Novel Methods of Generating Self-Invertible Matrix for Hill Cipher Algorithm

Bibhudendra Acharya bibhudendra@gmail.com
Department of Electronics & Communication Engineering
National Institute of Technology Rourkela
Rourkela, 769 008, India

Girija Sankar Rath gsrath@nitrkl.ac.in
Professor, Department of Electronics & Communication Engineering
National Institute of Technology Rourkela
Rourkela, 769 008, India

Sarat Kumar Patra skpatra@nitrkl.ac.in
Professor, Department of Electronics & Communication Engineering
National Institute of Technology Rourkela
Rourkela, 769 008, India

Saroj Kumar Panigrahy skp.nitrkl@gmail.com
Department of Computer Science & Engineering
National Institute of Technology Rourkela
Rourkela, 769 008, India

Abstract

In this paper, methods of generating self-invertible matrix for Hill Cipher algorithm have been proposed. The inverse of the matrix used for encrypting the plaintext does not always exist. So, if the matrix is not invertible, the encrypted text cannot be decrypted. In the self-invertible matrix generation method, the matrix used for the encryption is itself self-invertible. So, at the time of decryption, we need not to find inverse of the matrix. Moreover, this method eliminates the computational complexity involved in finding inverse of the matrix while decryption.

Keywords: Hill Cipher, Encryption, Decryption, Self-invertible matrix.

1. INTRODUCTION

Today, in the information age, the need to protect communications from prying eyes is greater than ever before. Cryptography, the science of encryption, plays a central role in mobile phone communications, pay-TV, e-commerce, sending private emails, transmitting financial information, security of ATM cards, computer passwords, electronic commerce and touches on many aspects of our daily lives [1]. Cryptography is the art or science encompassing the principles and methods of transforming an intelligible message (plaintext) into one that is unintelligible (ciphertext) and then retransforming that message back to its original form. In modern times, cryptography is considered to be a branch of both mathematics and computer science, and is affiliated closely with information theory, computer security, and engineering [2].

Conventional Encryption is referred to as symmetric encryption or single key encryption. It can be further divided into categories of classical techniques and modern techniques. The hallmark of conventional encryption is that the cipher or key to the algorithm is shared, i.e., known by the parties involved in the secured communication. Substitution cipher is one of the basic components of classical ciphers. A substitution cipher is a method of encryption by which units of plaintext are substituted with ciphertext according to a regular system; the units may be single letters (the most common), pairs of letters, triplets of letters, mixtures of the above, and so forth. The receiver deciphers the text by performing an inverse substitution [3]. The units of the plaintext are retained in the same sequence as in the ciphertext, but the units themselves are altered. There are a number of different types of substitution cipher. If the cipher operates on single letters, it is termed a simple substitution cipher; a cipher that operates on larger groups of letters is termed polygraphic. A monoalphabetic cipher uses fixed substitution over the entire message, whereas a polyalphabetic cipher uses a number of substitutions at different times in the message— such as with homophones, where a unit from the plaintext is mapped to one of several possibilities in the ciphertext. Hill cipher is a type of monoalphabetic polygraphic substitution cipher.

In this paper, we proposed novel methods of generating self-invertible matrix which can be used in Hill cipher algorithm. The objective of this paper is to overcome the drawback of using a random key matrix in Hill cipher algorithm for encryption, where we may not be able to decrypt the encrypted message, if the matrix is not invertible. Also the computational complexity can be reduced by avoiding the process of finding inverse of the matrix at the time of decryption, as we use self-invertible key matrix for encryption.

The organization of the paper is as follows. Following the introduction, the basic concept of Hill Cipher is outlined in section 2. Section 3 discusses about the modular arithmetic. In section 4, proposed methods for generating self-invertible matrices are presented. Finally, section 5 describes the concluding remarks.

