Global Journal of Pure and Applied Mathematics.
ISSN 0973-1768 Volume 11, Number 6 (2015), pp. 4763-4769

http://www.ripublication.com

Robust Cryptosystem using Enhanced Energy Efficient Hill Cipher Algorithm with Involutory Key

Kalaichelvi V., Manimozhi K., Meenakshi P., Poornima M. & Sumathi A.

Assistant Professor, SASTRA University, Kumbakonam

Abstract

In this paper we have proposed an energy efficient cryptosystem using enhanced Hill Cipher algorithm with an involutory key. In Hill Cipher, inverse of the matrix is required at the decryption side. In fact that, not all the matrices have inverse. If the matrix is not invertible, then the cipher text cannot be decrypted. In 2007, Acharya introduced Self Invertible matrix method to overcome that problem. Consequently, many research papers were published based on Self Invertible matrix that can take account of only positive integers and not negative numbers. This paper suggests that the same non singular key matrix can be used at the encryption and decryption end. Consequently at the time of decryption inverse of the key matrix is not essential. The key matrix can include both *positive* and *negative* numbers. Furthermore, this proposed method get rid of the computational complexity concerned in finding the inverse of the matrix while decryption.

Keyword: Hill Cipher, encryption, decryption and non-singular matrix.

1. Introduction

Information security is an important issue. Cryptography, the science of encryption, plays a central role in mobile phone communications, 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. The cryptosystems are divided into two parts, first is the symmetric or private cryptosystem and the other type is the asymmetric or public key cryptosystem. In symmetric cryptosystem, same key is used by both the sender and receiver. Symmetric ciphers use substitution or transposition techniques or mixed of these two techniques, substitution map each plaintext elements into ciphertext elements, while transposition transpose the positions of plaintext elements. There are a number of

different types of substitution cipher. Hill cipher is a type of monoalphabetic polygraphic substitution cipher.

Hill Cipher is one of the most well-known Substitution techniques that can be used to defend information from unauthorized access. Hill Cipher has many advantages in data encryption. First, it is resistant to the frequency letter analysis. It's also very straightforward since it uses matrix multiplication. Finally, it has high speed and high throughput. However, noninvertible key matrix is the main downside problem of Hill Cipher, because few of the matrices have inverse. This means that the encrypted text can't be decrypted. This paper suggests a novel technique in Hill Cipher algorithm to defeat its key problem of noninvertible key matrix. In order to avoid this problem, we suggest to use the same key matrix at both the encryption and decryption side but the matrix should be a non-singular one. So, at the time of decryption, we need not find inverse of the matrix. Furthermore, this technique eradicates the computational complexity involved in finding the inverse of the matrix.

The organization of the paper is as follows. Section 2 discuss about the various research papers related to hill cipher. Basic concepts of Hill Cipher are outlined in section 3. Section 4 discuss about the modular arithmetic. In section 5, proposed methods are presented with examples. Finally, section 6 describes the concluding remarks.

2. Literature review

Hill cipher is a polyalphabetic block cipher algorithm based on linear algebra. Several researches have been done to improve the security of Hill cipher. Some of research papers have been discussed.

Yi-Shiung Yeh[1] presented a new polygraph substitution algorithm based on different bases. Their algorithm uses two coprime base numbers that are securely shared between the participants. The main weakness of this paper is that it is time overwhelming and is not efficient for dealing bulk data. Sadeenia [2] tried to make Hill cipher secure by using dynamic key matrix attained by random permutations of columns and rows of the master key matrix and transfers an encrypted plaintext and encrypted permutation vector to the receiving side. The number of dynamic keys are generated n!, where n refers to the size of the key matrix. Each plaintext is encrypted by a new key matrix that prevents the known-plaintext attack on the plaintext but it is vulnerable to known-plaintext attack on permutation vector, the same vulnerability of original Hill cipher. Lin Ch [3] stated that taking random numbers and using one-way hash function ruins the known-plaintext attack to the Hill cipher but their scheme is susceptible to chosen-cipher text attack. Ismail [5] aimed to improve the security of Hill cipher by introduction of an initial vector that multiplies each row of the current key matrix to construct the corresponding key of each block but it has several intrinsic security problems. Chefranov [6] proposed a modification to [11] that works analogous to Hill cipher permutation method, but it does not transfer permutation vector, instead both sides use a pseudo-random permutation generator, and only the number of the necessary permutation is transferred to the receiver. The number of dynamic keys is the same as [11]. Mohsen Toorani [7] proposed a symmetric

cryptosystem based on affine transformation. It uses one random number and generates other random numbers recursively using HMAC in chain. Ahmed Y Mahmoud [8, 10] proposed a modification to Hill cipher based on Eigen values HCM-EE. The HCM-EE produces dynamic encryption key matrix by exponentiation with the help of Eigen values but it is a time consuming process**.** Mohsen Toorani [11] proposed a symmetric cryptosystem based on affine transformation. It uses one random number and spawns other random numbers recursively using HMAC in chain.

