cryptography

MDPI

Article

Effect of Self-Invertible Matrix on Cipher Hexagraphic Polyfunction

Sally Lin Pei Ching [1,2] and Faridah Yunos [1,3,*]

[1] Department of Mathematics, Universiti Putra Malaysia, 43400 Serdang, Selangor, Malaysia; chilinG7_73@hotmail.com
[2] Boon Siew Honda Sdn. Bhd. (676896-A) 721, Persiaran Cassia Selatan 1, Kawasan Perindustrian Batu Kawan, 14100 Simpang Ampat, Penang, Malaysia
[3] Institute for Mathematical Research, Universiti Putra Malaysia, 43400 Serdang, Selangor, Malaysia
* Correspondence: faridahy@upm.edu.my

Received: 17 April 2019; Accepted: 13 June 2019; Published: 15 June 2019

Abstract: A cryptography system was developed previously based on Cipher Polygraphic Polyfunction transformations, $C_{i\times j}^{(t)} \equiv A_{i\times i}^{t} P_{i\times j} \ mod \ N$ where $C_{i\times j}$, $P_{i\times j}$, $A_{i\times i}$ are cipher text, plain text, and encryption key, respectively. Whereas, (t) is the number of transformations of plain text to cipher text. In this system, the parameters $(A_{i\times i}, (t))$ are kept in secret by a sender of messages. The security of this system, including its combination with the second order linear recurrence Lucas sequence (LUC) and the Ron Rivest, Adi Shamir and Leonard Adleman (RSA) method, until now is being upgraded by some researchers. The studies found that there is some type of self-invertible $A_{4\times4}$ should be not chosen before transforming a plain text to cipher text in order to enhance the security of Cipher Tetragraphic Trifunction. This paper also seeks to obtain some patterns of self-invertible keys $A_{6\times6}$ and subsequently examine their effect on the system of Cipher Hexagraphic Polyfunction transformation. For that purpose, we need to find some solutions $L_{3\times3}$ for $L_{3\times3}^{2} \equiv A_{3\times3} \mod N$ when $A_{3\times3}$ are diagonal and symmetric matrices and subsequently implement the key $L_{3\times3}$ to get the pattern of $A_{6\times6}$.

Keywords: Cipher Polygraphic; Hill cipher; self-invertible matrix; RSA; LUC

1. Introduction

Cryptography is defined as the science or study of the techniques of secret writing. It is the art or science encompassing the principles and methods of transforming an intelligible message (plain text) into one that is unintelligible (cipher text) and then transforming that message back to its original form [1]. Cryptography is considered to be a branch of both mathematics and computer science. They are affiliated closely with information theory, computer security, and engineering. The technology for practicing secret communication, which is widely known as encryption and decryption, was always done symmetrically until 1970s [2]. In early 1978, the RSA cryptosystem that was introduced by Ron Rivest, Adi Shamir, and Leonard Adleman became a phenomenon in the world of secrecy of which was regarded as the first practical realization of the asymmetric cryptosystem as opposed to symmetric cryptosystem [2,3]. In this paper, we are using the asymmetric cryptosystem which is based on Cipher Hexagraphic Polyfunction.

Mathematical Background

Several notations (refer to [4–7]) that we will be using while performing encryption process of Cipher Hexagraphic Polyfunction are shown as follows:

P is a corresponding number in a plain text. For example, $P = 50$ if the corresponding number for the plain text B is 50.

$P_{i\times j} = [p_{xy}]$ is a corresponding numbers sequence with a plain text, that is p_{xy} for every $x \leq i$ and $y \leq j$ that have been arranged based on i^{th} row and j^{th} column of a matrix. For example, the corresponding numbers sequence of the plain text P L E A S E is 80 76 69 65 83 69 and are arranged by the 3 rows 2 columns matrix such that $P_{3\times 2} = \begin{bmatrix} 80 & 65 \\ 76 & 83 \\ 69 & 69 \end{bmatrix}$.

C is a corresponding number in a cipher text monofunction. For example, if the corresponding number of the cipher text AB is 7686 it is produced from monofunction transformation so that $C = 7686$.

$C_{i\times j} = [c_{xy}]$ is a corresponding numbers sequence with a cipher text c_{xy} for every $x \leq i$ and $y \leq j$ that have been arranged based on i^{th} row and j^{th} column of a matrix produced from monofunction transformation. For example, the corresponding number sequence with the cipher text A B C D E F produced from monofunction transformation that is 65 66 67 68 69 70 is written in the matrix 3 rows 2 columns as $C_{3\times 2} = \begin{bmatrix} 65 & 68 \\ 66 & 69 \\ 67 & 70 \end{bmatrix}$.

$C^{(t)}_{i\times j} = [c^{(t)}_{xy}]$ is a corresponding numbers sequence with a cipher text $c^{(t)}_{xy}$ for every $x \leq i$ and $y \leq j$ that have been arranged based on i^{th} row and j^{th} column of a matrix at the t^{th} transformation for $t = 1, 2, 3, \ldots$. Let $C^{(1)}_{i\times j} = C_{i\times j}$ when $t = 1$. For example, the corresponding number of the cipher text M Z W V A D produced by third transformation is 78 90 87 86 65 68 arranged by the matrix 2 rows 3 columns as $C^{(3)}_{2\times 3} = \begin{bmatrix} 78 & 87 & 65 \\ 90 & 86 & 68 \end{bmatrix}$.

Encryption key $A_{i\times i} = [a_{xz}]$ is an integer sequence a_{xz} for every $x, z \leq i$ arranged based on a matrix i^{th} row and i^{th} column while $A^{-1}_{i\times i} = [b_{xz}]$ is the inverse matrix for $A_{i\times i}$ such that $|A_{i\times i}| \neq 0$.

Encryption key $L_{i\times i} = [m_{xz}]$ is an integer sequence m_{xz} for every $x, z \leq i$ arranged based on i^{th} row and i^{th} column of a matrix such that $L^2_{i\times i} \equiv A_{i\times i}$ while $L^{-1}_{i\times i} = [n_{xz}]$ is the inverse matrix for $L_{i\times i}$ such that $|L_{i\times i}| \neq 0$.

Several definitions (refer to [1,4,5,8,9]) that should be understood in this paper are as follows:

Definition 1. *Let N be any positive integer. Let us say that the equivalent number of plain text and cipher text are matrices of rows i and columns j:*

$$P_{i\times j} \equiv [p_{xy}] \ mod \ N,$$

and

$$C^{(t)}_{i\times j} \equiv c^{(t)}_{xy} \ mod \ N$$

with $P_{xy} < N$ for every $x \leq i$ and $y \leq j$.
Let the encryption key be an $i \times i$ matrix:

$$A^{(t)}_{i\times i} \equiv [a_{xz}] \ mod \ N$$

for every $x, z \leq i$.

Encryption algorithm of $P_{i\times j} \equiv [p_{xy}] \ mod \ N$ for the first transformation will produce a cipher text $C^{(1)}_{i\times j} \equiv c^{(1)}_{xy} \ mod \ N$ through

$$C^{(1)}_{i\times j} \equiv A^{(1)}_{i\times i} P_{i\times j} \ mod \ N$$

with $c^{(1)}_{xy} \equiv a_{x1}p_{1y} + a_{x2}p_{2y} \ mod \ N$ which is called Cipher Polygraphic Monofunction Transformation.

Next, the cipher text $C^{(1)}_{i\times j} \equiv [c^{(1)}_{xy}]$ *mod N was translated into a cipher text* $C^{(2)}_{i\times j} \equiv c^{(2)}_{xy}$ *mod N at the second transformation through*

$$C^{(2)}_{i\times j} \equiv A^{(2)}_{i\times i} C^{(1)}_{i\times j} \ mod\ N$$

with $c^{(2)}_{xy} \equiv a_{x1}c^{(1)}_{1y} + a_{x2}c^{(1)}_{2y}$ *mod N which is called Cipher Polygraphic Difunction Transformation.*

After that, the cipher text $C^{(2)}_{i\times j} \equiv [c^{(2)}_{xy}]$ *mod N was translated into a cipher text* $C^{(3)}_{i\times j} \equiv c^{(3)}_{xy}$ *mod N at the third transformation through*

$$C^{(3)}_{i\times j} \equiv A^{(3)}_{i\times i} C^{(2)}_{i\times j} \ mod\ N$$

with $c^{(3)}_{xy} \equiv a_{x1}c^{(2)}_{1y} + a_{x2}c^{(2)}_{2y}$ *mod N which is called Cipher Polygraphic Trifunction Transformation.*

Further, the equation of Cipher Polygraphic Polyfunction Transformation is

$$C^{(t)}_{i\times j} \equiv A^{(t)}_{i\times i} C^{(t-1)}_{i\times j} \ mod\ N$$

with $c^{(t)}_{xy} \equiv a_{x1}c^{(t-1)}_{1y} + a_{x2}c^{(t-1)}_{2y}$ *mod N.*

The transformation can be simplified as $C^{(t)}_{i\times j} \equiv A^{t}_{i\times i} P_{i\times j}$ *mod N if all the secret keys* $A^{(t)}_{i\times i}$ *are similar.*

In this research, we used $i = 6$ so that it is called Cipher Hexagraphic Polyfunction. Whereas, all the secret keys $A^{(t)}_{6\times 6}$ are similar so that the transformation can be simplified as $C^{(t)}_{6\times j} \equiv A^{t}_{6\times 6} P_{6\times j}$ *mod N*.

