International Journal of Mathematical Sciences
Vol. 16, Nos. 4, October-December 2017, pp. 279-292

ISSN: 0972-754X

PERFORMANCE ANALYSIS OF IMPROVED ENCIPHERING MATRICES

***Anooja. I*[1]*, Vinod. S*[2] *and Biju. G. S*[3]**

Abstract: Cryptography is the art of disguising data in order to share it through the in secure channel. In this paper, a novel encryption technique has been proposed and a comparative study of the proposed encryption scheme and the existing Hill cipher scheme is made. The output encrypted reveal that the proposed technique is quite reliable and robust.

Keywords: plaintext, ciphertext, enciphering, deciphering, cryptosystem

2010 AMS subject classifications: 94A60, 08A70, 08A62

1. Introduction

Hill Cipher is a symmetric cryptosystem that splits the plain text into a block of letters of a fixed size and then each block is converted into a disparate blocks of letters. Hill cipher is a block cipher that has several advantages such as disguising letter frequencies of the plaintext, its simplicity because of using matrix multiplication and inversion for enciphering and deciphering, its high speed and high throughput (see [1, 2, 3, 4, 5, 6]).

An enciphering transformation is a function *f* that converts any plaintext message into a cipher text message and deciphering transformation is a function f^{-1}, which reverse the process. Such a set-up is called a cryptosystem. In the process of developing a cryptosystem, first label all possible plaintext and cipher text message units by mathematical objects from which functions can be easily constructed. To facilitate rapid enciphering and deciphering, it is convenient to have a rule for performing a rearrangement of N integers $0,1,2,...,N-1$ as enciphering transformation and use the operations addition and multiplication modulo *N*. $\mathbb{Z}/N\mathbb{Z}$ is a ring, but it is not a field unless *N* is prime.

There are several cryptosystems in which matrix techniques are involved. Here we discuss some new techniques for enciphering and deciphering using matrices, which is more secure. In these methods also, the sender and receiver must agree with the matrix used for enciphering and deciphering before sending the message as in the existing techniques. In this paper, we discuss some systems for enciphering and deciphering using matrices with new techniques. The advantage of these systems is to maintain more security of the system.

IMPROVED HILL CIPHER TECHNIQUES

Most of the notations, definitions and results we mentioned here are standard and can be found in [7] and [8].

First Method

Suppose we have to send a message consists of *N* alphabets. First, consider a matrix $A \in M_n\left(\mathbb{Z}/N\mathbb{Z}\right)$, $n \in \mathrm{N}$ such that the determinant has no common factor with *N*.

$$\text{Let } A = \begin{bmatrix} a_{11} & a_{12} & . & . & . & a_{1n} \\ a_{21} & a_{22} & . & . & . & a_{2n} \\ . & . & & . & & . \\ . & . & & . & & . \\ . & . & & . & & . \\ a_{n1} & a_{n2} & . & . & . & a_{nn} \end{bmatrix} \text{ and } D = \det A \in \left(\mathbb{Z}/N\mathbb{Z}\right)^{*}.$$

Let D^{-1} denote the multiplicative inverse of *D* in $\mathbb{Z}/N\mathbb{Z}$.

In order to enciphering the message, we use the following techniques. Since the matrix under our consideration is an $n \times n$ matrix, group the letter occurring in the plaintext as *n* blocks with equal block length. Let it be *k*. If the length of the last block is less than *k*, we can add sufficient special characters to make the length of this block is also as *k*.

Then label each letter in the blocks by their numerical equivalents. i.e., each block corresponds to its numerical equivalents $\begin{bmatrix} x_{11} & x_{12} & . & . & . & x_{1k} \end{bmatrix}$ where each x_{ij} represents the additive inverse modulo *N* of each letter's numerical equivalent.

