Menemui Matematik
(Discovering Mathematics)

journal homepage: https://myjms.mohe.gov.my/index.php/dismath/

Exploring Self-Invertible 3 × 3 Matrices for Cipher Trigraphic Polyfunction with Distinct Encryption Keys

Faridah Yunos[1], Ummu Zulaikha Zulkifli[2*], Syakirah Ibrahim[3], Muhammad Asyraf Asbullah[4] and Witriany Basri[5]

[1,2,3,5]*Department of Mathematics and Statistics, Universiti Putra Malaysia, 43400 UPM Serdang, Selangor*
[4]*Institute For Mathematical Research, Universiti Putra Malaysia, 43400 UPM Serdang, Selangor*
[4]*Centre of Foundation Studies for Agriculture Science, Universiti Putra Malaysia, 43400 UPM Serdang,Selangor.*

[1]faridahy@upm.edu.my, [2]ummu.zulkifli13@gmail.com
*Corresponding author

Received: 7 July 2024
Accepted: 27 October 2024

ABSTRACT

The encryption keys with self-invertible matrix in Hill Cipher cryptography and its extension, have been proven through various studies reducing the complexity of obtaining its inverse. Several methods to generate these keys have been applied to specific systems. This paper aims to find a submatrix *id2* as a basis for generating self-invertible keys. Then, these keys are successfully implemented on a Cipher Trigraphic Polyfunction cryptosystem, which uses different encryption keys for each transformation.

Keywords: Cipher Trigraphic Polyfunction, Self-invertible Matrix, Different Encryption Keys

INTRODUCTION

Cryptography is referred to as the science or study of secret writing methods. It is the act of converting an understandable message (plaintext) into an incomprehensible message (ciphertext), and then returning the latter to the former, using concepts and techniques. The root of the word cryptography, crypt- is from the Greek language which means hidden or secret. In its earliest forms, people have tried to hide information they intended to keep to themselves by rearranging information so that symbols, numbers, and pictures are used in place of particular pieces.

According to Jackob (2001), today's cryptosystems are divided into two categories which are symmetric and asymmetric cryptosystems. Symmetric cryptosystems use the same key (the secret key) to encrypt and decode a message, while asymmetric cryptosystems use one key (the public key) to encrypt a message and a different key (the private key) to decrypt it. Public key cryptosystems are another name for asymmetric cryptosystems. The internet is not only considered the primary source of up-to-date information, but it is also utilized for business transactions, the sale of goods, and product advertising. Business can be conducted since it facilitates customer communication and all financial activities. Hence, the need to secure communications from prying eyes is more important than ever in today's technologically advanced world.

Hill Cipher is a symmetric polygraphic cipher based on linear algebra. It was first established by Hill (1929). It has been applied in cryptology to encrypt plaintext letters of order m into cipher letters which are based $\mathbb{Z}_m$ and then decrypt them back from ciphertext to plaintext. The encryption process can be expressed by $C \equiv KP (\mathrm{mod}\ m)$ where K represents a secret key matrix, P as plaintext, and C as ciphertext. Meanwhile, the decryption process can be expressed by $P \equiv K^{-1}C (\mathrm{mod}\ m)$ where the values of m can be any positive integers. In general, there are only some square matrices that are invertible over $\mathbb{Z}_m$. However, this algorithm has a weakness which is a known plaintext attack. During this attack, the adversary has both plaintext and its ciphertext version. This can be used to leak further secretive information.

According to Yeh et al. (1991), a novel polygraph substitution cryptosystem was used to defeat the known plaintext attack. The main characteristics of the system were that system used a number system with different bases and enforced the matrices transformation. The process of encryption and decryption are simple to use and suitable for parallel processing. The design of encoding and decoding devices is also available. This method succeeds in defeating known plaintext attacks. However, it has many mathematical modifications which result in time consuming and inefficient when it comes for dealing with large numbers of data.

A study by Overbey et al. (2005) is working on establishing formulas to compute the total number of matrices, the number of invertible matrices, and the number of involutory matrices over $\mathbb{Z}_m$ for any modulus m from known results of finite fields. Then, the result is compared with the total number of matrices and the number of involutory matrices for a given dimension and modulus, identifying the effects of change in dimension and modulus on the order of the keyspace. By observing the result, there is a rise of the dimension of key matrices which leads to a bigger keyspace which results from a large matrix dimension and an alphabet of prime order.