Definition 2. *A is called a self-invertible matrix if* $A \equiv A^{-1}$ *mod N. If A and* A^{-1} *are* $n \times n$ *matrices of integers and if* $AA^{-1} \equiv A^{-1}A \equiv I$ *mod N, where I is an identity matrix of order n, then* A^{-1} *is said to be an inverse of A modulo N.*

Definition 3. *A diagonal matrix is a square matrix all of whose entries are zero except possibly for those on the main diagonal.*

Definition 4. *A matrix is symmetric if it equals its transpose. That is,* $A^T = A$.

While, we use the generated self-invertible for $n \times n$ matrix where n is even, according to [9] as follows:

Let $A = \left[\begin{array}{ccc|cc} a_{11} & a_{12} & \cdots & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ \hline \cdots & \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & \cdots & a_{nn} \end{array}\right]$ be an $n \times n$ self-invertible matrix partitioned to $A = \left[\begin{array}{c|c} A_{11} & A_{12} \\ \hline A_{21} & A_{22} \end{array}\right]$, where n is even and each of $A_{11}, A_{12}, A_{21}, A_{22}$ are matrices of order $\frac{n}{2} \times \frac{n}{2}$. From $AA^{-1} = I$, the system of equations is $A_{12}A_{21} = I - A^2_{11}$, $A_{11}A_{12} + A_{12}A_{22} = 0$, $A_{21}A_{11} + A_{22}A_{21} = 0$ and $A_{21}A_{12} = I - A^2_{22}$. Hence, the solution for A is

$$\begin{bmatrix} A_{11} & (I - A_{11})k \\ (I + A_{11})k^{-1} & -A_{11} \end{bmatrix} or \begin{bmatrix} A_{11} & (I + A_{11})k \\ (I - A_{11})k^{-1} & -A_{11} \end{bmatrix} \quad (1)$$

where $k \in Z$. All the matrices in this case are in congruent of modulo N and $(k, N) = 1$.

In this section, we give some notations, definitions and a method to generate self-invertibles, which are related to this study. Next, in Section 2, we give previous studies involving Hill Cipher developed by earlier researchers. In Sections 3.1 and 3.2, we give some solutions for $L^2_{3\times 3} \equiv A_{3\times 3}$ *mod N* when matrix $A_{3\times 3}$ is diagonal and symmetric, respectively. Followed by discussion on how to generate

self-invertible 6×6 matrices from $L_{3\times3}$ in Section 3.3 and the effect of these generation on Cipher Hexagraphic Polyfunction in Section 3.4.

2. Literature Review

Hill Ciphers are an application of linear algebra to cryptology (the science of making and breaking codes and ciphers). It was introduced by Lester S. Hill [10]. The Hill Cipher is a polygraphic substitution cipher based on linear algebra. The core of Hill cipher is matrix manipulations. For encryption, algorithm takes m successive plain text letters and instead of that substitutes m cipher letters. In the Hill cipher, each character is assigned to a numerical value like $a = 0, b = 1, \ldots, z = 25$. The substitution of cipher text letters in the place of plain text letters leads to m linear equation and simply can be written as $C \equiv KP \ mod \ 26$, where C and P are column vectors of length m, representing the plain text and cipher text, respectively, and K is an $m \times m$ matrix, which is the encryption key. The inverse of a matrix K is needed in the process of decryption. It satisfies condition $KK^{-1} \equiv K^{-1}K \equiv I \ mod \ 26$, where I is an identity matrix. The encryption process is $C = E_k(P) = K_p$. Whereas, the decryption is $P = D_k(C) = K^{-1}C = K^{-1}K_p = P$.

Many researchers developed different methods to improve the quality of Hill Cipher. Some applications of Number Theory to Cryptography was investigated by [4]. Based on the modulo arithmetic concept, she developed a number of encryption methods by employing the Cipher Digraphic [11], RSA (Ron Rivest, Adi Shamir and Leonard Adleman) [3] and LUC (second order linear recurrence Lucas sequence) [12] systems. The system called Cipher Digraphic Polyfunction in the form of $C^{(t)}_{2\times j} \equiv A^t_{2\times2}P_{2\times j} \ mod \ N$ with $(|A_{2\times2}|, N) = 1$ and $|A_{2\times2}| \neq 0$ and $A^t_{2\times2} \neq I$ for $t \in 1, 2, 3, \ldots$ is developed and its weaknesses are investigated.

The encryption from monofunction transformation is extended to Cipher Digraphic Polyfunction transformation modulo N with different encryption keys used in every transformation [5]. An encryption of Cipher Digraphic Polyfunction is defined as $C^{(t)}_{2\times j} \equiv \prod_{u=0}^{t-1} A^{(t-u)}_{2\times2} P_{2\times j} \ mod \ N$, $|A^{(t)}_{2\times2}| \neq 0$ and $(|A^{(t)}_{2\times2}|, N) = 1$ for every $t = 1, 2, 3, \ldots$, then $P_{2\times j}$ has a unique solution and the decryption algorithm is defined as $P_{2\times j} \equiv (\prod_{u=0}^{t-1} A^{(t-u)}_{2\times2})^{-1} C^{(t)}_{2\times j} \ mod \ N$. They also stated condition $\prod_{u=0}^{t-1} A^{(t-u)}_{2\times2} \not\equiv I \ mod \ N$ to be held, so that the cipher text would not be the same as plain text.

According to [9], the decryption process requires using an inverse of matrix but the matrix's inverse does not always exist. If the matrix is not invertible, then the encrypted text cannot be decrypted. They noticed the problem of non-invertible matrix key in Hill Cipher and proposed methods of generating self-invertible matrices based on modular arithmetic. This is to make sure that the encrypted text can be decrypted. They are focusing on generating self-invertible $2 \times 2, 3 \times 3, 4 \times 4$ and an even self-invertible matrix. This technique can eliminate the computational complexity involved in finding inverse of the matrix during decryption process. They proposed a method of generating of self-invertible $n \times n$ matrix where n is even as in Equation (1).

An innovation in the age-old conventional cryptography technique of Hill Cipher using the concept of self-repetitive matrix were suggested by [13]. That is, if the matrix multiplied with itself will eventually result in an identity matrix after n multiplications, $A^n \equiv I \ mod \ N$. After $n+1$ multiplication, the matrix will repeat itself. That is, $A^nA \equiv IA \equiv A \ mod \ N$. Hence, $A^{n+1} \equiv A \ mod \ N$ where the initial conditions of self-repetitive matrix A should be square and non-singular. They concluded that this method is easy to implement and difficult to crack as it requires the cracker to find the inverse of many square matrices which is not computationally easy.

The robust cryptosystem algorithm for non-invertible matrices were suggested by [14]. They use public key ideas and key generations depending on various options and function without linear algebra steps to enhance the security of Hill Cipher against known plain text attacks due to all steps in Hill Cipher depending on linear algebra calculation. Each plain text character is converted into two cipher text characters and also in decryption, the process involves the conversion of two cipher text characters into one plain text character. While this algorithm solved the non-invertible matrix key

problem, there are other problems which caused the unsuitable algorithm to be implemented. One of the problems is that the idea of generating a new key in each block has no unique inverse to enhance the security of Hill Cipher as the attacker has no mathematical model to retrieve the key. Besides that, it also required to determine whether the key matrix's determinant is zero. However, a matrix with determinant zero does not have an inverse and the process of checking the determinant will increase the computational complexity as compared to the self-invertible method. The non-unique inverse may cause the problem in decryption process to get back the original plain text.

The ways using Non-Quadratic residues during the encryption process to improve security on Hill cipher has been studied by [8]. In Hill Cipher, a plain text is encrypted using a fixed value 26 during the computation. In the encryption algorithm from Reddy, each character is assigned to a non-quadratic residue value of a prime number P such that $C \equiv KP \ mod \ N$ where C and P represent transferred matrix and the plain text, respectively, whereas, K is a non-singular matrix representing the encryption key. Operations are performed with respect to $mod \ N$. This procedure is more flexible compared to mod 26 in Hill Cipher as it can consider any large prime greater than or equal to 53. Hence, the algorithm is less vulnerable from any attack.

