{and} C_4 = \begin{pmatrix} b_{33} & b_{34} \\ b_{43} & b_{44} \end{pmatrix}.$$

Apply Hill cipher by following equation $C = AP \mod p$.

$$C_i = AP_i \mod p$$

$$C_i = A(AP_i)^T \mod p$$

For $P_1$, $C_1$ and unknown key $A$:

$$C_1 = A(AP_1)^T \mod p$$

$$\begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} = \begin{pmatrix} x & y \\ z & w \end{pmatrix} \left( \begin{pmatrix} x & y \\ z & w \end{pmatrix} \begin{pmatrix} a_{11} & a_{13} \\ a_{31} & a_{33} \end{pmatrix} \right)^T \mod p$$

$$\begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} = \begin{pmatrix} x & y \\ z & w \end{pmatrix} \begin{pmatrix} xa_{11} + ya_{31} & za_{11} + wa_{31} \\ xa_{13} + ya_{33} & za_{13} + wa_{33} \end{pmatrix} \mod p$$

$$\begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} = \begin{pmatrix} a_{11}x^2 + a_{31}xy + a_{13}xy + a_{33}y^2 & a_{11}xz + a_{31}xw + a_{13}yz + a_{33}yw \\ a_{11}xz + a_{31}yz + a_{13}xw + a_{33}yw & a_{11}z^2 + a_{31}zw + a_{13}zw + a_{33}w^2 \end{pmatrix}.$$

This gives 4 non-linear system of equation:

$$\begin{aligned} b_{11} &= a_{11}x^2 + a_{31}xy + a_{13}xy + a_{33}y^2 \\ b_{12} &= a_{11}xz + a_{31}xw + a_{13}yz + a_{33}yw \\ b_{21} &= a_{11}xz + a_{31}yz + a_{13}xw + a_{33}yw \\ b_{22} &= a_{11}z^2 + a_{31}zw + a_{13}zw + a_{33}w^2 \end{aligned}$$

Each of the three plaintext-ciphertext components $C_2 = A(AP_2)^T$, $C_3 = A(AP_3)^T$ and $C_4 = A(AP_4)^T$ will:

$$\begin{aligned} b_{13} &= a_{12}x^2 + a_{32}xy + a_{14}xy + a_{34}y^2 \\ b_{14} &= a_{12}xz + a_{32}xw + a_{14}yz + a_{34}yw \\ b_{23} &= a_{12}xz + a_{32}yz + a_{14}xw + a_{34}yw \\ b_{24} &= a_{12}z^2 + a_{32}zw + a_{14}zw + a_{34}w^2 \\ b_{31} &= a_{21}x^2 + a_{41}xy + a_{23}xy + a_{43}y^2 \end{aligned}$$

$$
\begin{aligned}
b_{32} &= a_{21}xz + a_{41}xw + a_{23}yz + a_{43}yw \\
b_{41} &= a_{21}xz + a_{41}yz + a_{23}xw + a_{43}yw \\
b_{42} &= a_{21}z^2 + a_{41}zw + a_{23}zw + a_{43}w^2 \\
b_{33} &= a_{22}x^2 + a_{42}xy + a_{24}xy + a_{44}y^2 \\
b_{34} &= a_{22}xz + a_{42}xw + a_{24}yz + a_{44}yw \\
b_{43} &= a_{22}xz + a_{42}yz + a_{24}xw + a_{44}yw \\
b_{44} &= a_{22}z^2 + a_{42}zw + a_{24}zw + a_{44}w^2
\end{aligned}
$$

Solve the system with the help of **ApCoCoA** and its in-built tools.

The following example illustrate the computation.