Next, Acharya et al. (2007) proposed some methods of generating a self-invertible matrix for the Hill Cipher algorithm. The inverse of an encryption key does not always exist. If the key is not invertible, the encrypted text cannot be decrypted. There are some techniques to generate self-invertible matrices in order to eliminate the computational complexity for finding the inverse of encryption matrices. The detail of one of these techniques is presented in Section 4. The proposed methods was also used by some researchers such as Acharya et al. (2009), Yunos et al. (2018), Ching and Yunos (2019) and Yunos et al. (2023).

Acharya et al. (2009) continues the study to fix the original flaws of Hill Cipher which is known plaintext attacks by introducing involutory, permuted, and reiterative key matrices generation methods. The involutory matrix generation method deals with the key matrix inversion problem. Meanwhile, the permuted and reiterative matrices generation methods improve the system security because they can generate different patterns of keys for each plaintext encryption.

Wikramaratna (2011) defined a new type of matrix, called centro-invertible matrix where the inverse of the matrix can be found by rotating all the elements of the matrix through $180°$ about the mid-point of the matrix. They discussed the relationship between centro-invertible and involutory matrices and showed that there is a one-to-one correspondence between both of the matrices. The result allows all possible k by k centro-invertible matrices with integer entries modulo M to be enumerated by drawing on existing theoretical results for involutory matrices when working with modular arithmetic.

Yunos et al. (2018) worked on the solutions of the self-invertible matrix for Cipher Tetragraphic Trifunction by using methods from Acharya et al. (2007). However, they consider

$C_{4\times j}^{(t)} \equiv L_{4\times 4}^{(t)} P_{4\times j} (\mathrm{mod}\ N)$ where $C_{4\times j}$, $P_{4\times j}$ and $L_{4\times 4}$ are ciphertext, plaintext and encryption key respectively. Whereas, (t) represents the number of transformations of encryption for $t \in \{1,2,3\}$. Some solutions for self-invertible matrix $L_{2\times 2}^{3} \equiv A_{2\times 2} (\mathrm{mod}\ N)$ are obtained when $A_{2\times 2}$ is considered as $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} e & f \\ 0 & 0 \end{bmatrix}$ and $\begin{bmatrix} e & f \\ 0 & h \end{bmatrix}$ matrices. Self-invertible generating method form Acharya et al. (2007) is implemented to get a self-invertible 4×4 matrix. From there, ten types of self-invertible keys, $L_{4\times 4}$ are established. From this result, they generated $L_{4\times 4}$ from $L_{2\times 2}$ in the form of

$$L_{4\times 4} \equiv \begin{bmatrix} L_{2\times 2} & I - L_{2\times 2}) \\ (I + L_{2\times 2}) & -L_{2\times 2} \end{bmatrix} (\mathrm{mod}\ N)$$

with condition $L_{2\times 2} = A_{11}$ should be avoided as it caused a repeating process in the cryptosystem.

In the following year, Ching and Yunos (2019) made a research on the effect of self-invertible matrix on Cipher Hexagraphic Polyfunction with similar encryption key for each transformation, but they consider $C_{6\times j}^{(t)} \equiv L_{6\times 6}^{(t)} P_{6\times j} (\mathrm{mod}\ N)$. In this system, the sender of messages kept the parameters $\left(A_{6\times 6}, (t)\right)$ as secret. The main objective of this research was to secure some patterns of the self-invertible matrices $L_{6\times 6}$ and observe the effect when applying it to the Cipher Hexagraphic Polyfunction transformation system. There are nine solutions of $L_{3\times 3}$ were obtained from $L_{3\times 3}^{2} \equiv A_{3\times 3} (\mathrm{mod}\ N)$ where $A_{3\times 3}$ is a diagonal and symmetric matrices. Then, they generated $L_{6\times 6}$ from $L_{3\times 3}$ in the form of

$$L_{6\times 6} \equiv \begin{bmatrix} L_{3\times 3} & (I - L_{3\times 3}) \\ (I + L_{3\times 3}) & -L_{3\times 3} \end{bmatrix} (\mathrm{mod}\ N).$$

After observing the patterns, it was found that plaintext would be easily obtained by the adversary if these encryption keys were used in the system. It was due to the repeating process of the self-invertible encryption keys in the system. From there, nine self-invertible matrices, $L_{6\times 6}$ were generated.