The effect of self-invertible matrix on Cipher Tetragraphic Trifunction were presented by [7]. The authors gave some solutions $L_{2\times2}$ for $L_{2\times2}^3 \equiv A_{2\times2} \ mod \ N$. If $A_{2\times2}$ is zero, then $L_{2\times2} = \begin{bmatrix} 0 & b \\ 0 & 0 \end{bmatrix}$ or $\begin{bmatrix} 0 & 0 \\ c & 0 \end{bmatrix}$ or $\begin{bmatrix} 1 & b \\ -b^{-1} & -1 \end{bmatrix}$ or $\begin{bmatrix} -1 & b \\ -b^{-1} & 1 \end{bmatrix}$. If $A_{2\times2}$ is identity, then $L_{2\times2} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ or $\begin{bmatrix} -2^{-1} & -3(4c)^{-1} \\ c & -2^{-1} \end{bmatrix}$. If $A_{2\times2}$ is $\begin{bmatrix} e & f \\ 0 & 0 \end{bmatrix}$, then $L_{2\times2} = \begin{bmatrix} e^{3^{-1}} & fe^{-2.3^{-1}} \\ 0 & 0 \end{bmatrix}$ or $\begin{bmatrix} a & b \\ -a^2b^{-1} & -a \end{bmatrix}$. If $A_{2\times2}$ is $\begin{bmatrix} e & f \\ 0 & h \end{bmatrix}$, then $L_{2\times2} = \begin{bmatrix} e^{3^{-1}} & f(e^{-2.3^{-1}} + e^{3^{-1}}h^{3^{-1}} + h^{2.3^{-1}}) \\ 0 & h^{3^{-1}} \end{bmatrix}$ or $\begin{bmatrix} a & b \\ -(e^{2.3^{-1}} + ae^{3^{-1}} + a^2)b^{-1} & -(e^{3^{-1}} + a) \end{bmatrix}$. If $A_{2\times2}$ is $\begin{bmatrix} e & f \\ g & h \end{bmatrix}$, then $L_{2\times2} = \begin{bmatrix} e^{3^{-1}} & 0 \\ g(3e^{2.3^{-1}})^{-1} & -2e^{3^{-1}} \end{bmatrix}$. As a result, they choose the $L_{2\times2}$ so that A is not in the form of $A \equiv 0 \ mod \ N$, $A \equiv I \ mod \ N$, lower and upper triangular matrix A. Furthermore, the use of a secret key $L_{4\times4} \equiv \begin{bmatrix} L_{2\times2} & I - L_{2\times2} \\ I + L_{2\times2} & -L_{2\times2} \end{bmatrix} \mod N$ should be avoided in order to enhance the security of Cipher Tetragraphic Trifunction transformations, $C_{4\times4}^{(t)} \equiv L_{4\times4}^t P_{4\times4} \ mod \ N$ where $t \in 1, 2, 3$.

3. Results and Discussion

3.1. Some Solutions $L_{3\times3}$ for a Diagonal Matrix $L_{3\times3}^2 \equiv A_{3\times3} \ mod \ N$

We assume the encryption key $A_{3\times3} \equiv \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix} \ mod \ N$ and $L_{3\times3} \equiv \begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix} \ mod \ N$ with $a, b, c, d, e, f, g, h, i$ and a_{ij} for $i, j = 1, 2, 3$ are integers such that $L_{3\times3}^2 \equiv A_{3\times3} \ mod \ N$. To get $L_{3\times3}$, we need to solve simultaneous equations as shown below.

$$a^2 + bd + cg \equiv a_{11} \ mod \ N, \tag{2}$$

$$ab + be + ch \equiv a_{12} \ mod \ N, \tag{3}$$

$$ac + bf + ci \equiv a_{13} \ mod \ N, \tag{4}$$

$$da + ed + fg \equiv a_{21} \ mod \ N, \tag{5}$$

$$db + e^2 + fh \equiv a_{22} \ mod \ N, \tag{6}$$

$$dc + ef + fi \equiv a_{23} \ mod \ N, \tag{7}$$

$$ga + hd + ig \equiv a_{31} \ mod \ N, \tag{8}$$

$$gb + he + hi \equiv a_{32} \ mod \ N, \tag{9}$$

and

$$gc + hf + i^2 \equiv a_{33} \ mod \ N. \tag{10}$$

Proposition 1. *Let* $L_{3\times3} \equiv \begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix}$ *mod* N *and* b, c, d, f, g, h *be relatively prime with* N. *The solution to a diagonal matrix* $L^2_{3\times3}$ *mod* N *is*

$$L_{3\times3} \equiv \begin{bmatrix} a & b & c \\ d & e & f \\ g & bc^{-1}d^{-1}fg & i \end{bmatrix} \ mod \ N, \tag{11}$$

where $a \equiv 2^{-1}(-bfc^{-1} + dcf^{-1} - fgd^{-1})$ *mod* N, $e \equiv 2^{-1}(bfc^{-1} - dcf^{-1} - fgd^{-1})$ *mod* N *and* $i \equiv 2^{-1}(-bfc^{-1} - dcf^{-1} + fgd^{-1})$ *mod* N.

Proof. Let $\begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix}^2 \equiv \begin{bmatrix} a^2 + bd + cg & 0 & 0 \\ 0 & db + e^2 + fh & 0 \\ 0 & 0 & gc + hf + i^2 \end{bmatrix}$ *mod* N. Substituting $a_{12} = a_{13} = a_{21} = a_{23} = a_{31} = a_{32} = 0$ into Equations (2)–(10).

From Equation (3),

$$-chb^{-1} \equiv a + e \ mod \ N \ \ for \ \ (b, N) = 1. \tag{12}$$

From Equation (4),

$$-bfc^{-1} \equiv a + i \ mod \ N \ \ for \ \ (c, N) = 1. \tag{13}$$

From Equation (5),

$$-fgd^{-1} \equiv a + e \ mod \ N \ \ for \ \ (d, N) = 1. \tag{14}$$

From Equation (7),

$$-dcf^{-1} \equiv e + i \ mod \ N \ \ for \ \ (f, N) = 1. \tag{15}$$

From Equation (8),

$$-hdg^{-1} \equiv a + i \ mod \ N \ \ for \ \ (g, N) = 1. \tag{16}$$

From Equation (9),

$$-gbh^{-1} \equiv e + i \ mod \ N \ \ for \ \ (h, N) = 1. \tag{17}$$

Substituting Equation (12) into Equation (14), we get

$$chb^{-1} \equiv fgd^{-1} \ mod \ N. \tag{18}$$

Substituting Equation (13) into Equation (16), we get

$$bfc^{-1} \equiv hdg^{-1} \ mod \ N. \tag{19}$$

Substituting Equation (15) into Equation (17), we get

$$dcf^{-1} \equiv gbh^{-1} \ mod \ N. \tag{20}$$

Hence, from Equations (18)–(20),

$$h \equiv bc^{-1}d^{-1}fg \ mod \ N. \tag{21}$$

From Equation (12), we have

$$a \equiv -fgd^{-1} - e \ mod \ N. \tag{22}$$

From Equation (15), we have

$$e \equiv -dcf^{-1} - i \ mod \ N. \tag{23}$$

Substituting Equation (23) into Equation (22), we get

$$a \equiv -fgd^{-1} + dcf^{-1} + i \ mod \ N. \tag{24}$$

Followed by substituting this equation into Equation (13), we have

$$i \equiv 2^{-1}(-bfc^{-1} + fgd^{-1} - dcf^{-1}) \ mod \ N. \tag{25}$$

Now, substituting Equation (25) into Equations (24) and (23), we get the following.

$$a \equiv 2^{-1}(-fgd^{-1} + dcf^{-1} - bfc^{-1}) \ mod \ N, \tag{26}$$

and

$$e \equiv 2^{-1}(-fgd^{-1} - dfc^{-1} + bfc^{-1}) \ mod \ N. \tag{27}$$

Finally, we substitute Equations (21) and (25)–(27) into Equations (2)–(10) to get $L_{3\times3}$ in terms of b, c, d, f and g. □

Next, we give an implementation for Proposition 1.

Example 1. *We let* $(b, c, d, f, g) \equiv (1, 2, 3, 4, 5)$ *mod* 13. *Then, by using Equations (25)–(27), we have* $L_{3\times3} \equiv \begin{bmatrix} 4 & 1 & 2 \\ 3 & 11 & 4 \\ 5 & 12 & 7 \end{bmatrix}$ *mod* 13. *Then,* $L_{3\times3}^2 \equiv \begin{bmatrix} 29 & 39 & 26 \\ 65 & 172 & 78 \\ 91 & 221 & 107 \end{bmatrix} \equiv 3I \mod 13.$

3.2. Some Solutions $L_{3\times3}$ for a Symmetric Matrix $L_{3\times3}^2 \equiv A_{3\times3}$ mod N

We investigate the key's feature $L_{3\times3}$ such that $L_{3\times3}^2 \equiv A_{3\times3} \ mod \ N$ where $A_{3\times3}$ is a symmetric matrix to secure our Cipher Hexagraphic Polyfunction system.

Proposition 2. *Let* $L_{3\times3} \equiv \begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix}$ *mod* N *and* $(2, N) = (b - d, N) = (c - g, N) = (f - h, N) = 1$. *Then* $L_{3\times3}$ *with* $a \equiv 2^{-1}((fg - ch)(b - d)^{-1} - (gb - dc)(f - h)^{-1} + (hd - bf)(c - g)^{-1}) \ mod \ N$, $e \equiv 2^{-1}((gb - dc)(f - h)^{-1} - (hd - bf)(c - g)^{-1} + (fg - ch)(b - d)^{-1}) \ mod \ N$ *and* $i \equiv 2^{-1}((hd - bf)(c - g)^{-1} - (fg - ch)(b - d)^{-1} + (gb - dc)(f - h)^{-1}) \ mod \ N$ *are solutions to a symmetric matrix* $L_{3\times3}^2 \ mod \ N$.

Proof. Let $\begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix}^2 \equiv \begin{bmatrix} a^2 + bd + cg & x & y \\ x & db + e^2 + fh & z \\ y & z & gc + hf + i^2 \end{bmatrix} \ mod \ N$. Substitute $a_{12} = a_{21} = x, a_{13} = a_{31} = y$ and $a_{23} = a_{32} = z$ into Equations (2)–(10). Substituting Equation (3) into Equation (5), we get $(a + e)(b - d) \equiv fg - ch \ mod \ N$.