2. HILL CIPHER

It is developed by the mathematician Lester Hill in 1929. The core of Hill cipher is matrix manipulations. For encryption, algorithm takes m successive plaintext letters and instead of that substitutes m cipher letters. In Hill cipher, each character is assigned a numerical value like $a = 0, b = 1, \ldots, z = 25$ [4]. The substitution of ciphertext letters in the place of plaintext letters leads to m linear equation. For $m = 3$, the system can be described as follows:

$$\begin{aligned} C_1 &= (K_{11}P_1 + K_{12}P_2 + K_{13}P_3) \bmod 26 \\ C_2 &= (K_{21}P_1 + K_{22}P_2 + K_{23}P_3) \bmod 26 \\ C_1 &= (K_{31}P_1 + K_{32}P_2 + K_{33}P_3) \bmod 26 \end{aligned} \quad \ldots (1)$$

This case can be expressed in terms of column vectors and matrices:

$$\begin{pmatrix} C_1 \\ C_2 \\ C_3 \end{pmatrix} = \begin{bmatrix} K_{11} & K_{12} & K_{13} \\ K_{21} & K_{22} & K_{23} \\ K_{31} & K_{32} & K_{33} \end{bmatrix} \begin{pmatrix} P_1 \\ P_2 \\ P_3 \end{pmatrix} \quad \ldots (2)$$

or simply we can write as $C = KP$, where C and P are column vectors of length 3, representing the plaintext and ciphertext respectively, and K is a 3×3 matrix, which is the encryption key. All operations are performed $\bmod 26$ here. Decryption requires using the inverse of the matrix K. The inverse matrix K^{-1} of a matrix K is defined by the equation $KK^{-1} = K^{-1}K = I$, where I is the Identity matrix. But the inverse of the matrix does not always exist, and when it does, it satisfies the preceding equation. K^{-1} is applied to the ciphertext, and then the plaintext is recovered. In general term we can write as follows:

For encryption: $C = E_k(P) = K_p$ … (3)

For decryption: $P = D_k(C) = K^{-1}C = K^{-1}K_p = P$ … (4)

3. MODULAR ARITHMETIC

The arithmetic operation presented here are addition, subtraction, unary operation, multiplication and division [5]. Based on this, the self-invertible matrix for Hill cipher algorithm is generated. The congruence modulo operator has the following properties:

1. $a \equiv b \mod p$ if $n \mid (a-b)$
2. $(a \mod p) = (b \mod p) \Rightarrow a \equiv b \mod p$
3. $a \equiv b \mod p \Rightarrow b \equiv a \mod p$
4. $a \equiv b \mod p$ and $b \equiv a \mod p \Rightarrow a \equiv c \mod p$

Let $Z_p = [0,1,..., p-a]$ the set of residues modulo p. If modular arithmetic is performed within this set Z_p, the following equations present the arithmetic operations:

1. Addition : $(a+b) \bmod p = [(a \bmod p) + (b \bmod p)] \bmod p$
2. Negation : $-a \bmod p = p - (a \bmod p)$
3. Subtraction : $(a-b) \bmod p = [(a \bmod p) - (b \bmod p)] \bmod p$
4. Multiplication : $(a*b) \bmod p = [(a \bmod p) * (b \bmod p)] \bmod p$
5. Division : $(a/b) \bmod p = c$ when $a = (b*c) \bmod p$

The following Table exhibits the properties of modular arithmetic.

Property	Expression
Commutative Law	$(\omega + x) \bmod p = (x + \omega) \bmod p$ $(\omega * x) \bmod p = (x * \omega) \bmod p$
Associative law	$[(\omega + x) + y] \bmod p = [\omega + (x + y)] \bmod p$
Distribution Law	$[\omega * (x + y)] \bmod p = [\{(\omega * x) \bmod p\} * \{(\omega * y) \bmod p\}] \bmod p$
Identities	$(0 + a) \bmod p = a \bmod p$ $and\ (1 * a) \bmod p = a \bmod p$
Inverses	For each $x \in Z_p$, $\exists\ y$ such that $(x + y) \bmod p = 0$ then $y = -x$ For each $x \in Z_p$ $\exists\ y$ such that $(x * y) \bmod p = 1$

Table 1: Properties of Modular Arithmetic

4. PROPOSED METHODS FOR GENERATING SELF-INVERTIBLE MATRIX

As Hill cipher decryption requires inverse of the matrix, so while decryption one problem arises that is, inverse of the matrix does not always exist [5]. If the matrix is not invertible, then encrypted text cannot be decrypted. In order to overcome this problem, we suggest the use of self-invertible matrix generation method while encryption in the Hill Cipher. In the self-invertible matrix generation method, the matrix used for the encryption is itself self-invertible. So, at the time of decryption, we need not to find inverse of the matrix. Moreover, this method eliminates the computational complexity involved in finding inverse of the matrix while decryption.