3. Hill Cipher

The Hill cipher algorithm is a polygraphic substitution cipher algorithm based on linear transformation, and is invented by Lester S. Hill in 1929. 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 $a = 0$, $b = 1,...,$ $z = 25$). The substitution of cipher text letters in the place of plaintext letters leads to *m* linear equation.

For $m = 3$, the system can be described as follows:

$$\mathbf{C_1 = (K_{11}P_1+K_{12}P_2+K_{13}P_3) \bmod 26}$$
$$\mathbf{C_2 = (K_{21}P_1+K_{22}P_2+K_{23}P_3) \bmod 26}$$
$$\mathbf{C_3 = (K_{31}P_1+K_{32}P_2+K_{33}P_3) \bmod 26}$$

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

$$\begin{pmatrix} C_1 \\ C_2 \\ C_3 \end{pmatrix} = \begin{pmatrix} K_{11} & K_{12} & K_{13} \\ K_{21} & K_{22} & K_{23} \\ K_{31} & K_{32} & K_{33} \end{pmatrix} \begin{pmatrix} P_1 \\ P_2 \\ P_3 \end{pmatrix} \mod 26$$

or

$$\mathbf{C = KP \bmod 26}$$

Decryption requires the inverse of the matrix K. The inverse matrix K^{-1} of a matrix K is defined by the equation $\mathbf{KK^{-1}=K^{-1}K=I}$, 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. To find K^{-1}, bit of mathematics are used. The important things to know are *determinants of matrices, matrix adjugates and Extended Euclid's algorithm* (to find inverses). K^{-1} is applied to the cipher text, and then the plaintext is recovered.

In general term we can write as follows:

$$\mathbf{P = K^{-1}C \bmod 26}$$

4. Modular Arithmetic

The arithmetic operations are addition, subtraction, unary operation, multiplication and division.

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

5. Proposed Enhanced Hill Cipher Algorithm

In symmetric key cryptosystem, both the sender and receiver will use the same key for encryption and decryption. But, in Hill cipher, a different key (K^{-1}) is used to decrypt the message. So, it is more contradict to symmetric key cryptosystem.

To use the same key in both sides, a method that uses the self invertible matrix has been proposed [7, 10]. In the Self Invertible Matrix method, the same matrix is used at both encryption and decryption side. But, it is suitable only for the matrix with positive integers and not with negative numbers.

To overcome the above said problem, this paper recommends using the same non-singular key matrix at both the encryption and decryption end. The key matrix can contain both positive and negative integers. Inverse matrix is not required at the time of decryption, which eradicates the computational complexity involved in finding the inverse of the matrix.

Encryption:

1. Convert the plaintext character into numerical value.
2. Choose a non singular square key matrix K.
3. Calculate C = KP mod 26 where C & P are column vectors of length n.

$$\begin{pmatrix} C_1 \\ C_2 \\ . \\ . \\ C3 \end{pmatrix} = \begin{pmatrix} K_{11} & K_{12} & K_{13} \\ K_{21} & K_{22} & K_{23} \\ . & & \\ . & & \\ K_{31} & K_{32} & K_{33} \end{pmatrix} \begin{pmatrix} P_1 \\ P_2 \\ . \\ . \\ P_3 \end{pmatrix} \bmod 26$$

where

$\mathbf{C_1 = K_{11}P_1+K_{12}P_2+\ldots. +K_{1n}P_n}$
$\mathbf{C_2 = K_{21}P_1+K_{22}P_2+\ldots. +K_{2n}P_n}$
.
.
$\mathbf{Cn = K_{n1}P_1+K_{n2}P_2+\ldots. +K_{nn}P_n}$

Decryption:

1. Add the column vector C as the $(n+1)^{th}$ column in the key matrix.

$$K^1 = \begin{pmatrix} K_{11} & K_{12} & \ldots\ldots. & K_{1n} & C_1 \\ K_{21} & K_{22} & \ldots\ldots. & K_{2n} & C_2 \\ . & & & & \\ K_{n1} & K_{n2} & \ldots\ldots.. & K_{nn} & C_n \end{pmatrix}$$