Hence,

$$a \equiv (fg - ch)(b - d)^{-1} - e \ mod \ N for \ (b - d, N) = 1. \tag{28}$$

Substituting Equation (4) into Equation (8), we have $(a+i)(c-g) \equiv hd - bf \ mod\ N$. Hence,

$$i \equiv (hd - bf)(c-g)^{-1} - a \ mod\ N \ \ for \ \ (c-g, N) = 1. \tag{29}$$

Substituting Equation (7) into Equation (9), we have $(e+i)(f-h) \equiv gb - dc \ mod\ N$. Hence,

$$e \equiv (gb - dc)(f-h)^{-1} - i \ mod\ N \ \ for \ \ (f-h, N) = 1. \tag{30}$$

From Equations (28)–(30), we get the following

$$a \equiv 2^{-1}((fg - ch)(b-d)^{-1} - (gb - dc)(f-h)^{-1} + (hd - bf)(c-g)^{-1}) \ mod\ N, \tag{31}$$

$$e \equiv 2^{-1}((gb - dc)(f-h)^{-1} - (hd - bf)(c-g)^{-1} + (fg - ch)(b-d)^{-1}) \ mod\ N, \tag{32}$$

and

$$i \equiv 2^{-1}((hd - bf)(c-g)^{-1} - (fg - ch)(b-d)^{-1} + (gb - dc)(f-h)^{-1}) \ mod\ N. \tag{33}$$

Finally, we substitute Equations (31)–(33) into Equations (2)–(10) to get $L_{3\times 3}$ in terms of b, c, d, f, g and h. □

Next, we give an implementation of Proposition 2 as follows.

Example 2. *We let* $(b, c, d, f, g, h) \equiv (1, 2, 3, 4, 5, 6)$ *mod* 13. *Then, by using Equations (31)–(33) we have* $L_{3\times 3} \equiv \begin{bmatrix} 3 & 1 & 2 \\ 3 & 6 & 4 \\ 5 & 6 & 1 \end{bmatrix}$ *mod* 13. *Then,* $L_{3\times 3}^2 \equiv \begin{bmatrix} 9 & 8 & 12 \\ 8 & 11 & 8 \\ 12 & 8 & 9 \end{bmatrix}$ *mod* 13.

Now, from Proposition 2, we consider four cases when $L_{3\times 3}^2$ are symmetric as follows.

Case 1

From Equations (31)–(33), we let $b - d = 1$, $f - h = 1$ and $c - g = 1$. Thus, we get $b = 1 + d$, $f = 1 + h$ and $c = 1 + g$, respectively. For this case, we get the following result.

Corollary 1. *Let* $(2, N) = (4, N) = 1$. *If* $L_{3\times 3} \equiv \begin{bmatrix} -h - 2^{-1} & 1+d & 1+g \\ d & g + 2^{-1} & 1+h \\ g & h & -d - 2^{-1} \end{bmatrix}$ *mod* N, *then* $L_{3\times 3}^2 \equiv \begin{bmatrix} a_{11} & a_{12} & -a_{12} \\ a_{12} & a_{11} & a_{12} \\ -a_{12} & a_{12} & a_{11} \end{bmatrix}$ *mod* N *is symmetric where* $a_{11} \equiv 4^{-1} + d + h + g + g^2 + h^2 + d^2 \ mod\ N$ *and* $a_{12} \equiv g + gh + gd - hd \ mod\ N$.

Proof.

Let $L_{3\times 3} \equiv \begin{bmatrix} -h - 2^{-1} & 1+d & 1+g \\ d & g + 2^{-1} & 1+h \\ g & h & -d - 2^{-1} \end{bmatrix}$ *mod* N and $L_{3\times 3}^2 \equiv \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix}$ *mod* N.

Now,

$$a_{11} \equiv (-h-2^{-1})^2 + d(1+d) + g(1+g) \equiv 4^{-1} + d + g + h + d^2 + g^2 + h^2 \bmod N,$$
$$a_{12} \equiv -(h+2^{-1})(1+d) + (1+d)(g+2^{-1}) + (1+g)h \equiv g + gh + gd - hd \bmod N,$$
$$a_{13} \equiv -(h+2^{-1})(1+g) + (1+d)(1+h) - (1+g)(d+2^{-1}) \equiv hd - g - gh - gd \equiv -a_{12} \bmod N,$$
$$a_{21} \equiv -d(h+2^{-1}) + d(g+2^{-1}) + (1+h)g \equiv g + gh + gd - hd \equiv a_{12} \bmod N,$$
$$a_{22} \equiv (1+d)d + (2^{-1}+g)^2 + (1+h)h \equiv 4^{-1} + d + h + g + g^2 + h^2 + d^2 \equiv a_{11} \bmod N,$$
$$a_{23} \equiv d(1+g) + (2^{-1}+g)(1+h) - (1+h)(d+2^{-1}) \equiv g + gh + gd - hd \equiv a_{12} \bmod N,$$
$$a_{31} \equiv -g(2^{-1}+h) + hd - (2^{-1}+d)g \equiv hd - g - gh - gd \equiv -a_{12} \bmod N,$$
$$a_{32} \equiv g(1+d) + h(2^{-1}+g) - (d+2^{-1})h \equiv g + gh + gd - hd \equiv a_{12} \bmod N \text{ and}$$
$$a_{33} \equiv (1+g)g + (1+h)h + (2^{-1}+d)^2 \equiv 4^{-1} + d + h + g + g^2 + h^2 + d^2 \equiv a_{11} \bmod N.$$

Therefore, $L_{3\times3}^2 \equiv \begin{bmatrix} a_{11} & a_{12} & -a_{12} \\ a_{12} & a_{11} & a_{12} \\ -a_{12} & a_{12} & a_{11} \end{bmatrix} \bmod N$ is symmetric. □

Next, we give an implementation for Corollary 1.

Example 3. *We let* $(d,g,h) \equiv (1,2,3) \bmod 13$. *Then, we have* $L_{3\times3} \equiv \begin{bmatrix} 3 & 2 & 3 \\ 1 & 9 & 4 \\ 2 & 3 & 5 \end{bmatrix} \bmod 13$. *Followed by* $L_{3\times3}^2 \equiv \begin{bmatrix} 4 & 7 & 6 \\ 7 & 4 & 7 \\ 6 & 7 & 4 \end{bmatrix} \bmod 13$.

Case 2

From Equations (31)–(33), we let $b-d=1$, $f-h=-1$ and $c-g=-1$. Thus, we get $b=1+d$, $f=-1+h$ and $c=-1+g$, respectively. Followed by the following result.

Corollary 2. *Let* $(4,N)=1$. *If* $L_{3\times3} \equiv \begin{bmatrix} h-2^{-1} & 1+d & -1+g \\ d & -g+2^{-1} & -1+h \\ g & h & -d-2^{-1} \end{bmatrix} \bmod N$, *then* $L_{3\times3}^2 \equiv \begin{bmatrix} a_{11} & a_{12} & a_{12} \\ a_{12} & a_{11} & -a_{12} \\ a_{12} & -a_{12} & a_{11} \end{bmatrix} \bmod N$, *where* $a_{11} \equiv 4^{-1} + d - h - g + g^2 + h^2 + d^2 \bmod N$ *and* $a_{12} \equiv -g + gh - gd + hd \bmod N$.

Proof. The proving method is similar to Corollary 1. □

Example 4. *We let* $(d,g,h) \equiv (1,2,3) \bmod 13$. *Then, we have* $L_{3\times3} \equiv \begin{bmatrix} 9 & 2 & 1 \\ 1 & 5 & 2 \\ 2 & 3 & 5 \end{bmatrix} \bmod 13$. *Followed by* $L_{3\times3}^2 \equiv \begin{bmatrix} 7 & 5 & 5 \\ 5 & 7 & 8 \\ 5 & 8 & 7 \end{bmatrix} \bmod 13$.

Case 3

From Equations (31)–(33),we let $b-d=-1$, $f-h=-1$ and $c-g=1$. Thus, we get $b=-1+d$, $f=-1+h$ and $c=1+g$, respectively. Followed by the following result.

Corollary 3. *Let* $(2,N)=(4,N)=1$. *If* $L_{3\times3}\equiv\begin{bmatrix} h-2^{-1} & -1+d & 1+g \\ d & g+2^{-1} & -1+h \\ g & h & d-2^{-1} \end{bmatrix}$ *mod* N, *then* $L_{3\times3}^2\equiv\begin{bmatrix} a_{11} & a_{12} & a_{12} \\ a_{12} & a_{11} & a_{12} \\ a_{12} & a_{12} & a_{11} \end{bmatrix}$ *mod* N, *where* $a_{11}\equiv 4^{-1}-d-h+g+g^2+h^2+d^2$ *mod* N *and* $a_{12}\equiv -g+gh+gd+hd$ *mod* N.

Proof. The proving method is similar to Corollary 1. □

Example 5. *We let* $(d,g,h)\equiv(1,2,3)$ *mod* 13. *Then, we have* $L_{3\times3}\equiv\begin{bmatrix} 9 & 0 & 3 \\ 1 & 9 & 2 \\ 2 & 3 & 7 \end{bmatrix}$ *mod* 13. *Followed by* $L_{3\times3}^2\equiv\begin{bmatrix} 9 & 9 & 9 \\ 9 & 9 & 9 \\ 9 & 9 & 9 \end{bmatrix}$ *mod* 13.

Case 4

From Equations (31)–(33), we let $b-d=-1$, $f-h=1$ and $c-g=-1$. Thus, we get $b=-1+d$, $f=1+h$ and $c=-1+g$, respectively. Followed by the following result.