**Example 4.2.** The palintext and ciphertext are the matrices of order $2n \times 2n = 4 \times 4$. Suppose that known $P$ and $C$ are as given below:

$$
P = \begin{pmatrix} 11 & 4 & 11 & 15 \\ 4 & 17 & 11 & 7 \\ 18 & 7 & 2 & 4 \\ 19 & 8 & 8 & 17 \end{pmatrix} \mod 31.
$$

$$
C = \begin{pmatrix} 3 & 19 & 25 & 16 \\ 12 & 7 & 24 & 18 \\ 26 & 24 & 14 & 20 \\ 16 & 2 & 19 & 15 \end{pmatrix} \mod 31.
$$

Let the unknown key $A$ is an involutory matrix of order $2 \times 2$ and the entries from $\mathbb{Z}_{31}$, $A$ is given as:

$$
A = \begin{pmatrix} x & y \\ z & w \end{pmatrix} \mod 31
$$

where $x, y, z$ and $w$ are four unknowns. By Step 2 of Algorithm 3.2.1, symmetrically divide the plaintext $P$ and ciphertext $C$ into $n \times n \quad (2 \times 2)$ equal blocks

$$P = \left(\begin{array}{cc|cc} 11 & 4 & 11 & 15 \\ 4 & 17 & 11 & 7 \\ \hline 18 & 7 & 2 & 4 \\ 19 & 8 & 8 & 17 \end{array}\right) \mod 31. \tag{4.4}$$

$$C = \left(\begin{array}{cc|cc} 3 & 19 & 25 & 16 \\ 12 & 7 & 24 & 18 \\ \hline 26 & 24 & 14 & 20 \\ 16 & 2 & 19 & 15 \end{array}\right) \mod 31. \tag{4.5}$$

Step 3 of Algorithm 3.2.1 says pick $ij$-element of each symmetric block 4.2 and assemble together to create fleeting blocks $i.e$ 11-element to construct $P_1$, similarly 12-element → $P_2$, 21-element → $P_3$ and 22-element → $P_4$

$$P_1 = \begin{pmatrix} 11 & 18 \\ 11 & 2 \end{pmatrix}, P_2 = \begin{pmatrix} 4 & 7 \\ 15 & 4 \end{pmatrix},$$
$$P_3 = \begin{pmatrix} 4 & 19 \\ 11 & 8 \end{pmatrix}, P_4 = \begin{pmatrix} 17 & 8 \\ 7 & 17 \end{pmatrix}$$

From Step 7 of Algorithm 3.2.1, select $ij$-block of ciphertext $\mathbf{C}$ 4.2. 11-block → $C_1$, 12-block → $C_2$, 21-block → $C_3$ and 22-block → $C_4$.

$$C_1 = \begin{pmatrix} 3 & 19 \\ 12 & 7 \end{pmatrix}, C_2 = \begin{pmatrix} 25 & 16 \\ 24 & 18 \end{pmatrix},$$
$$C_3 = \begin{pmatrix} 26 & 24 \\ 16 & 2 \end{pmatrix}, C_4 = \begin{pmatrix} 14 & 20 \\ 19 & 15 \end{pmatrix}.$$

Apply Hill cipher by following equation $C = AP \mod p$.

$$C_i = A(AP_i)^T \mod p$$

For $P_1$, $C_1$ and unknown key $A$:

$$AP_1 = \begin{pmatrix} x & y \\ z & w \end{pmatrix} \begin{pmatrix} 11 & 18 \\ 11 & 2 \end{pmatrix} = \begin{pmatrix} 11x + 11y & 11z + 11w \\ 18x + 2y & 18z + 2w \end{pmatrix} \mod 31$$

$$(AP_1)^T = \begin{pmatrix} 11x + 11y & 18x + 2y \\ 11z + 11w & 18z + 2w \end{pmatrix} \mod 31$$

$$C_1 = A(AP_1)^T \mod p$$

$$C_1 = \begin{pmatrix} x & y \\ z & w \end{pmatrix} \begin{pmatrix} 11x + 11y & 11z + 11w \\ 18x + 2y & 18z + 2w \end{pmatrix} \mod 31$$

$$\begin{pmatrix} 3 & 19 \\ 12 & 7 \end{pmatrix} = \begin{pmatrix} 11x^2 + 11xy + 18xy + 2y^2 & 11xz + 11xw + 18yz + 2yw \\ 11xz + 11yz + 18xw + 2yw & 11z^2 + 11zw + 18zw + 2w^2 \end{pmatrix} \mod 31.$$

This gives 4 non-linear system of equation:

$$\begin{aligned} 3 &= 11x^2 + 11xy + 18xy + 2y^2 \mod 31 \\ 19 &= 11xz + 11xw + 18yz + 2yw \mod 31 \\ 12 &= 11xz + 11yz + 18xw + 2yw \mod 31 \\ 7 &= 11z^2 + 11zw + 18zw + 2w^2 \mod 31 \end{aligned}$$