Then the plaintext can be expressed as the form

$$\mathrm{P} = \begin{bmatrix} x_{11} & x_{12} & . & . & . & x_{1k} \\ x_{21} & x_{22} & . & . & . & x_{2k} \\ . & . & & . & & . \\ . & . & & . & & . \\ . & . & & . & & . \\ x_{n1} & x_{n2} & . & . & . & x_{nk} \end{bmatrix}.$$

This can be converted in to a ciphertext by using the relation $C = A\mathrm{P}$, where

$$C = \begin{bmatrix} x_{11}' & x_{12}' & \cdot\;\cdot\;\cdot & x_{1k}' \\ x_{21}' & x_{22}' & \cdot\;\cdot\;\cdot & x_{2k}' \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ x_{n1}' & x_{n2}' & \cdot\;\cdot\;\cdot & x_{nk}' \end{bmatrix}$$

For deciphering, first we have to find out A^{-1} and then substitute A^{-1} in the relation $\mathrm{P} = A^{-1}C$.

$$\begin{bmatrix} x_{11} & x_{12} & \cdot\;\cdot\;\cdot & x_{1k} \\ x_{21} & x_{22} & \cdot\;\cdot\;\cdot & x_{2k} \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ x_{n1} & x_{n2} & \cdot\;\cdot\;\cdot & x_{nk} \end{bmatrix} = \begin{bmatrix} D^{-1}c_{11} & D^{-1}c_{12} & \cdot\;\cdot\;\cdot & D^{-1}c_{1n} \\ D^{-1}c_{21} & D^{-1}c_{22} & \cdot\;\cdot\;\cdot & D^{-1}c_{2n} \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ D^{-1}c_{n1} & D^{-1}c_{n2} & \cdot\;\cdot\;\cdot & D^{-1}c_{nn} \end{bmatrix}$$

$$\begin{bmatrix} x_{11}' & x_{12}' & \cdot\;\cdot\;\cdot & x_{1k}' \\ x_{21}' & x_{22}' & \cdot\;\cdot\;\cdot & x_{2k}' \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ x_{n1}' & x_{n2}' & \cdot\;\cdot\;\cdot & x_{nk}' \end{bmatrix}$$

where c_{ji} is the cofactor of a_{ij}.

Example

Suppose, ‘A’ wants to send the following message to, ‘B’.

“ HAND OVER THE DIAMONDS TOMORROW ”

For, consider $N = 26$ and choose $A = \begin{bmatrix} 03 & 01 & 05 \\ 07 & 03 & 02 \\ 04 & 09 & 01 \end{bmatrix} \in M_3(\mathbb{Z}/26\mathbb{Z})$, arbitrarily.

Clearly, $D = \det A = 3$ and $(D, 26) = (3, 26) = 1$.

Also, $D^{-1} = 3^{-1} = 9$ (w.r.to modulo 26).

Now, group the letters in the message into 3 blocks of equal length, then the plaintext becomes

HANDOVERT HEDIAMOND STOMORROW

and the corresponding matrix of P as per our rule (additive inverse modulo *N*) is

$$\mathrm{P} = \begin{bmatrix} 19 & 00 & 13 & 23 & 12 & 05 & 22 & 09 & 07 \\ 19 & 22 & 23 & 18 & 00 & 14 & 12 & 13 & 23 \\ 08 & 07 & 12 & 14 & 12 & 09 & 09 & 12 & 04 \end{bmatrix}$$

Now, $C = A\mathrm{P}$ becomes

$$\begin{bmatrix} 03 & 01 & 05 \\ 07 & 03 & 02 \\ 04 & 09 & 01 \end{bmatrix} \begin{bmatrix} 19 & 00 & 13 & 23 & 12 & 05 & 22 & 09 & 07 \\ 19 & 22 & 23 & 18 & 00 & 14 & 12 & 13 & 23 \\ 08 & 07 & 12 & 14 & 12 & 09 & 09 & 12 & 04 \end{bmatrix}$$

$$= \begin{bmatrix} 12 & 05 & 18 & 01 & 18 & 22 & 19 & 22 & 12 \\ 24 & 02 & 02 & 09 & 04 & 17 & 00 & 22 & 22 \\ 21 & 23 & 11 & 08 & 08 & 25 & 23 & 09 & 05 \end{bmatrix}$$

The corresponding ciphertext is

OVIZIEHEO CYYRWJAEE FDPSSBDRV

Then send this to B. After receiving this message by B, B have to calculate A^{-1} and use the relation $\mathrm{P} = A^{-1}C$ for deciphering.