Corollary 4. *Let* $(2,N)=(4,N)$. *If* $L_{3\times3}\equiv\begin{bmatrix} -h-2^{-1} & -1+d & -1+g \\ d & -g+2^{-1} & 1+h \\ g & h & d-2^{-1} \end{bmatrix}$ *mod* N, *then* $L_{3\times3}^2\equiv\begin{bmatrix} a_{11} & a_{12} & -a_{12} \\ a_{12} & a_{11} & -a_{12} \\ -a_{12} & -a_{12} & a_{11} \end{bmatrix}$ *mod* N, *where* $a_{11}\equiv 4^{-1}-d+h-g+g^2+h^2+d^2$ *mod* N *and* $a_{12}\equiv g+gh-gd-hd$ *mod* N.

Proof. The proving method is similar to Corollary 1. □

Example 6. *We let* $(d,g,h)\equiv(1,2,3)$ *mod* 13. *Then, we have* $L_{3\times3}\equiv\begin{bmatrix} 3 & 0 & 1 \\ 1 & 5 & 4 \\ 2 & 3 & 7 \end{bmatrix}$ *mod* 13. *Followed by* $L_{3\times3}^2\equiv\begin{bmatrix} 11 & 3 & 10 \\ 3 & 11 & 10 \\ 10 & 10 & 11 \end{bmatrix}$ *mod* 13.

Now, we investigate the key's feature $L_{3\times3}$ such that $L_{3\times3}^2\equiv A_{3\times3}$ *mod* N where $A_{3\times3}$ is a symmetric matrix by subtituting $c=f=0$ into Equations (31)–(33). We get the following result.

Corollary 5. *Let* $(2,N)=(4,N)=(h,N)=(g,N)=1$. *If* $L_{3\times3}\equiv\begin{bmatrix} 2^{-1}(gbh^{-1}-hdg^{-1}) & b & 0 \\ d & -2^{-1}(gbh^{-1}-hdg^{-1}) & 0 \\ g & h & 2^{-1}(-hdg^{-1}-gbh^{-1}) \end{bmatrix}$ *mod* N *then,* $L_{3\times3}^2\equiv(4^{-1}(g^2b^2h^{-2}+h^2d^2g^{-2})+2^{-1}bd)I$ *mod* N.

Proof.

Let $L_{3\times3} \equiv \begin{bmatrix} 2^{-1}(gbh^{-1} - hdg^{-1}) & b & 0 \\ d & -2^{-1}(gbh^{-1} - hdg^{-1}) & 0 \\ g & h & 2^{-1}(-hdg^{-1} - gbh^{-1}) \end{bmatrix} mod\ N.$

Then, $L^2_{3\times3} \equiv \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix} mod\ N$

where

$$
\begin{aligned}
a_{11} &\equiv 4^{-1}(gbh^{-1} - hdg^{-1})^2 + bd\ mod\ N \equiv 4^{-1}(g^2b^2h^{-2} + h^2d^2g^{-2}) + 2^{-1}bd\ mod\ N,\\
a_{12} &\equiv 2^{-1}b(gbh^{-1} - hdg^{-1}) + 2^{-1}b(hdg^{-1} - gbh^{-1}) \equiv 0\ mod\ N,\\
a_{13} &\equiv 0\ mod\ N,\\
a_{21} &\equiv 2^{-1}d(gbh^{-1} - hdg^{-1}) + 2^{-1}(hdg^{-1} - gbh^{-1})d \equiv 0\ mod\ N,\\
a_{22} &\equiv 4^{-1}(hdg^{-1} - gbh^{-1})^2 + bd \equiv a_{11}\ mod\ N,\\
a_{23} &\equiv 0\ mod\ N,\\
a_{31} &\equiv 2^{-1}g(gbh^{-1} - hdg^{-1}) + hd + 2^{-1}(-hdg^{-1} - gbh^{-1})g \equiv 0\ mod\ N,\\
a_{32} &\equiv gb + 2^{-1}h(hdg^{-1} - gbh^{-1}) + 2^{-1}(-hdg^{-1} - gbh^{-1})h \equiv 0\ mod\ N\ and\\
a_{33} &\equiv 4^{-1}(-hdg^{-1} - gbh^{-1})^2\ mod\ N\\
&\equiv 4^{-1}(g^2b^2h^{-2} + 2bd + h^2d^2g^{-2})\ mod\ N \equiv 4^{-1}(g^2b^2h^{-2} + h^2d^2g^{-2}) + 2^{-1}bd \equiv a_{11}\ mod\ N.
\end{aligned}
$$

We can clearly see that $L^2_{3\times3} \equiv (4^{-1}(g^2b^2h^{-2} + h^2d^2g^{-2}) + 2^{-1}bd)I\ mod\ N.$ □

Next, we give an implementation for Corollary 5.

Example 7. *We let* $(b, d, g, h) \equiv (1, 2, 3, 4)\ mod\ 13$. *Then, we have* $L_{3\times3} \equiv \begin{bmatrix} -21 & 1 & 0 \\ 2 & 21 & 0 \\ 3 & 4 & -51 \end{bmatrix} \equiv \begin{bmatrix} 5 & 1 & 0 \\ 2 & 8 & 0 \\ 3 & 4 & 1 \end{bmatrix} mod\ 13$. *Followed by* $L^2_{3\times3} \equiv \begin{bmatrix} 27 & 13 & 0 \\ 26 & 66 & 0 \\ 29 & 39 & 1 \end{bmatrix} \equiv \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} mod\ 13.$

Futhermore, we investigate the key's feature of $L_{3\times3}$ such that $L^2_{3\times3} \equiv A_{3\times3}\ mod\ N$ where $A_{3\times3}$ is a symmetric matrix by subtituting $b = c = f = 0$ into Equations (31)–(33). We get the following result.

Corollary 6. *If* $L_{3\times3} \equiv \begin{bmatrix} -2^{-1}hdg^{-1} & 0 & 0 \\ d & 2^{-1}hdg^{-1} & 0 \\ g & h & -2^{-1}hdg^{-1} \end{bmatrix} mod\ N$, *where* $(g, N) = (2, N) = 1$, *then* $L^2_{3\times3} \equiv 4^{-1}h^2d^2g^{-2}I\ mod\ N$.

Proof. The proving method is similar to Corollary 5. □

Lastly, we investigate the key's feature $L_{3\times3}$ such that $L^2_{3\times3} \equiv A_{3\times3}\ mod\ N$ where $A_{3\times3}$ is a symmetric matrix by substituting $d = g = h = 0$ into Equations (31)–(33). We get the following result.

Corollary 7. *If* $L_{3\times3} \equiv \begin{bmatrix} -2^{-1}bfc^{-1} & b & c \\ 0 & 2^{-1}bfc^{-1} & f \\ 0 & 0 & -2^{-1}bfc^{-1} \end{bmatrix} mod\ N$, *where* $(c, m) = (2, N) = 1$, *then* $L^2_{3\times3} \equiv 4^{-1}b^2f^2c^{-2}I\ mod\ N$.

Proof. The proving method is similar to Corollary 5. □

3.3. Generation of Self-Invertible Matrix

In this section, we apply in the following example, the method of generating of self-invertible $n \times n$ matrices that was mentioned earlier. In this paper, we choose $n = 6$.

Example 8. *Consider* $L_{3\times3}$ *and* $L_{6\times6}$ *as two secret keys. Let* $L_{3\times3} \equiv \begin{bmatrix} a & b & c \\ d & -a-fgd^{-1} & f \\ g & bc^{-1}d^{-1}fg & -a-bfc^{-1} \end{bmatrix}$ *mod* N *with* $a = 2^{-1}(-fgd^{-1} + dcf^{-1} - bfc^{-1})$, *where* b, c, d, f, g, h *are relatively prime with* N. *This is the solution to a diagonal matrix* $L^2_{3\times3}$ *mod* N *using Proposition 1.*

Now, let $A_{11} = L_{3\times3}$ *and* $A_{22} \equiv -A_{11} \equiv -L_{3\times3} \equiv \begin{bmatrix} -a & -b & -c \\ -d & a+fgd^{-1} & -f \\ -g & -bc^{-1}d^{-1}fg & a+bfc^{-1} \end{bmatrix}$ *mod* N.

We choose $k = 1$, *therefore* $A_{12} \equiv k(I - A_{11}) \equiv \begin{bmatrix} 1-a & -b & -c \\ -d & 1+a+fgd^{-1} & -f \\ -g & -bc^{-1}d^{-1}fg & 1+a+bfc^{-1} \end{bmatrix}$ *mod* N.

and $A_{21} \equiv I + A_{11} \equiv k^{-1}(I + L_{3\times3}) \equiv \begin{bmatrix} 1+a & b & c \\ d & 1-a-fgd^{-1} & f \\ g & bc^{-1}d^{-1}fg & 1-a-bfc^{-1} \end{bmatrix}$ *mod* N. *Since* $L_{6\times6} \equiv \begin{bmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{bmatrix}$ *mod* N, *then*

$$L_{6\times6} \equiv \left[\begin{array}{ccc|ccc} a & b & c & 1-a & -b & -c \\ d & -a-fgd^{-1} & f & -d & 1+a+fgd^{-1} & -f \\ g & bc^{-1}d^{-1}fg & -a-bfc^{-1} & -g & -bc^{-1}d^{-1}fg & 1+a+bfc^{-1} \\ \hline 1+a & b & c & -a & -b & -c \\ d & 1-a-fgd^{-1} & f & -d & a+fgd^{-1} & -f \\ g & bc^{-1}d^{-1}fg & 1-a-bfc^{-1} & -g & -bc^{-1}d^{-1}fg & a+bfc^{-1} \end{array}\right] \text{ mod } N.$$

Suppose $k = 1$, using similar procedure as in Example 8, we can get all the following self-invertible matrices produced by $L_{3\times3}$ from Proposition 2 and Corrolaries 1–7.

