

Involutory, Permuted and Reiterative Key Matrix Generation Methods for Hill Cipher System

Bibhudendra Acharya¹, Sarat Kumar Patra², and Ganapati Panda²

¹Department of E & TC, NIT Raipur, Chhattisgarh-492010, India
bibhudendra@gmail.com

²Department of ECE, NIT Rourkela, Orissa-769008, India
{skpatra, gpanda}@nitrrkl.ac.in

Abstract—The Hill matrix algorithm is known for being the first purely algebraic cryptographic system and for starting the entire field of algebraic cryptology. 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 Involutory, Permuted and Reiterative key matrix generation method for Hill Cipher system. Involutory matrix generation method solves the key matrix inversion problem. Permuted and Reiterative key matrix generation method enhancement increases the Hill system's security considerably

Index Terms— Encryption, Decryption, Involutory matrix, Permuted matrix, Hill Cipher.

I. INTRODUCTION

Cryptography plays a very important role in military and business applications to maintain the secrecy of messages and to prevent information from tampering and eavesdropping. It is especially true when the computer network is growing at a tremendous speed so that more and more transactions are made via the Internet. This is due to the fact that networks accessibility and communication efficiency have increased dramatically. However, ensuring that the contents of transactions are safely delivered to the actual recipient has become an important issue and it is expected to be more crucial in the near future.

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 decipheres the text by performing an inverse substitution. 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 [1].

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. But the drawback of this algorithm is that 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. Moreover, Hill cipher can be easily broken with a known plaintext attack revealing weak security [2]. In order to repair these flaws of the original Hill cipher, in this paper we proposed involutory, permuted and Reiterative key matrix generation method for Hill Cipher system. Involutory matrix generation method solves the key matrix inversion problem. Permuted and Reiterative key matrix generation method generates different key for each block encryption and this enhancement increases the Hill system's security considerably.

Following the introduction, the basic concept of Hill Cipher is outlined in section II. Section III presents the proposed Involutory, Permuted and Reiterative key matrix generation methods. Finally Section IV describes the concluding remarks.

II. HILL CIPHER

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 $b = \lceil l/m \rceil$. 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 $\{0, 1, \dots, n-1\}$, 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

This research work was carried out at the Department of ECE, NIT Rourkela, Orissa-769008, India.
Corresponding author: bibhudendra@gmail.com

$$C = E_K(P) = KP \text{ mod } n. \tag{1}$$

Similarly, decryption is performed by computing

$$P = D_K(C) = K^{-1}C \text{ mod } n. \tag{2}$$

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]. Furthermore, due to its linear nature, the basic Hill cipher succumbs to known-plaintext attacks [2-4].

III. PROPOSED INVOLUTORY, PERMUTED AND SELF-REITERATIVE MATRIX GENERATION METHODS

As described in section II, 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 Involutory and Permuted and Self-Reiterative key Matrix Generation Methods for Hill Cipher System [3, 5, 6].

A Involutory Matrix Formulation

In this section generation of Involutory matrix by modifying the values of a column and a row excepting the corresponding diagonal element is outlined. We suggest the use of involutory matrix generation method for generating the key matrix while encryption with the Hill Cipher. 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 messages; no additional hardware would be needed to compute inverses before decrypting. Method of generating random involutory matrix is described as follows:

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

matrix partitioned to $A = \begin{bmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{bmatrix}$

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

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, $A_{12} A_{21} = I - A_{11}^2 = 1 - a_{11}^2$ (3)

and $A_{12}(a_{11}I + A_{22}) = 0$ (4)

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 $A_{21}A_{12} = I - A_{22}^2$ (5)

So, A_{22}^2 must have rank of $(n-2)$ with Eigen values $+1$ of $(n-2)$ multiplicity.

Therefore, A_{22} must have $(n-2)$ number of Eigen values of ± 1 .

It can also be proved that the consistent solution obtained for elements A_{21} & A_{12} by solving the equation (5) term by term will also satisfy the equation (3)

Since $A_{21}A_{12} = I - A_{22}^2$

$A_{21} = A_{21} \times k$ (k may be any value 1 to $n-1$)

$A_{12} = A_{12} / k$

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 (5).
5. Since $A_{21}A_{12} = I - A_{22}^2$ then $A_{21} = A_{21} \times k$ (k may be any value 1 to $n-1$) & $A_{12} = A_{12} / k$
6. Finally formulate the matrix.