Since $A^{-1} = \begin{bmatrix} 21 & 06 & 13 \\ 09 & 03 & 01 \\ 17 & 01 & 18 \end{bmatrix}$, $\mathrm{P} = A^{-1}C$ becomes

$$\begin{bmatrix} 21 & 06 & 13 \\ 09 & 03 & 01 \\ 17 & 01 & 18 \end{bmatrix} \begin{bmatrix} 12 & 05 & 18 & 01 & 18 & 22 & 19 & 22 & 12 \\ 24 & 02 & 02 & 09 & 04 & 17 & 00 & 22 & 22 \\ 21 & 23 & 11 & 08 & 08 & 25 & 23 & 09 & 05 \end{bmatrix}$$

$$= \begin{bmatrix} 19 & 00 & 13 & 23 & 12 & 05 & 22 & 09 & 07 \\ 19 & 22 & 23 & 18 & 00 & 14 & 12 & 13 & 23 \\ 08 & 07 & 12 & 14 & 12 & 09 & 09 & 12 & 04 \end{bmatrix}$$

i.e., P = HAND OVER THE DIAMONDS TOMORROW, that is what is the plaintext.

Second Method

Next, we give a more secured technique for enciphering and deciphering, which differs from the technique we applied in the previous method.

Suppose we have to send a message consists of *N* alphabets. First, consider a matrix $A \in M_n(\mathbb{Z}/N\mathbb{Z})$, $n \in$ □ such that the determinant has no common factor with *N*.

$$\text{Suppose} \quad A = \begin{bmatrix} a_{11} & a_{12} & . & . & . & a_{1n} \\ a_{21} & a_{22} & . & . & . & a_{2n} \\ . & . & & & . & . \\ . & . & & & . & . \\ . & . & & & . & . \\ a_{n1} & a_{n2} & . & . & . & a_{nn} \end{bmatrix} \quad \text{and } D = \det A \in (\mathbb{Z}/N\mathbb{Z})^{*}.$$

Let D^{-1} denote the multiplicative inverse of *D* in $\mathbb{Z}/N\mathbb{Z}$.

In order to enciphering the message, we use the following techniques. Since the matrix under our consideration is an $n \times n$ matrix, group the letter occurring in the plaintext as *n* blocks with equal block length. Let it be *k*. If the length of the last block is less than *k*, we can add sufficient special characters to make the length of this block *k*. Then regroup the blocks into *k* new blocks each of length *n* in which each block is formed by the letters in the corresponding position in the existing blocks. Then label each letter in the blocks by their numerical equivalents. i.e., each block corresponds to its numerical equivalents $\begin{bmatrix} x_{11} \\ x_{21} \\ . \\ . \\ . \\ x_{n1} \end{bmatrix}$

where each x_{ij} considered additive inverse modulo N of each letter's numerical equivalent. Then the plaintext can be expressed as the form

$$\mathrm{P} = \begin{bmatrix} x_{11} & x_{12} & . & . & . & x_{1k} \\ x_{21} & x_{22} & . & . & . & x_{2k} \\ . & . & & . & & . \\ . & . & & . & & . \\ . & . & & . & & . \\ x_{n1} & x_{n2} & . & . & . & x_{nk} \end{bmatrix}.$$

This can be converted in to a ciphertext by using the relation $C = A\mathrm{P}$, where

$$C = \begin{bmatrix} x_{11}' & x_{12}' & . & . & . & x_{1k}' \\ x_{21}' & x_{22}' & . & . & . & x_{2k}' \\ . & . & & . & & . \\ . & . & & . & & . \\ . & . & & . & & . \\ x_{n1}' & x_{n2}' & . & . & . & x_{nk}' \end{bmatrix}$$