A is called self-invertible matrix if $A = A^{-1}$. The analyses presented here for generation of self-invertible matrix are valid for matrix of +ve integers, that are the residues of modulo arithmetic on a prime number.

4.1 Generation of self-invertible 2×2 matrix

Let $A=\begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$, then, $A^{-1}=\dfrac{\text{adjoint}(A)}{\text{determinant}(A)}=\dfrac{(\text{cofactor}(A))^T}{\text{determinant}(A)}$

$\therefore A^{-1}=\dfrac{1}{\Delta a}\begin{bmatrix} a_{22} & -a_{12} \\ -a_{21} & a_{11} \end{bmatrix}$, where, Δa is the $\text{determinant}(A)$

A is said to be self-invertible if $A=A^{-1}$

So, $a_{12}=-a_{12}/\Delta a$ & $a_{21}=-a_{21}/\Delta a$

$\therefore \Delta a=-1$ and $a_{11}=-a_{22} \Rightarrow a_{11}+a_{22}=0$ … (5)

Example: (For modulo 13)

$A=\begin{bmatrix} 2 & 3 \\ 12 & 11 \end{bmatrix}$

4.2 Generation of self-invertible 3×3 matrix

Let $A=\left[\begin{array}{c:cc} a_{11} & a_{12} & a_{13} \\ \hdashline a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{array}\right]=\left[\begin{array}{c:c} A_{11} & A_{12} \\ \hdashline A_{21} & A_{22} \end{array}\right]$

where A_{11} is a 1×1 matrix = $[a_{11}]$, A_{12} is a 1×2 matrix = $[a_{12} \quad a_{13}]$,

A_{21} is a 2×1 matrix = $\begin{bmatrix} a_{21} \\ a_{31} \end{bmatrix}$ and A_{22} is 2×2 matrix = $\begin{bmatrix} a_{22} & a_{23} \\ a_{32} & a_{33} \end{bmatrix}$

If A is self-invertible then,

$A_{11}{}^2+A_{12}A_{21}=I, \quad A_{11}A_{12}+A_{12}A_{22}=0,$

$A_{21}A_{11}+A_{22}A_{21}=0, \quad$ and $A_{21}A_{12}+A_{22}^2=I$ … (6)

Since A_{11} is 1×1 matrix = $[a_{11}]$ and $A_{21}(a_{11}I+A_{22})=0$

For non- trivial solution, it is necessary that $a_{11}I+A_{22}=0$

That is $a_{11}=-$ (one of the Eigen values of A_{22})

$A_{21}A_{12}$ can also be written as

$A_{21}A_{12}=\begin{bmatrix} a_{21} & 0 \\ a_{31} & 0 \end{bmatrix}\begin{bmatrix} a_{12} & a_{13} \\ 0 & 0 \end{bmatrix}=\begin{bmatrix} a_{21}a_{12} & a_{21}a_{13} \\ a_{31}a_{12} & a_{31}a_{13} \end{bmatrix}$

So $A_{21}\ A_{12}$ is singular and

$A_{21}A_{12}=I-A_{22}^2$ … (7)

Hence A_{22} must have an Eigen value ± 1. It can be shown that $Trace[A_{21}A_{12}]=A_{12}A_{21}$.

Since it can be proved that if $A_{11}=a_{11}=-$ (one of the Eigen values of A_{22}),

then, any non-trivial solution of the equation (7) will also satisfy

$A_{12}A_{21}=1-a_{11}{}^2$ … (8)

Example: (For modulo 13)

Take $A_{22}=\begin{bmatrix} 2 & 5 \\ 1 & 6 \end{bmatrix}$ which has Eigen value $\lambda=1$ and 7

$a_{11}=-7=6$ or $-1=12$

If $a_{11}=6$,

then, $A_{21}A_{12}=I-A_{22}^2=I-\begin{bmatrix} 2 & 5 \\ 1 & 6 \end{bmatrix}\begin{bmatrix} 2 & 5 \\ 1 & 6 \end{bmatrix}=I-\begin{bmatrix} 9 & 1 \\ 8 & 2 \end{bmatrix}=\begin{bmatrix} 5 & 12 \\ 5 & 12 \end{bmatrix}$

$a_{21}a_{12}=5$. So, $a_{21}=5$ and $a_{12}=1$

$a_{21}a_{13}=12$. So, $a_{13}=\frac{12}{5}=5$ and $a_{31}=\frac{5}{1}=5$

So the matrix will be $A=\begin{bmatrix}6 & 1 & 5\\ 5 & 2 & 5\\ 5 & 1 & 6\end{bmatrix}$. Other matrix can also be obtained if we take $a_{11}=12$.