B Permuted Matrix Formulation

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

Let P_{kl} be a permutation matrix defined as

$$P_{ij} = 1 \text{ for } \begin{cases} i = k, j = 1 \\ \text{or } i = l, j = k \\ \text{or } i = j \text{ but } i \neq k, \text{ or } \neq l \end{cases}$$

$$0 \text{ otherwise}$$

Thus $P_{kl} A P_{kl}$ exchanges k^{th} row with l^{th} row and k^{th} column with l^{th} column.

So k^{th} and l^{th} diagonal elements of original matrix A are exchanged.

Let the diagonal elements of A given by $(a_{11}, a_{22}, \dots, a_{mm})$ be represented by α_1 .

Similarly the matrix with diagonal elements $(a_{11}, a_{22}, \dots, a_m a_m, a_{m-1} a_{m-1})$ is represented by α_2 .

The $\alpha_1 \dots \alpha_{m!}$ number of matrix can be formed by the permutation by permuting the diagonal elements of the original matrix by P corresponding permuted matrix.

Since there shall $m!$ number self-invertible matrix by permutation of the original self-invertible matrix & encryption can be done as

α_{i1} = Key matrix for 1^{st} m characters

α_{i2} = Key matrix of 2^{nd} m characters

⋮

$\alpha_{im!}$ = Key matrix of $m!^{th}$ m characters

Where $i_1, i_2, i_3 \dots$ are the random numbers between 1 to $m!$ which can be generated by modulo $m!+1$.

With i_1 as the seed element and multiplying factor t .

$i_1 = r$

$i_2 = r \times t \text{ mod } m!+1$

⋮

$\alpha_{im!} = i_{m!-1} \times t \text{ mod } m!+1$

C Generation of Reiterative Matrix

In this section generation of a reiterative matrix of exponent n is presented. The reiterative matrix of exponent n is defined as for which $C^n = I$ for the smallest value of n . C is necessarily a non-singular square matrix of value n (the value where the matrix becomes an identity matrix) through the method of brute force may not be the best idea; because the matrix is of dimension greater than 5×5 and with mod index greater than 91, the brute force technique might take very long time and n value may be in the range of millions. Hence, it would be comfortable to know the value of n and then generate a random matrix accordingly. This can be done as algorithm follows:

1. Let A be a diagonal matrix with diagonal elements d_i , $i = 1, 2, \dots, m$ where $d_i \neq d_j$ when $i \neq j$. Then determine

the smallest n_i such that $d_i^{n_i} = 1$. Then calculate $n = LCM(n_1, n_2, \dots, n_m)$

2. Pick up any random invertible square matrix B

3. Generate $C = B^{-1}AB$

4. Then n calculated in the step 1 will be smallest integer such that $C^n = I$

proof:

$$(B^{-1}AB)^2 = B^{-1}AB \cdot B^{-1}AB = B^{-1}A^2B$$

$$\text{Therefore } (B^{-1}AB)^n = B^{-1}A^nB$$

$$\text{Since } A^n = I, (B^{-1}AB)^n = I$$

IV. CONCLUSION

We have presented involutory, permuted and self-reiterative key matrix generation methods to overcome the weakness of the Hill cipher. 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 messages; 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. Permuted matrix and reiterative key generation method generates "different" key for each block of data encryption, thereby significantly increases its resistance to various attacks.

REFERENCES

- [1] W. Stallings, *Cryptography and Network Security*, 4th edition, Prentice Hall, 2005.
- [2] Saeednia, S., "How to make the Hill cipher secure", *Cryptologia*, 24(4), 2000, pp. 353-360.
- [3] 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
- [4] Overbey, J., Traves, W., and Wojdylo, J., "On the keyspace of the Hill cipher", *Cryptologia*, 29(1), 2005, pp. 59-72.
- [5] Koblitz, N., "A Course in Number Theory and Cryptography", Springer-Verlag, New York, 1987.
- [6] Lerma, M.A., 2005. Modular Arithmetic. http://www.math.northwestern.edu/~mlerma/problem_solving/results/modular_arith.pdf