i.e.,
$$\begin{bmatrix} x_{11}' & x_{12}' & . & . & . & x_{1k}' \\ x_{21}' & x_{22}' & . & . & . & x_{2k}' \\ . & . & & . & & . \\ . & . & & . & & . \\ . & . & & . & & . \\ x_{n1}' & x_{n2}' & . & . & . & x_{nk}' \end{bmatrix} = \begin{bmatrix} a_{11} & a_{12} & . & . & . & a_{1n} \\ a_{21} & a_{22} & . & . & . & a_{2n} \\ . & . & & . & & . \\ . & . & & . & & . \\ . & . & & . & & . \\ a_{n1} & a_{n2} & . & . & . & a_{nn} \end{bmatrix}$$
$$\begin{bmatrix} x_{11} & x_{12} & . & . & . & x_{1k} \\ x_{21} & x_{22} & . & . & . & x_{2k} \\ . & . & & . & & . \\ . & . & & . & & . \\ . & . & & . & & . \\ x_{n1} & x_{n2} & . & . & . & x_{nk} \end{bmatrix}$$

For deciphering, first we have to calculate A^{-1} and then substitute A^{-1} in the relation $\mathrm{P} = A^{-1}C$.

i.e.,
$$\begin{bmatrix} x_{11} & x_{12} & . & . & . & x_{1k} \\ x_{21} & x_{22} & . & . & . & x_{2k} \\ . & . & & . & & . \\ . & . & & . & & . \\ . & . & & . & & . \\ x_{n1} & x_{n2} & . & . & . & x_{nk} \end{bmatrix} = \begin{bmatrix} D^{-1}c_{11} & D^{-1}c_{12} & . & . & . & D^{-1}c_{1n} \\ D^{-1}c_{21} & D^{-1}c_{22} & . & . & . & D^{-1}c_{2n} \\ . & . & & . & & . \\ . & . & & . & & . \\ . & . & & . & & . \\ D^{-1}c_{n1} & D^{-1}c_{n2} & . & . & . & D^{-1}c_{nn} \end{bmatrix}$$
$$\begin{bmatrix} x_{11}' & x_{12}' & . & . & . & x_{1k}' \\ x_{21}' & x_{22}' & . & . & . & x_{2k}' \\ . & . & & . & & . \\ . & . & & . & & . \\ . & . & & . & & . \\ x_{n1}' & x_{n2}' & . & . & . & x_{nk}' \end{bmatrix}$$

where c_{ji} is the cofactor of a_{ij}.

Then regroup the text to get the original message.

Example

Suppose, ‘A’ wants to send the following message to, ‘B’.

“ HAND OVER THE DIAMONDS TOMORROW ”

For, consider $N = 26$ and choose $A = \begin{bmatrix} 03 & 01 & 05 \\ 07 & 03 & 02 \\ 04 & 09 & 01 \end{bmatrix} \in M_3\left(\mathbb{Z}/26\mathbb{Z}\right)$, arbitrarily.

Clearly, $D = \det A = 3$ and $\left(D, 26\right) = \left(3, 26\right) = 1$.

Also, $D^{-1} = 3^{-1} = 9$ (w.r.to modulo 26).

Now, group the letters in the message into 3 blocks of equal length, then the plaintext becomes

HANDOVERT HEDIAMOND STOMORROW

Then regroup these blocks as follows

HHS AET NDO DIM OAO VMR EOR RNO TDW

and the corresponding matrix of P as per our rule is

$$\mathrm{P} = \begin{bmatrix} 19 & 00 & 13 & 23 & 12 & 05 & 22 & 09 & 07 \\ 19 & 22 & 23 & 18 & 00 & 14 & 12 & 13 & 23 \\ 08 & 07 & 12 & 14 & 12 & 09 & 09 & 12 & 04 \end{bmatrix}$$

Now, $C = A\mathrm{P}$ becomes

$$\begin{bmatrix} 03 & 01 & 05 \\ 07 & 03 & 02 \\ 04 & 09 & 01 \end{bmatrix} \begin{bmatrix} 19 & 00 & 13 & 23 & 12 & 05 & 22 & 09 & 07 \\ 19 & 22 & 23 & 18 & 00 & 14 & 12 & 13 & 23 \\ 08 & 07 & 12 & 14 & 12 & 09 & 09 & 12 & 04 \end{bmatrix}$$

$$= \begin{bmatrix} 12 & 05 & 18 & 01 & 18 & 22 & 19 & 22 & 12 \\ 24 & 02 & 02 & 09 & 04 & 17 & 00 & 22 & 22 \\ 21 & 23 & 11 & 08 & 08 & 25 & 23 & 09 & 05 \end{bmatrix}$$

The corresponding ciphertext is

OCF VYD IYP ZRS IWS EJB HAD EER OEV

Then send this to B. After receiving this message by B, B have to calculate A^{-1} and use the relation $\mathrm{P} = A^{-1}C$ for deciphering.