From Propositions 2, we get $L_{6\times6} \equiv \left[\begin{array}{ccc|ccc} a & b & c & 1-a & -b & -c \\ d & e & f & -d & 1-e & -f \\ g & h & i & -g & -h & 1-i \\ \hline 1+a & b & c & -a & -b & -c \\ d & 1+e & f & -d & -e & -f \\ g & h & 1+i & -g & -h & -i \end{array}\right]$ *mod* N where

$a = 2^{-1}((fg-ch)(b-d)^{-1} - (gb-dc)(f-h)^{-1} + (hd-bf)(c-g)^{-1})$,
$e = a + (gb-dc)(f-h)^{-1} - (hd-bf)(c-g)^{-1}$,
$i = -a + (hd-bf)(c-g)^{-1}$ and
$(b-d, N) = (f-h, N) = (c-g, N) = (2, N) = 1$.
From Corrolary 1, we get

$$L_{6\times6} \equiv \left[\begin{array}{ccc|ccc} -h-2^{-1} & 1+d & 1+g & 1+h+2^{-1} & -1-d & -1-g \\ d & g+2^{-1} & 1+h & -d & 1-g-2^{-1} & -1-h \\ g & h & -d-2^{-1} & -g & -h & 1+d+2^{-1} \\ \hline 1-h-2^{-1} & 1+d & 1+g & h+2^{-1} & -1-d & -1-g \\ d & 1+g+2^{-1} & 1+h & -d & -g-2^{-1} & -1-h \\ g & h & 1-d-2^{-1} & -g & -h & d+2^{-1} \end{array}\right] \text{ mod } N.$$

From Corrolary 2, we get

$$L_{6\times6} \equiv \left[\begin{array}{ccc|ccc} h-2^{-1} & 1+d & -1+g & 1-h+2^{-1} & -1-d & 1-g \\ d & -g+2^{-1} & -1+h & -d & 1-g+2^{-1} & 1-h \\ g & h & -d-2^{-1} & -g & -h & 1+d+2^{-1} \\ \hline 1+h-2^{-1} & 1+d & -1+g & -h+2^{-1} & -1-d & 1-g \\ d & 1-g+2^{-1} & -1+h & -d & g-2^{-1} & 1-h \\ g & h & 1-d-2^{-1} & -g & -h & d+2^{-1} \end{array}\right] \ mod\ N.$$

From Corrolary 3, we get

$$L_{6\times6} \equiv \left[\begin{array}{ccc|ccc} h-2^{-1} & -1+d & 1+g & 1-h+2^{-1} & 1-d & -1-g \\ d & g+2^{-1} & -1+h & -d & 1-g-2^{-1} & 1-h \\ g & h & d-2^{-1} & -g & -h & 1-d+2^{-1} \\ \hline 1+h-2^{-1} & -1+d & 1+g & -h+2^{-1} & 1-d & -1-g \\ d & 1+g+2^{-1} & -1+h & -d & -g-2^{-1} & 1-h \\ g & h & 1+d-2^{-1} & -g & -h & -d+2^{-1} \end{array}\right] \ mod\ N.$$

From Corrolary 4, we get

$$L_{6\times6} \equiv \left[\begin{array}{ccc|ccc} -h-2^{-1} & -1+d & -1+g & 1+h+2^{-1} & 1-d & 1-g \\ d & g+2^{-1} & 1+h & -d & 1+g-2^{-1} & -1-h \\ g & h & d-2^{-1} & -g & -h & 1-d+2^{-1} \\ \hline 1-h-2^{-1} & -1+d & -1+g & h+2^{-1} & 1-d & 1-g \\ d & 1-g+2^{-1} & 1+h & -d & g-2^{-1} & -1-h \\ g & h & 1+d-2^{-1} & -g & -h & -d+2^{-1} \end{array}\right] \ mod\ N.$$

From Corrolary 5, we get

$$L_{6\times6} \equiv \left[\begin{array}{ccc|ccc} a & b & 0 & a+2hdg^{-1} & -b & 0 \\ d & -a & 0 & -d & 3a+2hdg^{-1} & 0 \\ g & h & -a-hdg^{-1} & -g & -h & 3(a+hdg^{-1}) \\ \hline 3a+2hdg^{-1} & b & 0 & -a & -b & 0 \\ d & a+2hdg^{-1} & 0 & -d & a & 0 \\ g & h & a+hdg^{-1} & -g & -h & a+hdg^{-1} \end{array}\right] \ mod\ N$$

where $a = 2^{-1}(gbh^{-1} - hdg^{-1})$.

From Corrolary 6, we get

$$L_{6\times6} \equiv \left[\begin{array}{ccc|ccc} -2^{-1}hdg^{-1} & 0 & 0 & 3(2^{-1}hdg^{-1}) & 0 & 0 \\ d & 2^{-1}hdg^{-1} & 0 & -d & 2^{-1}hdg^{-1} & 0 \\ g & h & 2^{-1}hdg^{-1} & -g & -h & 3(2^{-1}hdg^{-1}) \\ \hline 2^{-1}hdg^{-1} & 0 & 0 & 2^{-1}hdg^{-1} & 0 & 0 \\ d & 3(2^{-1}hdg^{-1}) & 0 & -d & -2^{-1}hdg^{-1} & 0 \\ g & h & 2^{-1}hdg^{-1} & -g & -h & 2^{-1}hdg^{-1} \end{array}\right] \ mod\ N.$$

From Corrolary 7, we get

$$L_{6\times6} \equiv \left[\begin{array}{ccc|ccc} -2^{-1}bfc^{-1} & b & c & 3(2^{-1}bfc^{-1}) & -b & -c \\ 0 & 2^{-1}bfc^{-1} & f & 0 & 2^{-1}bfc^{-1} & -f \\ 0 & 0 & -2^{-1}bfc^{-1} & 0 & 0 & 3(2^{-1}bfc^{-1}) \\ \hline 2^{-1}bfc^{-1} & b & c & 2^{-1}bfc^{-1} & -b & -c \\ 0 & 3(2^{-1}bfc^{-1}) & f & 0 & -2^{-1}bfc^{-1} & -f \\ 0 & 0 & 2^{-1}bfc^{-1} & 0 & 0 & 2^{-1}bfc^{-1} \end{array}\right] \ mod\ N.$$

3.4. Effect of Self-Invertible Key on Cipher Hexagraphic Polyfunction

Cipher Hexagraphic Polyfunction Transformation is constructed based on the following theorem.

Theorem 1. *Let Cipher Hexagraphic Polyfunction Transformation be defined as Definition 1. Say that the determinant for $A_{6\times6}$ is not a zero and $(|A_{6\times6}|, N) = 1$, so $P_{6\times j}$ have unique solutions and the decryption algorithms are as follows:*

$$C_{6\times j}^{(t-1)} \equiv A_{6\times6}^{-1} C_{6\times j}^{(t)} \; mod\, N,$$

$$C_{6\times j}^{(t-2)} \equiv A_{6\times6}^{-1} C_{6\times j}^{(t-1)} \; mod\, N,$$

$$\cdots$$

$$C_{6\times j}^{(2)} \equiv A_{6\times6}^{-1} C_{6\times j}^{(3)} \; mod\, N,$$

$$C_{6\times j}^{(1)} \equiv A_{6\times6}^{-1} C_{6\times j}^{(2)} \; mod\, N,$$

$$P_{6\times j} \equiv A_{6\times6}^{-1} C_{6\times j}^{(1)} \; mod\, N$$

where $A_{6\times6}^{-1}$ is the inverse matrix for $A_{6\times6}$ which acts as the decryption key.

Proof. Let Cipher Hexagraphic Polyfunction transformations be as follows.

$$C_{6\times j}^{(1)} \equiv A_{6\times6} P_{6\times j} \; mod\, N,$$

$$C_{6\times j}^{(2)} \equiv A_{6\times6} C_{6\times j}^{(1)} \; mod\, N,$$

$$C_{6\times j}^{(3)} \equiv A_{6\times6} C_{6\times j}^{(2)} \; mod\, N,$$

$$\cdots$$

$$C_{6\times j}^{(t-1)} \equiv A_{6\times6} C_{6\times j}^{(t-2)} \; mod\, N,$$

$$C_{6\times j}^{(t)} \equiv A_{6\times6} C_{6\times j}^{(t-1)} \; mod\, N.$$

There exist the inverse of $A_{6\times6}$ such that $A_{6\times6} A_{6\times6}^{-1} \equiv I \; mod\, N$ when $|A_{6\times6}| \neq 0$. So

$$A_{6\times6}^{-1} C_{6\times j}^{(t)} \equiv A_{6\times6}^{-1} A_{6\times6} C_{6\times j}^{(t-1)} \equiv C_{6\times j}^{(t-1)} \; mod\, N, \tag{34}$$

$$A_{6\times6}^{-1} C_{6\times j}^{(t-1)} \equiv A_{6\times6}^{-1} A_{6\times6} C_{6\times j}^{(t-2)} \equiv C_{6\times j}^{(t-2)} \; mod\, N, \tag{35}$$

$$\cdots$$

$$A_{6\times6}^{-1} C_{6\times j}^{(3)} \equiv A_{6\times6}^{-1} A_{6\times6} C_{6\times j}^{(2)} \equiv C_{6\times j}^{(2)} \; mod\, N, \tag{36}$$