For $P_2$, $C_2$ and unknown key $A$:

$$AP_2 = \begin{pmatrix} x & y \\ z & w \end{pmatrix} \begin{pmatrix} 4 & 7 \\ 15 & 4 \end{pmatrix} = \begin{pmatrix} 4x + 15y & 7x + 4y \\ 4z + 15w & 7z + 4w \end{pmatrix} \mod 31$$

$$(AP_2)^T = \begin{pmatrix} 4x + 15y & 4z + 15w \\ 7x + 4y & 7z + 4w \end{pmatrix} \mod 31$$

$$C_2 = A(AP_2)^T \qquad \mod p$$

$$\begin{pmatrix} 25 & 16 \\ 24 & 18 \end{pmatrix} = \begin{pmatrix} x & y \\ z & w \end{pmatrix} \begin{pmatrix} 4x + 15y & 4z + 15w \\ 7x + 4y & 7z + 4w \end{pmatrix} \mod 31$$

$$\begin{pmatrix} 25 & 16 \\ 24 & 18 \end{pmatrix} = \begin{pmatrix} 4x^2 + 15xy + 7xy + 4y^2 & 4xz + 15xw + 7yz + 4yw \\ 4xz + 15yz + 7xw + 4yw & 4z^2 + 15zw + 7zw + 4w^2 \end{pmatrix} \mod 31.$$

This gives 4 non-linear system of equation:

$$\begin{aligned} 25 &= 4x^2 + 15xy + 7xy + 4y^2 \mod 31 \\ 16 &= 4xz + 15xw + 7yz + 4yw \mod 31 \\ 24 &= 4xz + 15yz + 7xw + 4yw \mod 31 \\ 18 &= 4z^2 + 15zw + 7zw + 4w^2 \mod 31 \end{aligned}$$

For $P_3$, $C_3$ and unknown key $A$:

$$AP_3 = \begin{pmatrix} x & y \\ z & w \end{pmatrix} \begin{pmatrix} 4 & 19 \\ 11 & 8 \end{pmatrix} = \begin{pmatrix} 4x + 11y & 19x + 8y \\ 4z + 11w & 19z + 8w \end{pmatrix} \mod 31$$

$$(AP_3)^T = \begin{pmatrix} 4x+11y & 4z+11w \\ 19x+8y & 19z+8w \end{pmatrix} \mod 31$$

$$C_3 = A(AP_3)^T \qquad \mod 31$$

$$\begin{pmatrix} 26 & 24 \\ 16 & 2 \end{pmatrix} = \begin{pmatrix} x & y \\ z & w \end{pmatrix} \begin{pmatrix} 4x+11y & 4z+11w \\ 19x+8y & 19z+8w \end{pmatrix} \mod 31$$

$$\begin{pmatrix} 26 & 24 \\ 16 & 2 \end{pmatrix} = \begin{pmatrix} 4x^2+11xy+19xy+8y^2 & 4xz+11xw+19yz+8yw \\ 4xz+11yz+19xw+8yw & 4z^2+11zw+19zw+8w^2 \end{pmatrix} \mod 31.$$

This gives 4 non-linear system of equation:

$$\begin{aligned} 26 &= 4x^2+11xy+19xy+8y^2 \mod 31 \\ 24 &= 4xz+11xw+19yz+8yw \mod 31 \\ 16 &= 4xz+11yz+19xw+8yw \mod 31 \\ 2 &= 4z^2+11zw+19zw+8w^2 \mod 31 \end{aligned}$$

For $P_4$, $C_4$ and unknown key $A$:

$$AP_4 = \begin{pmatrix} x & y \\ z & w \end{pmatrix} \begin{pmatrix} 17 & 8 \\ 7 & 17 \end{pmatrix} = \begin{pmatrix} 17x+7y & 8x+17y \\ 17z+7w & 8z+17w \end{pmatrix} \mod 31$$

$$(AP_4)^T = \begin{pmatrix} 17x+7y & 17z+7w \\ 8x+17y & 8z+17w \end{pmatrix} \mod 31$$

$$C_4 = A(AP_4)^T \qquad \mod 31$$

$$\begin{pmatrix} 14 & 20 \\ 19 & 15 \end{pmatrix} = \begin{pmatrix} x & y \\ z & w \end{pmatrix} \begin{pmatrix} 17x+7y & 17z+7w \\ 8x+17y & 8z+17w \end{pmatrix} \mod 31$$

$$\begin{pmatrix} 14 & 20 \\ 19 & 15 \end{pmatrix} = \begin{pmatrix} 17x^2+7xy+8xy+17y^2 & 17xz+7xw+8yz+17yw \\ 17xz+7yz+8xw+17yw & 17z^2+7zw+8zw+17w^2 \end{pmatrix} \mod 31.$$