Yunos et al. (2023) worked on solutions of $L_{2\times 2}^{2} \equiv A_{2\times 2} (\mathrm{mod}\ N)$ where matrix $A_{2\times 2}$ act as public key with six categories which are $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} e & f \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & f \\ 0 & h \end{bmatrix}, \begin{bmatrix} e & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 0 & h \end{bmatrix}$ and $\begin{bmatrix} e & f \\ 0 & h \end{bmatrix}$. The work was based on a method from Acharya et al. (2007). The objective of the study is to generate suitable involutory matrices that will be used in the Cipher Trigraphic Polyfunction system with similar encryption keys. However, they consider $C_{3\times j}^{(t)} \equiv L_{3\times 3}^{(t)} P_{3\times j} (\mathrm{mod}\ N)$. It proposed six properties for different cases of matrices covered $A_{2\times 2}$. It also covered nonsingular matrices $L_{2\times 2} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ and three more cases: Case 1 with $c = 0$ and $a + d \neq 0$, Case 2 with $c \neq 0$ and $a + d = 0$ and Case 3 with $c = 0$ and $c + d = 0$. As a result,

$$L_{2\times 2} \equiv \begin{bmatrix} e^{\frac{1}{2}} & f\left(e^{\frac{1}{2}} + h^{\frac{1}{2}}\right)^{-1} \\ 0 & h^{\frac{1}{2}} \end{bmatrix} (\text{mod } N)$$

was chosen and subsequently generate two types of involutory matrices $L_{3\times 3}$ in the form of

$$L_{3\times 3} \equiv \begin{bmatrix} -e^{\frac{1}{2}} & (1-e)k^{-1} & -fk^{-1} \\ k & e^{\frac{1}{2}} & \left(e^{\frac{1}{2}} + 1\right)^{-1} f \\ 0 & 0 & 1 \end{bmatrix} (\text{mod } N)$$

and

$$L_{3\times 3} \equiv \begin{bmatrix} -h^{\frac{1}{2}} & 0 & k \\ -fk^{-1} & 1 & \left(h^{\frac{1}{2}} + 1\right)^{-1} f \\ (1-h)k^{-1} & 0 & h^{\frac{1}{2}} \end{bmatrix} (\text{mod } N).$$

However, it faced the same problem as Yunos et al. (2018) and Ching and Yunos (2019) where the plaintexts can easily be obtained by the parties when these keys are used in Cipher Trigraphic Polyfunction transformations due to the repeating process on finding plaintext and ciphertext. So, $L_{2\times 2}$ with this type should be avoided as encryption key in this system.

Previous studies by Yunos et al. (2018), Ching and Yunos (2019) and Yunos et al. (2023) had implemented some type of self-invertible keys in the encryption process for each transformation when using Cipher Tetragraphic Trifunction, Cipher Hexagraphic Polyfunction and Cipher Trigraphic Polyfunction respectively. All of them had the same weakness which is the plaintext can be obtained by the adversary when the encryption keys are similar for each transformation and the transformation is even-th.

The organization of this paper is as follows. Section 1 explains the varied implementation of self-invertible matrices in Hill cipher with its advantages and disadvantages. Section 2 consists of the preliminaries of this study. Section 3 of the cipher discussion on how to find some solutions of $L_{2\times 2}^2 \equiv A_{2\times 2}(\text{mod } N)$. Section 4 gives a detail method for generating a self-invertible matrix. Followed by the implementation of encryption key with self-invertible matrices an different encryption for each transformation in Cipher Trigraphic Polyfunction. The concluding section contains a summary of the paper.

PRELIMINARIES

The Cipher Trigraphic Polyfunction is constructed based on Cipher Polygraphic Polyfunction (Yunos et al., 2023) which is as follows:

Encryption Process

The encryption from $P_{i\times j}$ to $C_{i\times j}^{(t)}$ is as follows:

$$C_{i\times j}^{(t)} \equiv \prod_{u=0}^{t-1} A_{i\times i}^{(t-u)} P_{i\times j} (\text{mod } N) \text{ where } t \in \mathbb{Z}^+$$

where $A_{i\times i}^{(t)}$ act as an encryption key.

Decryption Process

If $\left|A_{i\times i}^{(t)}\right| \neq 0$ and $\left(\left|A_{i\times i}^{(t)}\right|, N\right) = 1$ for each t, then $P_{i\times j}$ has a unique solution and the decryption from $C_{i\times j}^{(t)}$ to $P_{i\times j}$ is as follows:

$$P_{i\times j} \equiv \prod_{u=1}^{t} \left(A_{i\times i}^{(u)}\right)^{-1} C_{i\times j}^{(t)} (\text{mod } N).$$

The following concept involves modular arithmetic, which will be used in proving Theorem 3.1 in the upcoming section.

