# Invertible, Involutory and Permutation Matrix Generation Methods for Hill Cipher System

Bibhudendra Acharya†, Debasish Jena*, Sarat Kumar Patra†, and Ganapati Panda†
†*Department of Electronics and Communication Engineering*
**Department of Computer Science & Engineering*
*National Institute of Technology Rourkela, Orissa-769008, India*
*bibhudendra@gmail.com, debasishjena@hotmail.com, {skpatra, gpanda}@nitrkl.ac.in*

## Abstract

*Hill cipher's susceptibility to cryptanalysis has rendered it unusable in practice, it still serves an important pedagogical role in both cryptology and linear algebra. Hill cipher requires inverse of the key matrix while decryption. In fact that not all the matrices have an inverse and therefore they will not be eligible as key matrices in the Hill cipher scheme. Furthermore, due to its linear nature, the basic Hill cipher succumbs to known-plaintext attacks. In order to repair these flaws of the original Hill cipher, in this paper we proposed Invertible, Involutory and Permutation Matrix Generation Methods for Hill Cipher System.*

## 1. Introduction

The history of cryptography can be traced back to the secret communication among people thousands of years ago. With the development of human society and industrial technology, theories and methods of cryptography have changed and improved gradually. In 1949, Shannon published his seminar paper "Communication theory of secrecy systems" [1], which marked the beginning of the modern cryptology.

The motivation for security is significant in the desire for secrecy in military affairs, nondisclosure in industrial or commercial applications and information sharing in modem society. These motivations have become particularly acute when computers or computer networks are used in processing and storing of secret and confidential information and in providing effective sharing of useful information. Data security is the science and study of methods of protecting data in computer and communication system from disclosure to unauthorized users. A cryptosystem provides protection against unauthorized disclosure and modification by the data encryption [2-4].

Cryptosystems are divided into the symmetric (Private Key) cryptosystem and the asymmetric (public key) cryptosystem depending on the key used. The symmetric cryptosystem is efficient but it is disadvantageous in that the key distribution process needs to be completed. On the other hand, the asymmetric cryptosystem is advantageous in that the key distribution process is not necessary because the key used for encryption can be made public by placing it in a public directory. However, it is less efficient than the symmetric cryptosystem as it takes much time for encryption/decryption [5].

The conventional cryptosystems, known as the private key cryptosystems, though not complex as the public key cryptosystems, still play important roles for its simplicity in design. Furthermore, the private key cryptosystems are very suitable for enciphering private files or protecting information transmitted over computer networks [2].

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 [5]. 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

978-0-7695-3516-6/08 $25.00 © 2008 IEEE
DOI 10.1109/ICACC.2009.101

from the plaintext is mapped to one of several possibilities in the ciphertext. Hill cipher is a type of monoalphabetic polygraphic substitution cipher. Hill cipher has several advantages such as disguising letter frequencies of the plaintext, its simplicity because of using matrix multiplication and inversion for enciphering and deciphering, its high speed, and high throughput [6, 7].

The idea of the Hill cipher is a simple matrix transformation. Let us consider an arbitrary plaintext string of length $l$, defined over an alphabet of order $n$. We divide that plaintext into $b$ blocks of length $m$, where $m$ is an arbitrarily chosen positive integer and $b = [l/m]$. It is noticed that if the length $l$ is not a multiple of $m$, the last plaintext block must be padded with $l - bm$ extra characters. Additionally, each character in the alphabet is coded with a unique integer in $\{0, 1, ..., n-1\}$, in other words, all the characters in the alphabet are mapped to the ring $Z_n$.