This gives 4 Non-linear system of equation:

$$\begin{aligned} 14 &= 17x^2+7xy+8xy+17y^2 \mod 31 \\ 20 &= 17xz+7xw+8yz+17yw \mod 31 \\ 19 &= 17xz+7yz+8xw+17yw \mod 31 \\ 15 &= 17z^2+7zw+8zw+17w^2 \mod 31 \end{aligned}$$

System of non-linear algebraic equations:

$$3 = 11x^2+11xy+18xy+2y^2 \tag{4.6}$$

$$19 = 11xz+11xw+18yz+2yw \tag{4.7}$$

$$12 = 11xz+11yz+18xw+2yw \tag{4.8}$$

$$7 = 11z^2+11zw+18zw+2w^2 \tag{4.9}$$

$$25 = 4x^2+15xy+7xy+4y^2 \tag{4.10}$$

$$16 = 4xz+15xw+7yz+4yw \tag{4.11}$$

$$24 = 4xz+15yz+7xw+4yw \tag{4.12}$$

$$18 = 4z^2+15zw+7zw+4w^2 \tag{4.13}$$

$$26 = 4x^2+11xy+19xy+8y^2 \tag{4.14}$$

$$24 = 4xz+11xw+19yz+8yw \tag{4.15}$$

$$16 = 4xz+11yz+19xw+8yw \tag{4.16}$$

$$2 = 4z^2+11zw+19zw+8w^2 \tag{4.17}$$

$$14 = 17x^2 + 7xy + 8xy + 17y^2 \tag{4.18}$$

$$20 = 17xz + 7xw + 8yz + 17yw \tag{4.19}$$

$$19 = 17xz + 7yz + 8xw + 17yw \tag{4.20}$$

$$15 = 17z^2 + 7zw + 8zw + 17w^2 \tag{4.21}$$

solve the above non-linear system of equation by using ApCoCoA and its in-built tools. We get:

$$w^2 + 3 = 0 \mod 31 \tag{4.22}$$

$$z + 5w = 0 \mod 31 \tag{4.23}$$

$$y + 8w = 0 \mod 31 \tag{4.24}$$

$$x + w = 0 \mod 31 \tag{4.25}$$

while solving these equations algebraically, we may get more than one value for some of unknowns. In this case, one can choose those values of unknowns for which "$A$"becomes involutory $i.e$ $A = A^{-1}$. Solving Equation 4.22, we get:

$$w = 11, 20 \mod 31 \tag{4.26}$$

Fix $w = 20 \mod 31$ and solve Equation 4.23, 4.24 and 4.25, we get:

$$x = 11 \mod 31, \quad y = 26 \mod 31, \quad z = 24 \mod 31. \tag{4.27}$$

From Equation 4.27, we get the following matrix:

$$A = \begin{pmatrix} 11 & 26 \\ 24 & 20 \end{pmatrix} \mod 31.$$

Now fix $w = 11 \mod 31$ and solve Equation 4.23, 4.24 and 4.25, we get:

$$x = 20 \mod 31, \quad y = 5 \mod 31, \quad z = 7 \mod 31. \tag{4.28}$$

From Equation 4.28, we get the following matrix:

$$A = \begin{pmatrix} 20 & 5 \\ 7 & 11 \end{pmatrix} \mod 31.$$

We find out the following keys,

$$\begin{pmatrix} 11 & 26 \\ 24 & 20 \end{pmatrix} \mod 31, \quad \begin{pmatrix} 20 & 5 \\ 7 & 11 \end{pmatrix} \mod 31.$$

As the algorithm is dealing with involutory key, we check each key involution by using ApCoCoA. And both the keys are involutory. Now to check whether the obtained keys satisfy the system of involutory keys.