Theorem 2.1. (Rosen, 2011) If $(a, N) = 1$, then $ax \equiv b(\text{mod } N)$ has exactly one solution in modulo N.

Definition 2.2. (Silverman et al., 2008) Let p be an odd prime number and let a be a number with $p \nmid a$. We say that a is a quadratic residue modulo p if a is a square modulo p, i.e., if there is a number c so that $c^2 \equiv a(\text{mod } p)$. If a is not a square modulo p, i.e., if there exists no such c, then a is called a quadratic nonresidue modulo p.

The following lemma is Euler's Criterion which is suitable to determine whether $x^2 \equiv a(\text{mod } N)$ has solutions or not.

Lemma 2.3. (Niven et al., 1991) If N is an odd prime and $N \nmid a$, then $x^2 \equiv a(\text{mod } N)$ has (1) solution if

$$a^{\frac{N-1}{2}} \equiv 1(\text{mod } N).$$

(2) no solution if

$$a^{\frac{N-1}{2}} \equiv -1(\text{mod } N).$$

Since Eulers Criterion is not suitable if a and N in a large size, then Legendre Symbol can be used to check whether the integer is a quadratic residue modulo prime as follows:

Theorem 2.4. (Raji, 2013) Given N is an odd prime and $N \nmid a$, then the Legendre symbol $\frac{a}{N}$ is defined as

$$\left(\frac{a}{N}\right) = \begin{cases} 1, & \text{if a is quadratic residue modulo } N \text{ and } a^{\frac{N-1}{2}} \equiv 1(\text{mod } N) \\ -1, & \text{if } a \text{ is quadratic nonresidue modulo} N \text{ and } a^{\frac{N-1}{2}} \equiv -1(\text{mod } N) \end{cases}$$

SOLUTIONS FOR $L_{2\times 2}^2 \equiv A_{2\times 2}(\text{mod } N)$

In this section, we proposed the following property in order to find the solution of $L_{2\times2}^2 \equiv A_{2\times2} (\text{mod } N)$.

Theorem 3.1. Let $(g, N) = 1$. The solution to $L_{2\times2}^2 \equiv \begin{bmatrix} e & f \\ g & h \end{bmatrix} (\text{mod } N)$ is

$$L_{2\times2} \equiv \begin{bmatrix} \sqrt{e - fg^{-1}y} & fg^{-1}\sqrt{y} \\ \sqrt{y} & \sqrt{h - fg^{-1}y} \end{bmatrix} (\text{mod } N), \tag{1}$$

where $y = \frac{-g^2(h+e) \pm 2g^2\sqrt{eh-fg}}{-((h-e)^2+4fg)}, \left(\frac{y}{N}\right) = 1, \left(\frac{eh-fg}{N}\right) = 1, \left(\frac{e-fg^{-1}y}{N}\right) = 1$, and $\left(\frac{h-fg^{-1}y}{N}\right) = 1$.

Proof. It is to show the condition to generate the suitable key feature for $L_{2\times2} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ and $A_{2\times2} = \begin{bmatrix} e & f \\ g & h \end{bmatrix}$ with e, f, g, h are integers such that $L_{2\times2}^2 \equiv A_{2\times2} (\text{mod } N)$ using simultaneous equations as follows:

$$a^2 + bc \equiv e (\text{mod } N), \tag{2}$$
$$ab + bd \equiv f (\text{mod } N), \tag{3}$$
$$ac + cd \equiv g (\text{mod } N), \tag{4}$$
$$bc + d^2 \equiv h (\text{mod } N), \tag{5}$$

From (3) and (4), we have

$$b \equiv f(a + d)^{-1} (\text{mod } N), \tag{6}$$

and

$$c \equiv g(a + d)^{-1} (\text{mod } N), \tag{7}$$

for $(a + d, N) = 1$ respectively. Followed by

$$b \equiv cfg^{-1} (\text{mod } N), \text{ where } (g, N) = 1. \tag{8}$$

Substituting (6), (7) and (8) into (2) and (5), we have

$$a \equiv \sqrt{e - c^2fg^{-1}} (\text{mod } N), \text{ for } \left(\frac{e - c^2fg^{-1}}{N}\right) = 1 \tag{9}$$

and

$$d \equiv \sqrt{h - c^2fg^{-1}} (\text{mod } N), \text{ for } \left(\frac{h - c^2fg^{-1}}{N}\right) = 1 \tag{10}$$