Since $A^{-1} = \begin{bmatrix} 21 & 06 & 13 \\ 09 & 03 & 01 \\ 17 & 01 & 18 \end{bmatrix}$, $\mathrm{P} = A^{-1}C$ becomes

$$\begin{bmatrix} 21 & 06 & 13 \\ 09 & 03 & 01 \\ 17 & 01 & 18 \end{bmatrix} \begin{bmatrix} 12 & 05 & 18 & 01 & 18 & 22 & 19 & 22 & 12 \\ 24 & 02 & 02 & 09 & 04 & 17 & 00 & 22 & 22 \\ 21 & 23 & 11 & 08 & 08 & 25 & 23 & 09 & 05 \end{bmatrix}$$

$$= \begin{bmatrix} 19 & 00 & 13 & 23 & 12 & 05 & 22 & 09 & 07 \\ 19 & 22 & 23 & 18 & 00 & 14 & 12 & 13 & 23 \\ 08 & 07 & 12 & 14 & 12 & 09 & 09 & 12 & 04 \end{bmatrix}$$

i.e., P = HHS AET NDO DIM OAO VMR EOR RNO TDW

Then regroup these blocks, we get

P = HAND OVER THE DIAMONDS TOMORROW, that is what is the plaintext.

Third Method

In the previous two methods we considered an arbitrary matrix *A*. But, in this section, we insert a new technique that instead of *A*, we take A^T (the transpose of *A*) which will strengthen the security more.

Suppose we have to send a message consists of *N* alphabets. First, consider a matrix $A \in M_n(\mathbb{Z}/N\mathbb{Z})$, $n \in$ □ such that the determinant has no common factor with *N*.

Let $A = \begin{bmatrix} a_{11} & a_{12} & \cdot & \cdot & \cdot & a_{1n} \\ a_{21} & a_{22} & \cdot & \cdot & \cdot & a_{2n} \\ \cdot & \cdot & & \cdot & & \cdot \\ \cdot & \cdot & & \cdot & & \cdot \\ \cdot & \cdot & & \cdot & & \cdot \\ a_{n1} & a_{n2} & \cdot & \cdot & \cdot & a_{nn} \end{bmatrix}$ and $D = \det A \in (\mathbb{Z}/N\mathbb{Z})^*$.

Let D^{-1} denote the multiplicative inverse of D in $\mathbb{Z}/N\mathbb{Z}$.

In order to enciphering the message, we use the following techniques. Since the matrix under our consideration is an $n \times n$ matrix, group the letter occurring in the plaintext as *n* blocks with equal block length. Let it be *k*. If the length of the last block is less than *k*, we can add sufficient special characters (punctuation marks, symbols etc.) to make the length of this block is also as *k*. Then label each letter in the blocks by their numerical equivalents. i.e., each block corresponds to its numerical equivalents $\begin{bmatrix} x_{11} & x_{12} & . & . & . & x_{1k} \end{bmatrix}$ where each x_{ij} considered additive inverse modulo *N* of each letter's numerical equivalent. Then the plaintext can be expressed as the form

$$\mathrm{P} = \begin{bmatrix} x_{11} & x_{12} & . \; . \; . & x_{1k} \\ x_{21} & x_{22} & . \; . \; . & x_{2k} \\ . & . & . & . \\ . & . & . & . \\ . & . & . & . \\ x_{n1} & x_{n2} & . \; . \; . & x_{nk} \end{bmatrix}.$$

This can be converted in to a ciphertext by using the relation $C = A^T\mathrm{P}$, where

$$C = \begin{bmatrix} x_{11}' & x_{12}' & . \; . \; . & x_{1k}' \\ x_{21}' & x_{22}' & . \; . \; . & x_{2k}' \\ . & . & . & . \\ . & . & . & . \\ . & . & . & . \\ x_{n1}' & x_{n2}' & . \; . \; . & x_{nk}' \end{bmatrix}$$