Hence, we find out the above both are satisfying keys.

Since the encryption and decryption key is unique but here we have two keys which satisfies the ciphertext and plaintext. Following the key generation algorithm, we concluded that first is actual key and the second is equivalent.

# Chapter 5

# Conclusion

In this section, we discuss the strengths and weaknesses of the encryption scheme based on Advanced Hill cipher technique. The scheme is proposed by Acharya et al [22] for the encryption of images.
The use of involutory Key matrix in the proposed scheme helps in encryption/decryption and saves time because the inverse of key is not needed. The two-level Hill cipher is used in the proposed AdvHill cipher technique which points out non-linearity in encryption because of which security of the system is increased. The transpose operation in between two-level Hill cipher adds complexity to the cryptosystem. Nonetheless, the clear difference can be seen between original Hill cipher and the AdvHill cipher technique.

The image encrypted by original Hill cipher, consisting of large area that is covered by gray level or same color, is not encrypted properly. But the AdvHill algorithm proposed by Achariya completely encrypts the images of gray level and also color images. This implies that compared to the original Hill cipher, the proposed AdvHill scheme is more reliable and encrypts the images properly.

Now we observe the weaknesses of the cryptosystem. The complete combined complexity of the proposed AdvHill technique is more than that of the original Hill cipher. As if the key matrix is of order $2 \times 2$, then there will be 4 blocks of matrices of order $2 \times 2$ and each block of the resultant ciphertext requires two matrix multiplication operation and one transpose operation. Since the key $A$ is fixed for one-time pass and is self invertible, the proposed AdvHill algorithm inherits the weaknesses of the original Hill cipher and because of which it cannot resist known plaintext attack. The cryptosystem can become more secure if for every block the key is changed. We have adaptability the keys to choose, as the key space is very large, in a reasonable way.

The scheme proposed against known plaintext attack is weak. We also provided a security analysis for the cipher. Known plaintext attack needs only small amount of computation and it is much faster than searching of the key.

By assuming the key matrix $A$ as a $n \times n$ matrix with $n^2$ unknowns and using the encryption algorithm with known plaintext-ciphertext pairs, we get a non-linear system of $4n^2$ equations in a $n^2$ unknowns. Even with this change made in Hill cipher, the scheme being proposed inherits Hill cipher's weakness. Advanced Hill cipher is vulnerable to known plaintext attack. Moreover, to mount this attack we can choose as many plaintext-ciphertext pairs as we like. So there will be larger number of equations and lesser number of unknowns. Further, the degree of resulting polynomial equations will never exceed 2. Efficient Gröebner basis computation algorithms and softwares are available to solve the resulting system of polynomial equations. See for instance, [41–44] for further details. This cryptosystem remains fragile and vulnerable to attacks.

# Bibliography

[1] O Abraham & GO Shefiu. An improved caesar cipher (icc) algorithm. *International Journal of Engineering Science & Advanced Technology [IJESAT]*, 2:1198–1202, 2012.

[2] T Jakobsen. A fast method for cryptanalysis of substitution ciphers. *Cryptologia*, 19:14–21, 1995.

[3] M. Kundu & S. Ghosh S. Som. A simple algebraic model based polyalphabetic substitution cipher. *Cryptologia*, 19:14–21, 1995.

[4] S.K.N. Kumar H.T. Panduranga. Advanced partial image encryption using two-stage hill cipher technique. *International Journal of Computer Applications*, 60:0975–8887, 2012.

[5] M.T. Thakur M.B. Singh. An analysis over secured image encryption approaches. *International Journal of Engineering Trends & Applications (IJETA)*, 5:0975–8887, 2018.

[6] S.K. Patra S.K. Panigrahy B. Acharya, G.S. Rath. Novel methods of generating self-invertible matrix for hill cipher algorithm. *International Journal of Security*, 1:14–21, 2007.

[7] W. Stallings. *Cryptography and Network Security, 4/E*, volume 4. Pearson Education India, 2006.

[8] J. Daemen & V. Rijmen. *The design of Rijndael: AES-the advanced encryption standard*, volume 1. Springer Science & Business Media, 2013.