The $b$ plaintext blocks can be rewritten as an $m \times b$ matrix $P$ over $Z_n$ using the one-to-one mapping between the original alphabet and the ring $Z_n$ explained above. Additionally, an $m \times m$ matrix $K$ with coefficients in $Z_n$ must be chosen as the secret key matrix. According to the above definitions, Hill encryption can be performed by computing

$$C = E_K(P) = KP \bmod n. \quad (1)$$

Similarly, decryption is performed by computing

$$P = D_K(C) = K^{-1}C \bmod n. \quad (2)$$

There might be some complications with the procedure outlined above due to the fact that not all the matrices $K$ have an inverse $K^{-1}$ over $Z_n$. In fact, those matrices $K$ with determinant 0, or with a determinant that has common factors with the modulus $n$, will be singular over $Z_n$, and therefore they will not be eligible as key matrices in the Hill cipher scheme [6, 7, 8]. Furthermore, due to its linear nature, the basic Hill cipher succumbs to known-plaintext attacks. In order to repair these flaws of the original Hill cipher, we proposed Invertible, Involutory and Permutation Matrix Generation Methods for Hill Cipher System.

The rest of this paper is organized as follows. The next section presents proposed Invertible, Involutory and Permutation matrix generation methods. Section 3 describes the concluding remarks.

## 2. Proposed Invertible, Involutory and Permutation Matrix Generation Methods

As described in section 1, Hill cipher requires inverse of the key matrix while decryption. In fact that not all the matrices have an inverse and therefore they will not be eligible as key matrices in the Hill cipher scheme. Furthermore, due to its linear nature, the basic Hill cipher succumbs to known-plaintext attacks. In order to repair these flaws of the original Hill cipher, in this section we proposed Invertible, Involutory and Permutation Matrix Generation Methods for Hill Cipher System [9-12].

### 2.1. Invertible matrix formulation

The matrix generated in invertible matrix formulation scheme is always invertible. So these matrices can be used as a key matrix in Hill cipher scheme. Here we have proposed two invertible matrix formulation methods.

#### 2.1.1. First Method

1. Select a random matrix $A$ of size $m \times m$
2. If it is singular and of rank $m-1$, then select principal-minor of matrix $A$ of $(m-1) \times (m-1)$ size which is non-singular.
3. Then add 1 to the diagonal element which is not included in non-singular.

$$A = \begin{bmatrix} a_{11} & . & . & a_{1m} \\ . & . & . & . \\ . & . & . & . \\ a_{m1} & . & . & a_{mn} \end{bmatrix} \quad (3)$$

If rank of $A$ is $m-1$ then select $A_{ii}$ = Principal minor eliminating $i^{th}$ row and $i^{th}$ column of $A$, such that $\Delta A_{ii} =$ is non-zero then $a_{ii} \leftarrow a_{ii} + 1$

To generate in the above method, If the rank of $A$ is $l$,

- Select non-singular principal-minor ($l \times l$).
- Then add 1 to all the principal diagonal elements

  which are not included in the principal-minor.

Above method has one limitation as one has to determine the rank of the matrix.

### 2.1.2. Second Method

$$A=\begin{bmatrix} a_{11} & . & . & a_{1m} \\ . & . & . & . \\ . & . & . & . \\ a_{m1} & . & . & a_{mn} \end{bmatrix} \quad (4)$$

$a_{11}$ = seed number (generation of random number)

$a_{12}=(a_{11}\times t) \bmod n$, where $t$ is any number prime to $n$

$a_{13}=(a_{12}\times t) \bmod n$

.

.

$a_{21}=(a_{1m}\times t) \bmod n$

Such matrix $A$ has rank one, if Trace $A \bmod n \neq 0$ then $K=A+I$ provided that the eigenvalue of $A$ is not equal to $(n-1)$.

$K$ can be found by adding 1 to any $(m-1)$ diagonal elements. And if Trace of $A \bmod n=0$ then $K=A+aI$, where $a$ = any scalar.