(since $\det A = \det A^T$, A^T satisfies the necessary conditions of the matrix which is needed for enciphering and deciphering).

i.e.,

$$\begin{bmatrix} x_{11}' & x_{12}' & . & . & . & x_{1k}' \\ x_{21}' & x_{22}' & . & . & . & x_{2k}' \\ . & . & & . & & . \\ . & . & & . & & . \\ . & . & & . & & . \\ x_{n1}' & x_{n2}' & . & . & . & x_{nk}' \end{bmatrix} = \begin{bmatrix} a_{11} & a_{12} & . & . & . & a_{1n} \\ a_{21} & a_{22} & . & . & . & a_{2n} \\ . & . & & . & & . \\ . & . & & . & & . \\ . & . & & . & & . \\ a_{n1} & a_{n2} & . & . & . & a_{nn} \end{bmatrix}$$

$$\begin{bmatrix} x_{11} & x_{12} & . & . & . & x_{1k} \\ x_{21} & x_{22} & . & . & . & x_{2k} \\ . & . & & . & & . \\ . & . & & . & & . \\ . & . & & . & & . \\ x_{n1} & x_{n2} & . & . & . & x_{nk} \end{bmatrix}$$

For deciphering, first we have to calculate A^{-1} and then substitute A^{-1} in the relation $\mathrm{P} = \left(A^{-1}\right)^T C$ (since $\left(A^{-1}\right)^T = \left(A^T\right)^{-1}$).

$$\begin{bmatrix} x_{11} & x_{12} & . & . & . & x_{1k} \\ x_{21} & x_{22} & . & . & . & x_{2k} \\ . & . & & . & & . \\ . & . & & . & & . \\ . & . & & . & & . \\ x_{n1} & x_{n2} & . & . & . & x_{nk} \end{bmatrix} = \begin{bmatrix} D^{-1}c_{11} & D^{-1}c_{12} & . & . & . & D^{-1}c_{1n} \\ D^{-1}c_{21} & D^{-1}c_{22} & . & . & . & D^{-1}c_{2n} \\ . & . & & . & & . \\ . & . & & . & & . \\ . & . & & . & & . \\ D^{-1}c_{n1} & D^{-1}c_{n2} & . & . & . & D^{-1}c_{nn} \end{bmatrix}$$

$$\begin{bmatrix} x_{11}' & x_{12}' & . & . & . & x_{1k}' \\ x_{21}' & x_{22}' & . & . & . & x_{2k}' \\ . & . & & . & & . \\ . & . & & . & & . \\ . & . & & . & & . \\ x_{n1}' & x_{n2}' & . & . & . & x_{nk}' \end{bmatrix}$$

where c_{ij} is the cofactor of a_{ij}.

Example

Suppose, 'A' wants to send the following message to, 'B'.

" HAND OVER THE DIAMONDS TOMORROW "

For, consider $N = 26$ and choose $A = \begin{bmatrix} 03 & 01 & 05 \\ 07 & 03 & 02 \\ 04 & 09 & 01 \end{bmatrix} \in M_3(\mathbb{Z}/26\mathbb{Z})$, arbitrarily.

Clearly, $D = \det A = 3$ and $(D, 26) = (3, 26) = 1$.

Also, $D^{-1} = 3^{-1} = 9$ (w.r.to modulo 26).

Now, group the message into 3 blocks of equal length, then the plaintext becomes

HANDOVERT HEDIAMOND STOMORROW

and the corresponding matrix of P as per our rule is

$$\mathrm{P} = \begin{bmatrix} 19 & 00 & 13 & 23 & 12 & 05 & 22 & 09 & 07 \\ 19 & 22 & 23 & 18 & 00 & 14 & 12 & 13 & 23 \\ 08 & 07 & 12 & 14 & 12 & 09 & 09 & 12 & 04 \end{bmatrix}$$