[9] B. Schneier. Description of a new variable-length key, 64-bit block cipher (blowfish). In *International Workshop on Fast Software Encryption*, volume 809, pages 191–204. Springer, 1993.

[10] L.M. Kohnfelder. *Towards a practical public-key cryptosystem.* PhD thesis, Massachusetts Institute of Technology, 1978. URL http://hdl.handle.net/1721.1/15993.

[11] T.K. Saha & M.A.A. Bhuiyan M.M. Rahman. Implementation of rsa algorithm for speech data encryption and decryption. *International Journal of Computer Science & Network Security (IJCSNS)*, 12:1–74, 2012.

[12] R. Singh & S. Kumar. Elgamal's algorithm in cryptography. *International Journal of Scientific & Engineering Research*, 3:1–4, 2012.

[13] W. Diffie & M. Hellman. New directions in cryptography. *IEEE transactions on Information Theory*, 22:644–654, 1976.

[14] A.J. Menezes & S. Vanstone D. Hankerson. *Guide to elliptic curve cryptography*, volume 1. Springer Science & Business Media, 2006.

[15] N. Kumar. Investigations in brute force attack on cellular security based on des and aes. *IJCEM International Journal of Computational Engineering & Management*, 14:50–52, 2011.

[16] M. Naor & M. Yung. Public-key cryptosystems provably secure against chosen ciphertext attacks. In *Proceedings of the twenty-second annual ACM symposium on Theory of computing*, volume 3860, pages 427–437. ACM, 1990.

[17] C. Rackoff & D.R. Simon. Non-interactive zero-knowledge proof of knowledge and chosen ciphertext attack. In *Annual International Cryptology Conference*, volume 576, pages 433–444. Springer, 1991.

[18] M. Matsui. Linear cryptanalysis method for des cipher. In *Workshop on the Theory and Application of of Cryptographic Techniques*, volume 765, pages 386–397. Springer, 1993.

[19] T. Siegenthaler. Decrypting a class of stream ciphers using ciphertext only. *IEEE Transactions on computers*, 34:81–85, 1985.

[20] J.J. Rotman. *A first course in abstract algebra*, volume 3. Prentice Hall, 2000.

[21] R. Cohen & M. Campana M. Girault. A generalized birthday attack. volume 330, pages 129–156, 1988.

[22] S.K. Patra B. Acharya, S.K. Panigrahy and G. Panda. Image encryption using advanced hill cipher algorithm. *ACEEE International Journal on Signal and Image Processing*, 1:37–41, 2010.

[23] ApCoCoA Team. Apcocoa: Applied computations in commutative algebra.

[24] K. Ruohonen. Mathematical cryptology. volume 1, pages 1–138. math.tut.fi, 2010.

[25] J.S. Coron. What is cryptography? *IEEE security & privacy*, 4:70–73, 2006.

[26] S. Singh & A. Jaiswal Md.S. Iqbal. Symmetric key cryptography: Technological developments in the field. *International Journal of Computer Applications*, 117:1–4, 2015.

[27] G.S. Kumar. Cryptography using transposition cipher. *Research Journal of Science and Technology*, 9:48–50, 2017.

[28] S. Saeednia. How to make the hill cipher secure. *Cryptologia*, 24:353–360, 2000.

[29] D.T. Lee T.C. Wu, C.L. Lei & V. Rijmen. Information security. In *11th International Conference*, volume 5222, pages 215–227. Springer Science & Business Media, 2008.

[30] A. Joux. *Algorithmic cryptanalysis*, volume 2. Chapman & Hall/CRC, 2009.

[31] M. Joye & M. Tunstall. *Fault analysis in cryptography*, volume 147. Springer, 2012.

[32] F. Grieu. A chosen messages attack on the iso/iec 9796-1 signature scheme. In *International Conference on the Theory and Applications of Cryptographic Techniques*, volume 1807, pages 70–80. Springer, 2000.

[33] J.J. McKinnon. *Hacking: 3 Books in 1: A Beginners Guide for Hackers (How to Hack Websites, Smartphones, Wireless Networks) + Linux Basic for Hackers (Command Line and All the Essentials) + Hacking with Kali Linux.* Independently Published, 2020. ISBN 9798619696806. URL https://www.hackers-arise.com/post/2019/04/30/cryptography-basics-part-2-attack-models-for-cryptanalysis; https://books.google.com.pk/books?id=v-9bzQEACAAJ.