Since the inversion of higher dimensional matrix is time consuming, another method of encryption by introducing involutory key matrix is presented in the next subsection. Where key matrix

$$K=K^{-1} \text{ or } K^2=I \quad (5)$$

## 2.2. Involutory matrix formulation

As Hill cipher decryption requires inverse of the matrix, we suggest the use of involutory matrix generation method for generating the key matrix while encryption with the Hill Cipher [13, 14]. Involutory matrices, which eliminates necessity of matrix inverses for Hill decryptions. This meant that same machinery could be used both for encryption and decryption of massages; no additional hardware would be needed to compute inverses before decrypting. Moreover this algorithm generates the different key matrix for each block encryption instead of keeping the key matrix constant. This increases the secrecy of data. In order to generate different key matrix each time, the encryption algorithm randomly generates the seed number and from this key matrix is generated. Method of generating random involutory matrix is described as follows:

$$\text{Let } A=\begin{bmatrix} b & bt & bt^2 & ... & bt^{m-1} \\ bt^m & bt^{m+1} & bt^{m+2} & ... & bt^{2m-1} \\ ... & ... & ... & ... & ... \\ bt^{m(m-1)} & bt^{m(m+1)} & bt^{m(m+1)} & ... & bt^{m^2-1} \end{bmatrix} \quad (6)$$

Matrix $A$ of size $m\times m$ is generated by a set of random number of modulo $n$ is given by

$$a_{ij}=bt^{m(i-1)+j-1} \bmod n \quad (7)$$

where $b$ is the seed element and $t$ multiplying factor is singular of $rank\ 1$ if $trace\ A \neq 0 \bmod n$ and $rank\ 0$ if $trace\ A=0 \bmod n$.

Proof: It is proved that if $\lambda_i$ is the eigen value of matrix $A(m\times m)$ then the characteristic equation of $A$,

$\lambda_i^m+a_{m-1}\lambda_i^{m-1}+...+a_0=0$ for $i=1,...,m$

Then, $s_m+a_{m-1}s_{m-1}+...+a_1s_1+na_0=0 \quad (8)$

Where, $s_j=\sum_{i=1}^{n}\lambda_i^{j-1}=trace\ \text{of}\ A^j$

After due algebraic manipulation it can be shown that

$$s_1+a_{m-1}=0 \quad (9)$$

$s_2+s_1a_{m-1}+2a_{m-2}=0$

$s_{m-k}+a_{m-1}s_{m-1}+...+(m-k)a_K=0$

. .

. .

$s_{m-1}+a_{m-1}s_{m-2}+...+a_2s_1+(m-1)a_1=0$

and $s_m+a_{m-1}s_{m-1}+...+ma_0=0$

$trace\ \text{of}\ A=b[1+t^{m+1}+t^{2(m+1)}+t^{3(m+1)}+...+t^{(m-1)(m+1)}]$

$=b.g(t)$

where $g(t)=1+t^{m+1}+t^{2(m+1)}+t^{3(m+1)}+...$

The $trace\ \text{of}\ A^2=b^2g^2(t)$

$trace\ \text{of}\ A^j=b^jg^j(t)$

. .

. .

$trace\ \text{of}\ A^m=b^mg^m(t)$

So, $a_{m-1}=-s_1=-g(t) \bmod n$

$a_{m-2}=-\frac{1}{2}[s_2+a_{m-1}s_1]=-\frac{1}{2}[(g(t))^2-(g(t))^2]=0$

$$a_{m-3} = -\frac{1}{3}[s_3 + a_{m-1}s_2 + a_{m-2}s_1]$$

$$= -\frac{1}{3}[(g(t))^3 - g(t)(g(t))^2] = 0$$

$$a_{m-4} = -\frac{1}{4}[s_4 + a_{m-1}s_3 + a_{m-2}s_2 + a_{m-3}s_1]$$

$$= -\frac{1}{4}[(g(t))^4 - g(t)(g(t))^3] = 0 \qquad (10)$$

Similarly $a_1 = 0$ & $a_0 = 0$.

So $\lambda^m - k\lambda^{m-1} = 0$ where $k = bg(t) \bmod n$

Hence the matrix has $(m-1)$ number of eigenvalue of zero and one eigenvalue of $k$.

**2.2.1. Formulation of Matrix**

Let $\left[\begin{array}{c|ccc} a_{11} & a_{12} & \dots & a_{1m} \\ \hline a_{21} & a_{22} & \dots & a_{2m} \\ \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & \dots & a_{mm} \end{array}\right]$ be an $m \times m$ self-invertible matrix partitioned to $\left[\begin{array}{c|c} A_{11} & A_{12} \\ \hline A_{21} & A_{22} \end{array}\right]$.