4.3 Generation of self-invertible 4×4 matrix

Let $A=\left[\begin{array}{cc:cc} a_{11} & a_{12} & a_{13} & a_{14}\\ a_{21} & a_{22} & a_{23} & a_{24}\\ \hdashline a_{31} & a_{32} & a_{33} & a_{34}\\ a_{41} & a_{42} & a_{43} & a_{44}\end{array}\right]$ be self-invertible matrix partitioned as $A=\left[\begin{array}{c:c} A_{11} & A_{12}\\ \hdashline A_{21} & A_{22}\end{array}\right]$,

where $A_{11}=\begin{bmatrix}a_{11} & a_{12}\\ a_{21} & a_{22}\end{bmatrix}$, $A_{12}=\begin{bmatrix}a_{13} & a_{14}\\ a_{23} & a_{24}\end{bmatrix}$, $A_{21}=\begin{bmatrix}a_{31} & a_{32}\\ a_{41} & a_{42}\end{bmatrix}$, $A_{22}=\begin{bmatrix}a_{33} & a_{34}\\ a_{43} & a_{42}\end{bmatrix}$

Then, $A_{12}A_{21}=I-A_{11}^{\,2}$, $A_{11}A_{12}+A_{12}A_{22}=0$,

$A_{21}A_{11}+A_{22}A_{21}=0$, and $A_{21}A_{12}=I-A_{22}^2$

In order to obtain solution for all the four matrix equations, $A_{12}A_{21}$ can be factorized as

$$A_{12}A_{21}=(I-A_{11})(I+A_{11}) \quad \ldots (9)$$

So, if $A_{12}=(I-A_{11})k$ or $(I+A_{11})k$

$A_{21}=(I+A_{11})\frac{1}{k}$ or $(I-A_{11})\frac{1}{k}$, where k is a scalar constant.

Then, $A_{11}A_{12}+A_{12}A_{22}=A_{11}(I-A_{11})k+(I-A_{11})kA_{22}$ or $k(A_{11}+A_{22})(I-A_{11})$

So, $A_{11}+A_{22}=0 \quad or \quad A_{11}=I$ … (10)

Since $A_{11}=I$ is a trivial solution, then, $A_{11}+A_{22}=0$ is taken.

When we solve the 3rd and 4th matrix equations, same solution is obtained.

Example: (For Modulo 13)

Take $A_{22}=\begin{bmatrix}1 & 3\\ 8 & 4\end{bmatrix}$ then, $A_{11}=\begin{bmatrix}12 & 10\\ 5 & 9\end{bmatrix}$

Take $A_{12}=I-A_{11}$ with $k=1$. Then, $A_{12}=\begin{bmatrix}2 & 3\\ 8 & 5\end{bmatrix}$ and $A_{21}=\begin{bmatrix}0 & 10\\ 5 & 10\end{bmatrix}$

So $A=\begin{bmatrix}12 & 10 & 2 & 3\\ 5 & 9 & 8 & 5\\ 0 & 10 & 1 & 3\\ 5 & 10 & 8 & 4\end{bmatrix}$

4.4 A general method of generating an even self-invertible matrix

Let $A=\left[\begin{array}{ccc:cc} a_{11} & a_{12} & \ldots & \ldots & a_{1n}\\ a_{21} & a_{22} & \ldots & \ldots & a_{2n}\\ \ldots & \ldots & \ldots & \ldots & \ldots\\ \hdashline \ldots & \ldots & \ldots & \ldots & \ldots\\ a_{n1} & a_{n2} & \ldots & \ldots & a_{nn}\end{array}\right]$ be an $n\times n$ self-invertible matrix partitioned to $A=\left[\begin{array}{c:c} A_{11} & A_{12}\\ \hdashline A_{21} & A_{22}\end{array}\right]$,

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

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

If A_{12} is one of the factors of $I - A_{11}^2$ then A_{21} is the other.
Solving the 2nd matrix equation results $A_{11} + A_{22} = 0$.
Then form the matrix.