respectively. Now, from (7) we get

$$a + d \equiv c^{-1}g (\text{mod } N), \text{for } (c, N) = 1. \tag{11}$$

Substitute (9) and (10) into (11) gives the following:

$$\sqrt{e - c^2fg^{-1}} + \sqrt{h - c^2fg^{-1}} \equiv c^{-1}g(\text{mod } N)$$
$$\sqrt{ge - c^2f} + \sqrt{hg - c^2f} \equiv c^{-1}g\sqrt{g}(\text{mod } N)$$
$$2\sqrt{(ge - c^2f)(hg - c^2f)} \equiv c^{-2}g^3 - ge + 2c^2f - hg(\text{mod } N)$$
$$2c^2\sqrt{(ge - c^2f)(hg - c^2f)} \equiv g^3 - gec^2 + 2c^4f - hgc^2(\text{mod } N)$$
$$4c^4(ge - c^2f)(hg - c^2f) \equiv (g^3 - gec^2 + 2c^4f - hgc^2)^2(\text{mod } N)$$
$$-c^4g^2((h-e)^2 + 4fg) + 2c^2g^4(h+e) - g^6 \equiv 0(\text{mod } N).$$

Let $y = c^2, \alpha = -g^2((h-e)^2 + 4fg), \beta = 2g^4(h+e)$ and $\gamma = -g^6$ then the above equation can be written as

$$\alpha y^2 + \beta y + \gamma \equiv 0(\text{mod } N),$$

with the following roots:

$$y = \frac{-\beta \pm \sqrt{\beta^2 - 4\alpha\gamma}}{2\alpha} = \frac{-g^2(h+e) \pm 2g^2\sqrt{eh - fg}}{-((h-e)^2 + 4fg)}.$$

Since $c = \sqrt{y}$, then (8), (9) and (10) become $a = \sqrt{e - fg^{-1}y}, b = fg^{-1}\sqrt{y}$ and $d = \sqrt{h - fg^{-1}y}$. Hence, we get

$$L_{2\times2} \equiv \begin{bmatrix} \sqrt{e - fg^{-1}y} & fg^{-1}\sqrt{y} \\ \sqrt{y} & \sqrt{h - fg^{-1}y} \end{bmatrix} (\text{mod } N). \quad \blacksquare$$

Example 3.2. The solution of $L_{2\times2}^2 \equiv \begin{bmatrix} 21 & 14 \\ 20 & 15 \end{bmatrix} (\text{mod } 23)$ are $\begin{bmatrix} 3 & 6 \\ 2 & 7 \end{bmatrix}, \begin{bmatrix} 20 & 17 \\ 21 & 16 \end{bmatrix}, \begin{bmatrix} 10 & 4 \\ 9 & 5 \end{bmatrix}$ and $\begin{bmatrix} 13 & 19 \\ 14 & 18 \end{bmatrix}$.

We name the submatrix $L_{2\times2}$ of a 3×3 matrix discussed in this section as $id2$. For the purpose of implementing the Cipher Trigraphic Polyfunction system, $id2$ is kept confidential from public because it serves as a basis for generating the encryption and decryption keys in the system.

GENERATION OF SELF-INVERTIBLE MATRIX

We implement the method for generating a self-invertible matrix that was presented by (Acharya et al., 2007) as follows:

Let $A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix}$ be an $n \times n$ self-invertible matrix partitioned to

$A = \begin{bmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{bmatrix}$, where $A_{11} = [a_{11}], A_{12} = [a_{12} \quad a_{13} \quad \ldots \quad a_{1n}], A_{21} = \begin{bmatrix} a_{21} \\ a_{31} \\ \ldots \\ a_{n1} \end{bmatrix}$, and

$A_{22} = \begin{bmatrix} a_{22} & a_{23} & \cdots & a_{2n} \\ a_{32} & a_{33} & \cdots & a_{3n} \\ \ldots & \ldots & \ldots & \ldots \\ a_{n2} & a_{n3} & \cdots & a_{nn} \end{bmatrix}$.