Where, $A_{11}$ is a $1\times1$ matrix $= [a_{11}]$,

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

$A_{21}$ is a $(m-1)\times1$ matrix $= \begin{bmatrix} a_{21} \\ a_{31} \\ \dots \\ a_{m1} \end{bmatrix}$ & $A_{22}$ is a $(m-1)\times(m-1)$ matrix $= \begin{bmatrix} a_{22} & a_{23} & \dots & a_{2m} \\ a_{32} & a_{33} & \dots & a_{3m} \\ \dots & \dots & \dots & \dots \\ a_{m2} & a_{m3} & \dots & a_{mm} \end{bmatrix}$.

If $A_{22} = A + I$

Then, $A_{22}$ will have eigenvalue 1 of $m-2$ multiplicity and $(m-1)^{th}$ eigenvalue will be $k+1$ where $k = trace$ of $A$.

So, $a_{11} = -(k+1)$, that is $a_{11} = -$(one of the Eigenvalues of $A_{22}$ other than 1) and $A_{21}A_{12} = I - A_{22}^2$ which can have multiple solutions and can be solved.

**2.2.2. Algorithm:**

1. Form the matrix $A$, with the seed number $b$ & multiplying factor $t$.
2. Take $A_{22} = A + I$
3. $A_{22}$ will have eigenvalue 1 of $m-2$ multiplicity and $(m-1)^{th}$ eigenvalue will be $k+1$ where $k = trace$ of $A$.
4. Set $a_{11} = -(k+1)$.
5. Obtain the consistent solution of all elements of $A_{21}$ & $A_{12}$ by using the equation $A_{21}A_{12} = I - A_{22}^2$.
6. Formulate the matrix completely.

**2.2.3. Example: (For modulo 13)**

Take seed number $= b = 13$ & multiplying factor $= t = 7$.

Let $B$ is a $4\times4$ self-invertible matrix.

Then, $A = \begin{bmatrix} 1 & 7 & 10 \\ 5 & 9 & 11 \\ 12 & 6 & 3 \end{bmatrix}$

So, $A_{22} = \begin{bmatrix} 2 & 7 & 10 \\ 5 & 10 & 11 \\ 12 & 6 & 4 \end{bmatrix}$ and eigen values of $A_{22}$ are 1, 1, 3.

So, $A_{11} = -3 = 10 = b_{11}$ and $A_{21}A_{12} = I - A_{22}^2$.

$$I - A_{22}^2 = \begin{bmatrix} 11 & 12 & 6 \\ 5 & 10 & 4 \\ 2 & 1 & 7 \end{bmatrix}$$

Then, $b_{21}b_{12} = 11,\ b_{21}b_{13} = 12, b_{21}b_{14} = 6,$

$b_{31}b_{12} = 5, b_{31}b_{13} = 10, b_{31}b_{14} = 4,$

$b_{41}b_{12} = 2, b_{41}b_{13} = 1, b_{41}b_{14} = 7$

If $b_{21} = 1, b_{12} = 11, b_{13} = 12, b_{14} = 6$, then

($b_{21}$ can be of any value from 1 to 12)

$$b_{31} = \frac{5}{11} = 4 \text{ and } b_{41} = \frac{2}{11} = 12$$

$$\therefore B = \begin{bmatrix} 10 & 11 & 12 & 6 \\ 1 & 2 & 7 & 10 \\ 4 & 5 & 10 & 11 \\ 12 & 12 & 6 & 4 \end{bmatrix}$$

## 2.3. Permutation matrix formulation

This scheme makes use of "random" permutations of columns and rows of a matrix to form a "different" key for each data encryption. Permutation matrix formulation scheme is described as follows:

If a matrix $A$ is involutory, then $PAP$ is also involutory, when $P$ is a permutation matrix.