Algorithm:

1. Select any arbitrary $\frac{n}{2} \times \frac{n}{2}$ matrix A_{22}.
2. Obtain $A_{11} = -A_{22}$
3. Take $A_{12} = k(I - A_{11})$ or $k\ (I + A_{11})$ for k a scalar constant.
4. Then $A_{21} = \frac{1}{k}(I + A_{11})$ or $\frac{1}{k}(I - A_{11})$
5. Form the matrix completely.

Example: (For modulo 13)
Let $A_{22} = \begin{bmatrix} 10 & 2 \\ 3 & 4 \end{bmatrix}$, then, $A_{11} = \begin{bmatrix} 3 & 11 \\ 10 & 9 \end{bmatrix}$
If k is selected as 2, $A_{12} = k(I - A_{11}) = \begin{bmatrix} 9 & 4 \\ 6 & 10 \end{bmatrix}$ and $A_{21} = \begin{bmatrix} 2 & 12 \\ 5 & 5 \end{bmatrix}$
So, $A = \begin{bmatrix} 3 & 11 & 9 & 4 \\ 10 & 9 & 6 & 10 \\ 2 & 12 & 10 & 2 \\ 5 & 5 & 3 & 4 \end{bmatrix}$

4.5 A general method of generating self-invertible matrix

Let $A = \left[\begin{array}{c:ccc} a_{11} & a_{12} & \dots & a_{1n} \\ \hdashline a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{array}\right]$ be an $n \times n$ self-invertible matrix partitioned to $A = \left[\begin{array}{c:c} A_{11} & A_{12} \\ \hdashline A_{21} & A_{22} \end{array}\right]$

A_{11} is a 1×1 matrix = $[a_{11}]$, A_{12} is a $1 \times (n-1)$ matrix = $[a_{12} \quad a_{13} \dots \quad a_{1n}]$

A_{21} is a $(n-1) \times 1$ matrix = $\begin{bmatrix} a_{21} \\ a_{31} \\ \dots \\ a_{n1} \end{bmatrix}$, A_{22} is a $(n-1) \times (n-1)$ matrix = $\begin{bmatrix} a_{22} & a_{23} & \dots & a_{2n} \\ a_{32} & a_{33} & \dots & a_{3n} \\ \dots & \dots & \dots & \dots \\ a_{n2} & a_{n3} & \dots & a_{nn} \end{bmatrix}$

So, $A_{12}\ A_{21} = I - {A_{11}}^2 = 1 - {a_{11}}^2$ … (12)
and $A_{12}(a_{11}I + A_{22}) = 0$ … (13)
Also, $a_{11} =$ – (one of the Eigen values of A_{22} other than 1)
Since $A_{21}A_{12}$ is a singular matrix having the rank 1
and $A_{21}A_{12} = I - A_{22}^2$ … (14)
So, ${A_{22}}^2$ must have rank of $(n-2)$ with Eigen values +1 of $(n-2)$ multiplicity.
Therefore, A_{22} must have Eigen values ± 1.
It can also be proved that the consistent solution obtained for elements A_{21} & A_{12} by solving the equation (14) term by term will also satisfy the equation (12).

Algorithm:

1. Select A_{22}, a non-singular $(n-1)\times(n-1)$ matrix which has $(n-2)$ number of Eigen values of either +1 or –1 or both.
2. Determine the other Eigen value λ of A_{22}.
3. Set $a_{11} = -\lambda$.
4. Obtain the consistent solution of all elements of A_{21} & A_{12} by using the equation (14).
5. Formulate the matrix.

Example: (For modulo 13)

Let $A_{22} = \begin{bmatrix} 9 & 6 & 10 \\ 12 & 10 & 2 \\ 5 & 3 & 4 \end{bmatrix}$ which has Eigen values $\lambda = \pm 1,\ 10$

So, $A_{11} = [3]$, and one of the consistent solutions of $A_{12} = [11 \quad 9 \quad 4]$ and $A_{21} = \begin{bmatrix} 10 \\ 2 \\ 5 \end{bmatrix}$

So, $A = \begin{bmatrix} 3 & 11 & 9 & 4 \\ 10 & 9 & 6 & 10 \\ 2 & 12 & 10 & 2 \\ 5 & 5 & 3 & 4 \end{bmatrix}$