Since A is self-invertible, it satisfies $A^2 = I$.
Now, if $A_{11}^2 + A_{12}A_{21} = 1$, then

$$A_{12}A_{21} = 1 - A_{11}^2 = 1 - a_{11}^2. \quad (12)$$

If $A_{11}A_{12} + A_{12}A_{22} = 0$, then

$$A_{12}(A_{11} + A_{22}) = 0. \quad (13)$$

If $A_{21}A_{11} + A_{22}A_{21} = 0$, then

$$A_{21}(A_{11} + A_{22}) = 0. \quad (14)$$

If $A_{21}A_{12} + A_{22}^2 = 1$, then

$$A_{21}A_{12} = 1 - A_{22}^2. \quad (15)$$

From (14), we know that $(A_{11} + A_{22}) = 0$. Then,

$$A_{22} = -A_{11} = -a_{11}. \quad (16)$$

If

$$A_{12}A_{21} = I - A_{11}^2 = 1 - a_{11}^2, \quad (17)$$

Then

$$A_{12}(a_{11}I + A_{22}) = 0. \quad (18)$$

Also, $a_{11} = -$(one of the Eigenvalues of A_{22} other than 1).
Since $A_{21}A_{12}$ is a singular matrix having the rank 1, then

$$A_{21}A_{12} = I - A_{22}^2. \quad (19)$$

So, A_{22} must have Eigenvalues ± 1.

The consistent solution obtained for matrix A_{21} and A_{12} by solving (19) term by term will also satisfy (17).

The algorithm below has been created to generate a self-invertible matrix. To align with our study, we take $A_{11} = L_{1\times1}, A_{22} = L_{2\times2}, A_{12} = L_{1\times2}$, and $A_{21} = L_{2\times1}$ to formulate A which is $L_{3\times3}$.

Algorithm 4.1 Generation of Self-Invertible Matrices

Input : Matrix A_{22}
Output: The self-invertible matrix A

1: Select A_{22}, a non-singular $(n-1)\times(n-1)$ matrix which has $(n-2)$ number of Eigenvalue of A_{22} either $+1$ or -1 or both.
2: Determine the other Eigenvalue λ of A_{22}.
3: Set $a_{11} = -\lambda$.
4: Obtain the consistent solution of all elements of A_{21} and A_{12} by using (19).
5: Formulate the matrix by substituting the value of $a_{11}, a_{12}, a_{13}, a_{21}, a_{22}, a_{23}, a_{31}, a_{32}$, and a_{33} respectively in the matrix A.

GENERATION OF SELF-INVERTIBLE 3×3 MATRICES BASED ON *id2*

In this section, we developing new property of matrix 3×3, $L_{3\times3} \equiv \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix} \equiv \begin{bmatrix} L_{1\times1} & L_{1\times2} \\ L_{2\times1} & L_{2\times2} \end{bmatrix} (\text{mod } N)$ that was self-invertible where $L_{2\times2}$ or $id2$ based on equation (1). For that reason, we do the similar steps in Algorithm 4.1 as follows:

(1) $L_{2\times2}$ must be a non-singular matrix where $|L_{2\times2}| \neq 0$. We can find the eigenvalue of $L_{2\times2}$ (i.e. either $+1$ or -1 or both) by solving a quadratic equation produced by $\det(\lambda I - L_{2\times2}) \equiv \lambda^2 - \left(\sqrt{e - fg^{-1}y} + \sqrt{h - fg^{-1}y}\right)\lambda + \sqrt{eh - fg^{-1}y(e+h) + f^2g^{-2}y^2} - f^{-1}y \equiv 0 (\text{mod } N)$.

Therefore,

$$\lambda \equiv \frac{-b^* \pm \sqrt{b^{*2} - 4a^*c^*}}{2a^*} (\text{mod } N) \tag{20}$$

where $a^* = 1, b^* = -\left(\sqrt{e - fg^{-1}y} + \sqrt{h - fg^{-1}y}\right)$ and

$c^* = \sqrt{eh - fg^{-1}y(e+h) + f^2g^{-2}y^2} - fg^{-1}y$.

(2) Determine the other Eigenvalue λ of $L_{2\times2}$.

(3) Set $a_{11} = -\lambda$.

(4) Supposed $L_{2\times1} = \begin{bmatrix} a_{21} \\ a_{31} \end{bmatrix}$ and $L_{1\times2} = [a_{12} \quad a_{13}]$. Implementing (19), we have

$$L_{2\times1}L_{1\times2} \equiv I - L_{2\times2}^2 \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} - \begin{bmatrix} e & f \\ g & h \end{bmatrix} = \begin{bmatrix} 1-e & -f \\ -g & 1-h \end{bmatrix} (\text{mod } N),$$

where it must be a singular matrix with $f = (1-e)(1-h)g^{-1}$. Followed by solving the following simultaneous equations:

$$a_{21}a_{12} \equiv 1 - e (\text{mod } N), \tag{21}$$
$$a_{21}a_{13} \equiv -f (\text{mod } N), \tag{22}$$
$$a_{31}a_{12} \equiv -g (\text{mod } N), \tag{23}$$
$$a_{31}a_{13} \equiv 1 - h (\text{mod } N). \tag{24}$$