$$A_{6\times6}^{-1} C_{6\times j}^{(2)} \equiv A_{6\times6}^{-1} A_{6\times6} C_{6\times j}^{(1)} \equiv C_{6\times j}^{(1)} \; mod\, N, \tag{37}$$

$$A_{6\times6}^{-1} C_{6\times j}^{(1)} \equiv A_{6\times6}^{-1} A_{6\times6} P_{6\times j} \equiv P_{6\times j} \; mod\, N, \tag{38}$$

and

$$(adj A_{6\times6}) C_{6\times j}^{(t)} \equiv |A_{6\times6}| C_{6\times j}^{(t-1)} \; mod\, N, \tag{39}$$

$$(adj A_{6\times6}) C_{6\times j}^{(t-1)} \equiv |A_{6\times6}| C_{6\times j}^{(t-2)} \; mod\, N, \tag{40}$$

$$\cdots$$

$$(adjA_{6\times 6})C^{(3)}_{6\times j} \equiv |A_{6\times 6}|C^{(2)}_{6\times j} \; mod\, N, \tag{41}$$

$$(adjA_{6\times 6})C^{(2)}_{6\times j} \equiv |A_{6\times 6}|C^{(1)}_{6\times j} \; mod\, N, \tag{42}$$

$$(adjA_{6\times 6})C^{(1)}_{6\times j} \equiv |A_{6\times 6}|P_{6\times j} \; mod\, N. \tag{43}$$

From Equations (34)–(38), we get the decryption algorithm as follows:

$$C^{(t-1)}_{6\times j} \equiv A^{-1}_{6\times 6}C^{(t)}_{6\times j} \; mod\, N,$$
$$C^{(t-2)}_{6\times j} \equiv A^{-1}_{6\times 6}C^{(t-1)}_{6\times j} \; mod\, N,$$
$$\dots$$
$$C^{(2)}_{6\times j} \equiv A^{-1}_{6\times 6}C^{(3)}_{6\times j} \; mod\, N,$$
$$C^{(1)}_{6\times j} \equiv A^{-1}_{6\times 6}C^{(2)}_{6\times j} \; mod\, N,$$
$$P_{6\times j} \equiv A^{-1}_{6\times 6}C^{(1)}_{6\times j} \; mod\, N.$$

From Equations (39)–(43), if $(|A_{6\times 6}|, N) = 1$ so $P_{6\times j}$ have unique solutions. □

In Theorem 1, the repeated process occured (that is $C^{(t)}_{6\times j} \equiv P_{6\times j} \; mod\, N$) when $A^t_{6\times 6} \equiv I \; mod\, N$. The sender can encryp the plain text until the $(t-1)th$ transformation to make sure that the message is kept in secret. It is different with the effect of such a system when we consider $A_{6\times 6} = \begin{bmatrix} L_{3\times 3} & (I - L_{3\times 3})k \\ (I + L_{3\times 3})k^{-1} & -L_{3\times 3} \end{bmatrix}$. The following is an example of using this key. Of course the use of long transformation from plain text to cipher text is more suitable for cryptographic proposals. We begin with examining the patterns of cipher text when using the small number of transformations.

Suppose the plain text numbers are arranged into $P_{6\times j}$. We choose any generated self-invertible matrix $L_{6\times 6}$. Before we proceed to do the encryption process, we need to make sure that the secret key that we have chosen fulfils the conditions as stated in Theorem 1; that is, $|L_{6\times 6}| \equiv 1 \; mod\, N$. Thus, $(|L_{6\times 6}|, N) = 1$. Now, the encryption process is as follows:

$$C^{(1)}_{6\times j} \equiv L_{6\times 6}P_{6\times j} \; mod\, N,$$
$$C^{(2)}_{6\times j} \equiv L_{6\times 6}C^{(1)}_{6\times j} \equiv P_{6\times j} \; mod\, N,$$
$$C^{(3)}_{6\times j} \equiv L_{6\times 6}C^{(2)}_{6\times j} \equiv C^{(1)}_{6\times j} \; mod\, N,$$
$$C^{(4)}_{6\times j} \equiv L_{6\times 6}C^{(3)}_{6\times j} \equiv P_{6\times j} \; mod\, N,$$
$$\dots\dots$$

The above process is continued such that $C^{(2g)}_{6\times j} \equiv P_{6\times j} \; mod\, N$ and $C^{(2g-1)}_{6\times j} \equiv P_{6\times j} \; mod\, N$ for $g \in Z^+$.

This is because of $L^2_{6\times 6} \equiv I \; mod\, N$. Thus, the transforming process after $C^{(1)}_{6\times j}$ is not necessary. Now, we scrutinize the condition for $A_{6\times 6}$ in Theorem 1. If we want to convert a plain text to its cipher text via the third transformation, it is necessary to consider condition $A_{6\times 6}A^{-1}_{6\times 6} \not\equiv I \; mod\, N$. Therefore, all nine patterns of self-invertible matrices ($L_{6\times 6}$) in Section 3.3 should be avoided from the system of Cipher Hexagraphic Polyfunction before implementing $L_{3\times 3}$. This can enhance the security of the cipher message.

Next, we give an implementation for the self-invertible matrix $L_{6\times 6}$ from Example 8.

Example 9. *We let* $(a,b,c,d,f,g) \equiv (109,35,77,91,13,1)$ *mod* 256. *Since* $77^{-1} = 133$ *and* $91^{-1} = 211$, *then we have*

$$L_{6\times6} \equiv \left[\begin{array}{ccc|ccc} 109 & 35 & 77 & 148 & 221 & 179 \\ 91 & 220 & 13 & 165 & 137 & 243 \\ 1 & 153 & 48 & 255 & 3 & 209 \\ \hline 110 & 35 & 77 & 147 & 221 & 179 \\ 91 & 221 & 13 & 165 & 36 & 243 \\ 1 & 153 & 49 & 255 & 3 & 208 \end{array}\right] \text{ mod } 256.$$

We have to make sure that the secret key follows the conditions $|L_{6\times6}| \neq 0$ *before proceeding to the encryption process. In this case,* $|L_{6\times6}| \equiv 171$ *mod* 256. *Since* $L_{6\times6}$ *satisfies* $(|L_{6\times6}|, 256) = 1$, *then* $P_{6\times6}$ *has a unique solution and the decryption for* $C^{(1)}_{6\times6}$ *uses* $P_{6\times6} \equiv L^{-1}_{6\times6} C^{(1)}_{6\times6}$ *mod* 256. *Let us say we use the phrase 'IHaveOneSister,TwoBrothersAndANiece' as the plain text and* $C^{(t)}_{6\times6} \equiv L^{t}_{6\times6} P_{6\times6}$ *mod* 256, *for* $t = 1,2,3$ *will be used. This message then be translated into the corresponding numbers based on ASCII (refer https://www.ascii-code.com) and [15] as follows:*
73 72 97 118 101 79 110 101 83 105 115 116 101 114 44 84 119 111 66 114 111 116 104 101 114 115 65 110 100 65 78 105 101 99 101 46

The numbers are arranged into matrix of 6 rows and 6 columns as follows:

$$P_{6\times6} \equiv \left[\begin{array}{ccc|ccc} 73 & 110 & 101 & 66 & 114 & 78 \\ 72 & 101 & 114 & 114 & 115 & 105 \\ 97 & 83 & 44 & 111 & 65 & 101 \\ \hline 118 & 105 & 84 & 116 & 110 & 99 \\ 101 & 115 & 119 & 104 & 100 & 101 \\ 79 & 116 & 111 & 101 & 65 & 46 \end{array}\right] \text{ mod } 256.$$

Now, the encryption process of this massage is as follows:

$$C^{(1)}_{6\times6} \equiv L_{6\times6} P_{6\times6} \equiv \left[\begin{array}{ccc|ccc} 192 & 179 & 187 & 138 & 47 & 137 \\ 100 & 133 & 207 & 188 & 180 & 41 \\ 45 & 235 & 243 & 13 & 60 & 205 \\ \hline 147 & 184 & 204 & 88 & 51 & 116 \\ 71 & 119 & 202 & 198 & 195 & 45 \\ 63 & 202 & 176 & 23 & 60 & 4 \end{array}\right] \text{ mod } 256,$$

$$C^{(2)}_{6\times6} \equiv L_{6\times6} C^{(1)}_{6\times6} \equiv \left[\begin{array}{ccc|ccc} 73 & 110 & 101 & 66 & 114 & 78 \\ 72 & 101 & 114 & 114 & 115 & 105 \\ 97 & 83 & 44 & 111 & 65 & 101 \\ \hline 118 & 105 & 84 & 116 & 110 & 99 \\ 101 & 115 & 119 & 104 & 100 & 101 \\ 79 & 116 & 111 & 101 & 65 & 46 \end{array}\right] \text{ mod } 256,$$

$$C^{(3)}_{6\times6} \equiv L_{6\times6} C^{(2)}_{6\times6} \equiv \left[\begin{array}{ccc|ccc} 192 & 179 & 187 & 138 & 47 & 137 \\ 100 & 133 & 207 & 188 & 180 & 41 \\ 45 & 235 & 243 & 13 & 60 & 205 \\ \hline 147 & 184 & 204 & 88 & 51 & 116 \\ 71 & 119 & 202 & 198 & 195 & 45 \\ 63 & 202 & 176 & 23 & 60 & 4 \end{array}\right] \text{ mod } 256.$$