Now, $C = A^T \mathrm{P}$ becomes

$$\begin{bmatrix} 03 & 07 & 04 \\ 01 & 03 & 09 \\ 05 & 02 & 01 \end{bmatrix} \begin{bmatrix} 19 & 00 & 13 & 23 & 12 & 05 & 22 & 09 & 07 \\ 19 & 22 & 23 & 18 & 00 & 14 & 12 & 13 & 23 \\ 08 & 07 & 12 & 14 & 12 & 09 & 09 & 12 & 04 \end{bmatrix}$$

$$= \begin{bmatrix} 14 & 00 & 14 & 17 & 06 & 19 & 04 & 10 & 16 \\ 18 & 25 & 08 & 21 & 16 & 24 & 09 & 00 & 08 \\ 11 & 25 & 19 & 09 & 20 & 10 & 13 & 05 & 07 \end{bmatrix}$$

The corresponding ciphertext is

MAMJUHWQK IBSFKCRAS PBHRGQNVT

Then send this to B. After receiving this message by B, B have to calculate A^{-1} and use the relation $\mathrm{P} = \left(A^{-1}\right)^T C$ for deciphering.

Since $A^{-1} = \begin{bmatrix} 21 & 06 & 13 \\ 09 & 03 & 01 \\ 17 & 01 & 18 \end{bmatrix}$, $\mathrm{P} = \left(A^{-1}\right)^{T} C$ becomes

$$\begin{bmatrix} 21 & 09 & 17 \\ 06 & 03 & 01 \\ 13 & 01 & 18 \end{bmatrix} \begin{bmatrix} 14 & 00 & 14 & 17 & 06 & 19 & 04 & 10 & 16 \\ 18 & 25 & 08 & 21 & 16 & 24 & 09 & 00 & 08 \\ 11 & 25 & 19 & 09 & 20 & 10 & 13 & 05 & 07 \end{bmatrix}$$

$$= \begin{bmatrix} 19 & 00 & 13 & 23 & 12 & 05 & 22 & 09 & 07 \\ 19 & 22 & 23 & 18 & 00 & 14 & 12 & 13 & 23 \\ 08 & 07 & 12 & 14 & 12 & 09 & 09 & 12 & 04 \end{bmatrix}$$

i.e., P = HAND OVER THE DIAMONDS TOMORROW, that is what is the plaintext.

Techniques used in each method is more secure than the predecessor one. In all these three methods it would be computationally infeasible to systematically determine plaintext from intercepted ciphertext. Even if the ciphertext is known, it should be computationally infeasible to determine the deciphering algorithm.

REFERENCES

[1] Lester S Hill. Cryptography in an algebraic alphabet, The American Mathematical Monthly, 36(6):306–312, 1929.

[2] Lester S Hill. Concerning certain linear transformation apparatus of cryptography, The American Mathematical Monthly, 38(3):135–154, 1931.

[3] Rushdi Hamamreh and Mousa Farajallah, Design of a robust cryptosystem algorithm for non-invertible matrices based on hill cipher. 9(5):1–16, 2009.

[4] IA Ismail, Mohammed Amin, and Hossam Diab, How to repair the hill cipher. Journal of Zhejiang University-Science A, 7(12):2022–2030, 2006.

[5] Jeffrey Overbey, William Traves, and Jerzy Wojdylo, On the keyspace of the hill cipher. Cryptologia, 29(1):59–72, 2005.

[6] Adam J Elbirt and Christof Paar, An instruction-level distributed processor for symmetric-key cryptography. IEEE Transactions on Parallel and distributed Systems, 16(5):468–480, 2005.

[7] Neal Koblitz. Algebraic methods of cryptography, Berlin Heidelberg New York: Springer, 1998.

[8] Alfred J Menezes, Paul C Van Oorschot, and Scott A Vanstone, Handbook of Applied Cryptography. Discrete Mathematics and Its Applications. CRC press, New York, 1996.

Anooja. I
Department of Mathematics,
CMS College Kottayam (Autonomous),
Kottayam, Kerala, India

Vinod.S
Department of Mathematics,
Government College for Women,
Thiruvananthapuram, Kerala, India

Biju.G.S
Department of Mathematics,
College of Engineering,
Thiruvananthapuram, Kerala, India