Another consistent solution of $A_{12} = [1 \quad 2 \quad 11]$ and $A_{21} = \begin{bmatrix} 6 \\ 9 \\ 3 \end{bmatrix}$

So, $A = \begin{bmatrix} 3 & 1 & 2 & 11 \\ 6 & 9 & 6 & 10 \\ 9 & 12 & 10 & 2 \\ 3 & 5 & 3 & 4 \end{bmatrix}$

4.6 Another method to generate self-invertible matrix

Let A be any non-singular matrix and E be its Eigen matrix. Then we know that $AE = E\lambda$, where λ is diagonal matrix with the Eigen values as diagonal elements. E the Eigen matrix is non-singular.

Then, $A = E\ \lambda E^{-1}$ … (15)

and $A^{-1} = \left(E\lambda E^{-1}\right)^{-1} = E^{-1}\ \lambda^{-1} E = E\lambda^{-1}E^{-1}$ … (16)

So, $A = A^{-1}$ only when $\lambda = \lambda^{-1}$

If $\lambda = \begin{bmatrix} \lambda_1 & 0 & 0 & 0 & . & . & 0 \\ 0 & \lambda_2 & 0 & 0 & . & . & 0 \\ . & . & . & . & . & . & . \\ . & . & . & . & . & . & . \\ 0 & 0 & 0 & 0 & . & . & \lambda_n \end{bmatrix}$ then, $\lambda^{-1} = \begin{bmatrix} \frac{1}{\lambda_1} & 0 & 0 & . & . & . & 0 \\ 0 & \frac{1}{\lambda_2} & 0 & 0 & . & . & 0 \\ . & . & . & . & . & . & . \\ . & . & . & . & . & . & . \\ 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{\lambda_n} \end{bmatrix}$

Thus $\lambda = \lambda^{-1}$ when $\lambda_i = \frac{1}{\lambda_i}$ or $\lambda_i = \pm 1$

Algorithm:

1. Select any nonsingular matrix E .
2. Form a diagonal matrix λ with $\lambda = \pm 1$ but all value of λ must not be equal.
3. Then compute $E\lambda E^{-1} = A$.

Example: (For modulo 13)

$$E = \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 8 \end{bmatrix}, \quad E^{-1} = \begin{bmatrix} -\frac{8}{3} & \frac{8}{3} & -1 \\ \frac{10}{3} & \frac{13}{3} & 2 \\ -1 & 2 & -1 \end{bmatrix} = \begin{bmatrix} 6 & 7 & 12 \\ 12 & 0 & 2 \\ 12 & 2 & 12 \end{bmatrix}$$

Take $\lambda = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 12 & 0 \\ 0 & 0 & 1 \end{bmatrix}$

$$A = E\ \lambda\ E^{-1} = \begin{bmatrix} 1 & 11 & 3 \\ 4 & 8 & 6 \\ 7 & 5 & 8 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 12 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 6 & 7 & 12 \\ 12 & 0 & 2 \\ 12 & 2 & 12 \end{bmatrix} = \begin{bmatrix} 5 & 0 & 5 \\ 10 & 1 & 6 \\ 3 & 0 & 8 \end{bmatrix}$$

5. CONCLUSION

This paper suggests efficient methods for generating self-invertible matrix for Hill Cipher algorithm. These methods encompass less computational complexity as inverse of the matrix is not required while decrypting in Hill Cipher. These proposed methods for generating self-invertible matrix can also be used in other algorithms where matrix inversion is required.

6. REFERENCES

1. Blakley G.R., "*Twenty years of cryptography in the open literature*", Security and Privacy 1999, Proceedings of the IEEE Symposium, 9-12 May 1999
2. Imai H., Hanaoka G., Shikata J., Otsuka A., Nascimento A.C., "*Cyptography with Information Theoretic Security*", Information Theory Workshop, 2002, Proceedings of the IEEE, 20-25 Oct 2002
3. A. J. Menezes, P.C. Van Oorschot, S.A. Van Stone, "*Handbook of Applied Cryptography*", CRC press, 1996
4. W. Stallings, "*Cryptography and Network Security*", 4th edition, Prentice Hall, 2005
5. Bruce Schneir, "*Applied Cryptography*", 2nd edition, John Wiley & Sons, 1996