Let $k = a_{12}$ for $(k, N) = 1$. From (21) and (23), we get

$$a_{21} \equiv (1-e)k^{-1} (\text{mod } N),$$

and

$$a_{31} \equiv -gk^{-1} (\text{mod } N).$$

respectively. Therefore, from (22) and (23) give

$$a_{13} \equiv -g^{-1}(1-h)k (\text{mod } N).$$

(5) From the steps above, we obtain $L_{1\times2} = [k \quad -g^{-1}(1-h)k]$ and $L_{2\times1} = \begin{bmatrix} (1-e)k^{-1} \\ -gk^{-1} \end{bmatrix}$. Hence, we will get

$$L_{3\times3} \equiv \begin{bmatrix} -\lambda & k & -g^{-1}(1-h)k \\ (1-e)k^{-1} & \sqrt{e-fg^{-1}y} & fg^{-1}\sqrt{y} \\ -gk^{-1} & \sqrt{y} & \sqrt{h-fg^{-1}y} \end{bmatrix} (\text{mod } N). \quad (25)$$

Example 4.1. We consider $L_{2\times2} = \begin{bmatrix} 3 & 6 \\ 2 & 7 \end{bmatrix}$ from Example 3.2 that is one solution of $L_{2\times2}^2 \equiv \begin{bmatrix} 21 & 14 \\ 20 & 15 \end{bmatrix} (\text{mod } 23)$ and let $e = 21, f = 14, g = 20, h = 15$ and $k = 3$. Now, we can generate self-invertible key $L_{3\times3} \equiv \begin{bmatrix} 14 & 3 & 9 \\ 1 & 3 & 6 \\ 1 & 2 & 7 \end{bmatrix} (\text{mod } 23)$ by implementing formula (25).

IMPLEMENTING DIFFERENT SELF-INVERTIBLE KEYS IN CIPHER TRIGRAPHIC POLYFUNCTION

We present a preliminary result when implementing different self-invertible keys for Cipher Trigraphic Polyfunction as follows:

Encryption Process

The encryption process from $P_{3\times j}$ to $C_{3\times j}^{(t)}$ is as follows:

$$C_{3\times j}^{(t)} \equiv \prod_{u=0}^{t-1} L_{3\times3}^{(t-u)} P_{3\times j} (\text{mod } N).$$

Decryption process

If $|L_{3\times3}^{-1}| \neq 0$ and $(|L_{3\times3}^{-1}|, N) = 1$, then the decryption process from $C_{3\times j}^{(t)}$ to $P_{3\times j}$ is as follows:

$$P_{3\times j} \equiv \prod_{u=0}^{t-1} L_{3\times3}^{(t-u)} C_{3\times j}^{(t)} (\text{mod } N).$$

Example 4.2. Suppose Alice wants to submit the following plaintext to Bob as follows:

$$P_{3\times3} \equiv \begin{bmatrix} 3 & 0 & 13 \\ 6 & 4 & 17 \\ 14 & 20 & 18 \end{bmatrix} (\text{mod } 23).$$

Let the self-invertible secret keys, $L_{3\times3}^{(t)}$ for transformation, $t = 1,2,3$ for both encryption and decryption processes are $L_{3\times3}^{(1)} = \begin{bmatrix} 10 & 22 & 22 \\ 1 & 6 & 5 \\ 6 & 7 & 8 \end{bmatrix}, L_{3\times3}^{(2)} = \begin{bmatrix} 14 & 3 & 9 \\ 1 & 3 & 6 \\ 1 & 2 & 7 \end{bmatrix}$ and

$L_{3\times3}^{(3)} = \begin{bmatrix} 14 & 21 & 21 \\ 1 & 5 & 6 \\ 16 & 4 & 3 \end{bmatrix}$ where $\left|L_{3\times3}^{(t)}\right| \neq 0 (\text{mod } 23)$ and $\left(\left|L_{3\times3}^{(t)}\right|, 23\right) = 1$. The encryption from $P_{3\times3}$ to ciphertext $C_{3\times3}^{(3)}$ is used the following process:

$$C_{3\times3}^{(3)} \equiv L_{3\times3}^{(3)} L_{3\times3}^{(2)} L_{3\times3}^{(1)} P_{3\times3} \equiv \begin{bmatrix} 3 & 19 & 0 \\ 1 & 8 & 20 \\ 12 & 21 & 15 \end{bmatrix} (\text{mod } 23)$$