[34] ManageEngine Log360. What is a brute force attack?, 2020. URL https://www.manageengine.com/log-management/cyber-security-attacks/what-is-brute-force-attack.html.

[35] J.B. Fraleigh. *A first course in abstract algebra*, volume 7. Pearson Education India, 2003.

[36] H. Seidl M. Müller-Olm. Analysis of modular arithmetic. *European Symposium on Programming, ESOP*, 15:46–60, 2005.

[37] B. Goddard & K.O'Bryant K.H. Rosen. *Elementary number theory and its applications*, volume 1. Pearson/Addison Wesley, 2005.

[38] P.C. Van Oorschot & S.A. Vanstone A.J.Menezes. *Handbook of Applied Cryptography*, volume 5. CRC press, 1996.

[39] J. Wojdylo J. Overbey, W. Traves. On the keyspace of the hill cipher. *Cryptologia*, 29:59–72, 2005.

[40] S.K. Patra S.K. Panigrahy B. Acharya, G.S. Rath. Novel methods of generating self-invertible matrix for hill cipher algorithm. *International Journal of Security*, 1:14–21, 2007.

[41] C. Edera & J. Perry. F5c: A variant of faugère's f5 algorithm with reduced gröbner bases. *Journal of Symbolic Computation*, 45:1442–1458, 2010.

[42] E. Ullah. *New Techniques for Polynomial System Solving*. PhD thesis, The University of Passau, 2012. URL https://www.researchgate.net/publication/283647835_New_Techniques_for_Polynomial_System_Solving.

[43] M. Kreuzer. Algebraic attacks galore! *Groups Complexity Cryptology*, 1: 231–259, 2010.

[44] P. Pudlak & J. Sgall R. Impaliazzo. Lower bounds for the polynomial calculus and the gröbner basis algorithm. *Groups Complexity Cryptology*, 8:127–144, 1999.

# ApCoCoA Codes for Cryptanalysis of Encryption Scheme based on Advanced Hill Cipher Algorithm

This Appendix contains ApCoCoA Codes for Cryptanalysis of image encryption using advanced hill cipher algorithm.

The calculation of **ModInv**, **InvoMat**, **AlgAttack** is performed in computer algebra system ApCoCoA.

## .1 Modular Inverses

**Algorithm 1**: Modular Inverse

```
Data: Q,M
Result: ModInv (Q,M)
$A1 := 1; A2 := 0; A3 := M;$
$B1 := 0; B2 := 1; B3 := Q;$
while $B3 < 0$ do
    $B3 := B3 + M;$
end
while $B3 <> 1$ do
    $Q := Div(A3, B3);$
    if $Q=0$ then
        Error;
    end
    $T1 := A1 - Q * B1; T2 := A2 - Q * B2; T3 := A3 - Q * B3;$
    $A1 := B1; A2 := B2; A3 := B3;$
    $B1 := T1; B2 := T2; B3 := T3;$
    if $B2 < 0$ then
        $B2 := B2 + M;$
    end
    if $B3 = 1$ then
        return $B2;$
    end
    if $B3 = 0$ then
        return
    end
end
```

## .2 Involutory Matrix

**Algorithm 2**: Involutory Matrix

```
Data: A,M
Result: Involutory Matrix
$I := Mat([[1,0],[0,1]])$;
while $A2 := A^2$ do
    $A2R := NewMat(2,2)$;
    for $I := 1To2$ do
        for $J := 1To2$ do
            $A2R[I][J] := Mod(A2[I][J], M)$;
        end
    end
    return $A2R = I$ ;
end
```

## .3 Algebraic Attack

**Algorithm 3**: Algebraic Attack

```
**Data**: P,C
**Result**: AlgAttack (P,C)
while AlgAttack (P,C) do
    $K := Mat([[x, y], [z, w]]);$
    $M := []; N := 1;$
    foreach A In P $C2 := K * Transposed(K * A);$
    $Cipher := C[N];$
    for I := 1 To 2 do
        for J := 1 To 2 do
            $Append(M, C2[I][J] - Cipher[I][J]);$
        end
    end
    $N := N + 1$  return ReducedGBasis ( Ideal (M ))
end
```