Therefore, the corresponding numbers of the cipher text from the first and third transformation is as follows:
À d - " G ? 3 … ë ¸ w Ê » Ï ó Ì Ê º Š ¼ CR X Æ ETB / ′ < 3 Ã < ‰) Í t - EOT
Now, maybe the third parties can analyze this message using the nine patterns of self-invertible matrices

mentioned in Section 3.3 even though they do not know the decryption keys. By using $P_{6\times 6} \equiv L_{6\times 6}C_{6\times 6} \mod 256$, *they can expect that the entries' element in the first row of* $P_{6\times 6}$ *are*

$$p_{11} = 45a + 29b + 238c + 147, p_{12} = 251a + 14b + 33c + 184, p_{13} = 239a + 5b + 67c + 204,$$

$$p_{14} = 50a + 246b + 246c + 88, p_{15} = 252a + 241b + 51, p_{16} = 21a + 252b + 201c + 116,$$

the entries' element in the second row of $P_{6\times 6}$ *are*

$$p_{21} = 45d + 227a + 227fgd^{-1} + 238f + 71, p_{22} = 251d + 242a + 242fgd^{-1} + 33f + 119,$$

$$p_{23} = 239d + 251a + 251fgd^{-1} + 67f + 202, p_{24} = 50d + 10a + 10fgd^{-1} + 246f + 198,$$

$$p_{25} = 252d + 15a + 15fgd^{-1} + 195, p_{26} = 21d + 4a + 4fgd^{-1} + 201f + 45,$$

the entries' element in the third row of $P_{6\times 6}$ *are*

$$p_{31} = 45g + 29bfgc^{-1}d^{-1} + 18a + 18bfc^{-1} + 63, p_{32} = 251g + 14bfgc^{-1}d^{-1} + 223a + 223bfc^{-1} + 202,$$

$$p_{33} = 239g + 5bfgc^{-1}d^{-1} + 189a + 189bfc^{-1} + 176, p_{34} = 50g + 246bfgc^{-1}d^{-1} + 10a + 10bfc^{-1} + 23,$$

$$p_{35} = 252g + 241bfgc^{-1}d^{-1} + 60, p_{36} = 21g + 252bfgc^{-1}d^{-1} + 55a + 55bfc^{-1} + 4,$$

the entries' element in the fourth row of $P_{6\times 6}$ *are*

$$p_{41} = 192 + 45a + 29b + 238c, p_{42} = 179 + 251a + 14b + 33c, p_{43} = 187 + 239a + 5b + 67c,$$

$$p_{44} = 138 + 50a + 246b + 246c, p_{45} = 47 + 252a + 241b, p_{46} = 137 + 21a + 252b + 201c,$$

the entries' element in the fifth row of $P_{6\times 6}$ *are*

$$p_{51} = 45d + 100 + 227a + 227fgd^{-1} + 238f, p_{52} = 251d + 133 + 242a + 242fgd^{-1} + 33f,$$

$$p_{53} = 239d + 207 + 251a + 251fgd^{-1} + 67f, p_{54} = 50d + 188 + 10a + 10fgd^{-1} + 246f,$$

$$p_{55} = 252d + 180 + 15a + 15fgd^{-1}, p_{56} = 21d + 41 + 4a + 4fgd^{-1} + 201f,$$

and the entries' element in the sixth row of $P_{6\times 6}$ *are*

$$p_{61} = 45g + 29bfgc^{-1}d^{-1} + 45 + 18a + 18bfc^{-1}, p_{62} = 251g + 14bfgc^{-1}d^{-1} + 235 + 223a + 223bfc^{-1},$$

$$p_{63} = 239g + 5bfgc^{-1}d^{-1} + 243 + 189a + 189bfc^{-1}, p_{64} = 50g + 246bfgc^{-1}d^{-1} + 13 + 10a + 10bfc^{-1,}$$

$$p_{65} = 252g + 241bfgc^{-1}d^{-1} + 60, p_{66} = 21g + 252bfgc^{-1}d^{-1} + 205 + 55a + 55bfc^{-1}.$$

Using the self-invertible such as in Example 8, there are 256^3 *combinations of* a, b *and* c *from the first and fourth rows,* 256^4 *combinations of* a, d, f *and* g *from the second and fifth rows and* 256^6 *combinations of* a, b, c, d, f *and* g *from the last row that need to be tested before deriving the actual value of the plain text. The same method is repeated by using another eight types of self-invertible keys until the actual message is found. It is not impossible to get it so fast with the appropriate algorithm and high performance computer.*

Previously, the study of self-invertible effects $A_{4\times 4}$ on the system of Cipher Polygraphic Polyfunction was pioneered by [7]. In this paper, we have the effect of using nine types of self-invertible keys $A_{6\times 6}$ on the same system. Perhaps in the future, we can expect the self-invertible pattern for $A_{i\times i}$ for any even number i. This scenario is aimed to strengthening the prerequisites for a secret key before sending the message.

4. Conclusions

In conclusion, we obtained nine solutions $L_{3\times3}$ from $L_{3\times3}^2 \equiv A_{3\times3}\ mod\ N$ where $A_{3\times3}$ is a diagonal and symmetric matricex. As a result, we produced nine patterns of self-invertible keys $\begin{bmatrix} L_{3\times3} & I - L_{3\times3} \\ I + L_{3\times3} & -L_{3\times3} \end{bmatrix}$ such as in Section 3.3. We found that the plain texts are easily obtained by third parties when these keys are used in Cipher Hexagraphic Polyfunction transformations. This is because the self-invertible encryption key causes the repeating process in the system. With this approach, we have updated the prerequisite for the secret key for the Cipher Polygraphic Polyfunction system for $A_{6\times6}$ before sending the secret message.

Author Contributions: Conceptualization, S.L.P.C. and F.Y.; methodology, F.Y.; software, S.L.P.C.; validation, F.Y. and S.L.P.C.; formal analysis, F.Y.; investigation, F.Y.; writing—original draft preparation, S.L.P.C.; writing—review and editing, F.Y.; supervision, F.Y.; funding acquisition, F.Y.

Funding: This research was funded by Universiti Putra Malaysia for a support via Geran Putra GP/2018/9595400.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Panigrahy, K.S.; Acharya, B.; Jena, D. Image Encryption Using Self-Invertible Key Matrix of Hill Cipher Algorithm. In Proceedings of the International Conference on Advance in Computing, Chikhli, India, 21–22 February 2008; pp. 1–4.
2. Asbullah, M.A.; Ariffin, M.R.K. Another Proof of Wiener's Short Secret Exponent. *Malays. J. Sci.* **2019**, 67–73. [CrossRef]
3. Rivest, R.; Shamir, A.; Adleman, L. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Commun. ACM* **1978**, *21*, 120–126. [CrossRef]
4. Yunos, F. Beberapa Penggunaan Teori Nombor Dalam Kriptografi. Ph.D. Thesis, University Putra Malaysia, Serdang, Malaysia, 2001.
5. Yunos, F.; Said, M.R.M.; Atan, K.A.M. Transformasi Polifungsi Saifer Digrafik Bermodulo N_1 dalam Sistem Kriptografi. In *Proceeding Simposium Kebangsaan Sains Matematik ke-9*; Persatuan Sains Matematik Malaysia; Institut Statistik Malaysia dan Pusat Pengajian Sains Matematik, Universiti Kebangsaan Malaysia: Selangor, Malaysia, 2001; pp. 88–95.
6. Yunos, F.; Atan, K.A.M.; Said, M.R.M. Transformasi Polifungsi LUC dalam Sistem Kriptografi. *J. Teknol.* **2002**, *37*, 21–38. [CrossRef]
7. Yunos, F.; Chin, L.S.; Said, M.R.M. Effect of Self-Invertible Matrix on Cipher Tetragraphic Trifunction. In *AIP Proceeding SKSM25*; Persatuan Sains Matematik Malaysia; AIP Publishing: Melville, NY, USA, 2016.
8. Reddy, L.S. A New Modal of Hill Cipher Using Non–Quadratic Residues. *Int. J. Soft Comput. Eng.* **2012**, *10*, 73–74.
9. Acharya, B.; Rath, G.S.; Patra, S.K.; Panigrahy, S.K. Novel Methods of Generating Self-invertible Matrix for Hill Cipher Algorithm. *Int. J. Secur.* **2007**, *1*, 14–21.
10. Rosen, K.H. *Elementary Number Theory and Its Applications (Six Edition)*; Addison-Wesley: Boston, MA, USA, 1987; pp. 224–230.
11. Kahn, D. *The Codebreakers. The Story of Secret Writing*; The Macmillan Company: London, UK, 1967; p. 404.
12. Smith, P. LUC Public Key Encryption: A Secure Alternative to RSA. *Dr. Dobb'S J.* **1993**, *18*, 44–48.
13. Mahapatra, A.; Dash, R. Data Encryption and Decryption by Using Hill Cipher Technique and Self Repetitive Matrix. Bachelor's Thesis, National Institute of Technology, Rourkela, India, 2007.
14. Hamamreh, R.A.; Farajallah, M. Design of a Robust Cryptosystem Algorithm for Non-Invertible Matrices Based on Hill Cipher. *Int. J. Comput. Sci. Netw. Secur.* **2009**, *9*, 11–16.
15. Shinge, S.R.; Patil, R. An Encryption Algorithm Based on ASCII Value of Data. *Int. J. Comput. Sci. Inf. Technol.* **2014**, *5*, 7232–7234.