Since $L_{3\times3}^{(t)}$ is self-invertible, Bob easily gets the original text via the decryption process as follows:

$$P_{3\times3} \equiv L_{3\times3}^{(1)} L_{3\times3}^{(2)} L_{3\times3}^{(3)} C_{3\times3}^{(3)} \equiv \begin{bmatrix} 3 & 0 & 13 \\ 6 & 4 & 17 \\ 14 & 20 & 18 \end{bmatrix} (\text{mod } 23)$$

In the context of Cipher Trigraphic Polyfunction, there appears to be a lack of concrete evidence demonstrating that employing self-invertible encryption with distinct secret keys for each transformation guarantees enhanced security compared to utilizing a single key. To further evaluate the system's safety, it is crucial to examine letter frequency patterns in the future. One confirmed advantage of this method, however, is no complexity computation needed to determine the inverse of the encryption keys.

CONCLUSION

In conclusion, this study managed to find a solution (i.e. $id2$) for matrix equation $L_{2\times2}^2 \equiv A_{2\times2} (\text{mod } N)$ through simultaneous congruent solutions. The $id2$ matrix in the form of an equation (1) then generates a self-invertible key (see equation (25) that acts as encryption and decryption keys of a Cipher Trigraphic Polyfunction Cryptographic system. Obviously, this study shows that the recipient of the message does not have any problem finding the inverse of the encryption key. However, it is still too early to claim that this system is secure for the needs of the industry. Therefore, future studies can be carried out to attack this system by analyzing of the letters frequency of its ciphertext. It is also necessary to consider the increased symmetrical key storage space compared to the conventional Hill Cipher.

REFERENCES

Acharya, B., Panigrahy, S. K., Patra, S. K., and Panda, G. (2009). Image Encryption using Advanced Hill Cipher Algorithm. *International Journal of Recent Trends in Engineering*, **1(1)**: 663 – 667.

Acharya, B., Rath, G. S., Patra, S. K., and Panigrahy, S. K. (2007). Novel Methods of Generating Self-Invertible Matrix for Hill Cipher Algorithm. *International Journal of Security*, **1(1)**: 14 – 21.

Ching, S. L. P. and Yunos, F. (2019). Effect of Self-invertible Matrix on Cipher Hexagraphic Polyfunction. *Cryptography*, **3(2)**:15.

Hill, L. S. (1929). Cryptography in an Algebraic Alphabet. *The American Mathematical Monthly*, **36**:306 – 312.

Jackob, M. (2001). White Paper: History of Encryption. Technical report, SANS Institute, East Lansing, Michigan.

Niven, I., Zuckerman, H. S., and Montgomery, H. L. (1991). An Introduction to the Theory of Numbers, John Wiley & Sons, 5th edition, pp. 47–115.

Overbey, J., Traves, W., and Wojdylo, J. (2005). On the Keyspace of the Hill Cipher. *Cryptologia*, **29**:59 – 72.

Raji, W. (2013). An Introductory Course in Elementary Number Theory, The Saylor Foundation, pp. 105 – 112.

Rosen, K. H. (2011). Elementary Number Theory, Pearson Education London, London, United Kingdom, pp. 141 – 158.

Silverman, J. H., Pipher, J., and Hoffstein, J. (2008). An Introduction to Mathematical Cryptography, Springer, New York, volume 1, pp. 1 – 58.

Wikramaratna, R. S. (2011). The Centro-invertible Matrix: A New Type of Matrix Arising in Pseudo-random Number Generation. *Linear Algebra and its Applications*, **434(1)**:144 – 151.

Yeh, Y. S., Wu, T. C., Chang, C. C., and Chang, W. C. (1991). A New Cryptosystem using Matrix Transformation. In *Proceedings of the 25th Annual 1991 IEEE International Carnahan Conference on Security Technology*, Taipei, Taiwan, pp. 131 – 138.

Yunos, F., Chin, L. S., and Said, M. R. M. (2018). Effect of Self-invertible Matrix on Cipher Tetragraphic Trifunction. In *AIP Conference Proceedings,* AIP Publishing LLC, *volume 1974*, pp. 020001.

Yunos, F., Kamaluzaman, A. Z., Jamaludin, M. S., and Basri, W. (2023). Solution of $L^2 = A$ Matrix to Generate Involutory Matrices for Cipher Trigraphic Polyfunction. *Applied Mathematics and Computational Intelligence*, **12(1)**:1 – 17.