Proof: $(PAP)^{-1} = P^{-1}A^{-1}P^{-1} = PAP$ (11)

Since $P^{-1} = P$

**2.3.1. Example**

Let $P = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$

$$PAP = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} 10 & 11 & 12 & 6 \\ 1 & 2 & 7 & 10 \\ 4 & 5 & 10 & 11 \\ 12 & 12 & 6 & 4 \end{bmatrix} \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$$

$$= \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} 12 & 6 & 10 & 11 \\ 7 & 10 & 1 & 2 \\ 10 & 11 & 4 & 5 \\ 6 & 4 & 12 & 12 \end{bmatrix} = \begin{bmatrix} 10 & 11 & 4 & 5 \\ 6 & 4 & 12 & 12 \\ 12 & 6 & 10 & 11 \\ 7 & 10 & 1 & 2 \end{bmatrix}$$

If the dimension of matrix is $m \times m$ , then there will be $m!$ number permutation matrix and $m!$ number of involutory matrix can be generated using same element.

## 3. Conclusion

We have presented invertible, involutory and permutation matrix generation methods to overcome the weakness of the Hill cipher. The matrix generated in invertible matrix formulation scheme is always invertible. So these matrices can be used as a key matrix in Hill cipher scheme. Involutory matrices, which eliminates necessity of matrix inverses for Hill decryptions. This meant that same machinery could be used both for encryption and decryption of massages; no additional hardware would be needed to compute inverses before decrypting. As to practical considerations, involutory matrices reduces time requirement for decryption in Hill cipher scheme. Permutation matrix generation method makes use of "random" permutations of columns and rows of a matrix to form a "different" key for each data encryption, thereby significantly increases its resistance to various attacks.

## 4. References


[1] C. E. Shannon, "Communication theory of secrecy systems", *Bell System Technical Journal*, 28 (4), 1949, pp. 656–715.

[2] Denning, D. E., *Cryptography and Data Securily*, Addison-Wesley, Mass., 1982.

[3] Koblitz, N., "A Course in Number Theory and Cryptography", Springer-Verlag, New York, 1987.

[4] Simmons, G. J., "Symmetric and Asymmetric Encryption," *ACM Computing Surveys*, Vol. 11, No. 4, 1979, pp. 304-330.

[5] W. Stallings, *Cryptography and Network Security*, 4th edition, Prent W.ice Hall, 2005.

[6] Overbey, J., Traves, W., and Wojdylo, J., "On the keyspace of the Hill cipher", *Cryptologia*, 29(l), 2005, pp. 59-72.

[7] Saeednia, S., "How to make the Hill cipher secure", *Cryptologia*, 24(4), 2000, pp. 353-360.

[8] Barr T.H., *Invitation to cryptography*, Prentice Hall, 2002.

[9] Bibhudendra Acharya, Girija Sankar Rath, Sarat Kumar Patra, and Saroj Kumar Panigrahy. "Novel Methods of Generating Self-Invertible Matrix for Hill Cipher Algorithm". *International Journal of Security* (CSC Journals). Vol. 1, Issue. (1), pp. 14-21, 2007.

[10] Petersen, K., 2000. Notes on Number Theory and Cryptography. http://www.math.unc.edu/Faculty/petersen/Coding/cr2.pdf

[11] Lerma, M.A., 2005. Modular Arithmetic. http://www.math.northwestern.edu/~mlerma/problem_solving/results/modular_arith.pdf

[12] Bibhudendra Acharya, Sarat Kumar Patra, and Ganapati Panda. "A Novel Cryptosystem Using Matrix Transformation", Proceedings of SPIT-IEEE Colloquium & International Conference, Vol. 4, 2008, pp. 92-95.

[13] Hill, L. S., "Cryptography in an Algebraic Alphabet," *American Mathematical Monthly*, Vol.36, No. 6, 1929, pp. 306-312.

[14] Hill, L. S., "Concerning Certain Linear Transformation Apparatus of Cryptography," *American Mathematical Monthly*, Vol. 38, No. 3, 1931, pp. 135-154.