Reduce the first n columns of K^1 to Identity matrix using Gauss seidel method for solving simultaneous linear equations.

$$= \begin{pmatrix} 1 & 0 \ldots\ldots . & 0 & C_1^1 \\ 0 & 1 \ldots\ldots\ldots.. & 0 & C_2^1 \\ & . & & \\ & . & & \\ 0 & 1 \ldots\ldots\ldots.. & 0 & C_n^1 \end{pmatrix}$$

that gives the plain text from C_1^1, C_2^1, …C_n^1
Here, $P_1=C_1^1\%26$, $P_2=C_2^1\%26$…. $P_n=C_n^1\%26$

Example:
Encryption:

$$\begin{pmatrix} 3 & -3 & 4 \\ 2 & -3 & 4 \\ 0 & -1 & 1 \end{pmatrix}\begin{pmatrix} 8 \\ 9 \\ 10 \end{pmatrix} \bmod 26 = \begin{pmatrix} 37 \\ 29 \\ 1 \end{pmatrix} \bmod 26 = \begin{pmatrix} 11 \\ 3 \\ 1 \end{pmatrix}$$

Decryption:

$$\begin{pmatrix} 3 & -3 & 4 & 11 \\ 2 & -3 & 4 & 3 \\ 0 & -1 & 1 & 1 \end{pmatrix} \bmod 26$$

$$\begin{pmatrix} 3 & 23 & 4 & 11 \\ 0 & 25 & 10 & 13 \\ 0 & 25 & 1 & 1 \end{pmatrix} \quad R_2=R_2-(2/3)\,R_1$$

$$\begin{pmatrix} 3 & 23 & 4 & 11 \\ 0 & 25 & 10 & 13 \\ 0 & 0 & 17 & 14 \end{pmatrix} \quad R_3=R_3-R_2$$

$$\begin{pmatrix} 3 & 23 & 0 & 23 \\ 0 & 25 & 0 & 17 \\ 0 & 0 & 17 & 14 \end{pmatrix} \quad \begin{matrix} R_1=R_1-4/17R_3 \\ R_2=R_2-10/17R_3 \end{matrix}$$

$$\begin{pmatrix} 3 & 0 & 0 & 24 \\ 0 & 25 & 0 & 17 \\ 0 & 0 & 17 & 14 \end{pmatrix} \quad R_1=R_1-23/25R_2$$

$$\begin{pmatrix} 1 & 0 & 0 & 8 \\ 0 & 1 & 0 & 9 \\ 0 & 0 & 1 & 10 \end{pmatrix} \quad \begin{matrix} R_1=R_1/3 \\ R_2=R_2/25 \\ R_3=R_3/17 \end{matrix}$$

The plaintext characters are P1=8, P2=9 and P3=10

Example 2:

Encryption:

$$\begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \begin{pmatrix} 8 \\ 9 \\ 10 \end{pmatrix} \bmod 26 = \begin{pmatrix} 339 \\ 540 \\ 224 \end{pmatrix} \bmod 26 = \begin{pmatrix} 1 \\ 20 \\ 16 \end{pmatrix}$$

Decryption:

$$\begin{pmatrix} 17 & 17 & 5 & 1 \\ 21 & 18 & 21 & 20 \\ 2 & 2 & 19 & 16 \end{pmatrix}$$

$$\begin{pmatrix} 17 & 17 & 5 & 1 \\ 0 & 23 & 24 & 5 \\ 0 & 0 & 23 & 22 \end{pmatrix} \quad \begin{matrix} R_2=R_2 - 21/17\ R_1 \\ R_3=R_3 - 2/17\ R_1 \end{matrix}$$

$$\begin{pmatrix} 17 & 17 & 0 & 3 \\ 0 & 23 & 0 & 25 \\ 0 & 0 & 23 & 22 \end{pmatrix} \quad \begin{matrix} R_1=R_1 - 5/23\ R_3 \\ R_2=R_2 - 24/23\ R_3 \end{matrix}$$

$$\begin{pmatrix} 17 & 0 & 0 & 6 \\ 0 & 23 & 0 & 25 \\ 0 & 0 & 23 & 22 \end{pmatrix} \quad R_1=R_1 - 17/23\ R_2$$

$$\begin{pmatrix} 1 & 0 & 0 & 8 \\ 0 & 1 & 0 & 9 \\ 0 & 0 & 1 & 10 \end{pmatrix} \quad \begin{matrix} R_1=R_1/17 \\ R2=R_2/23 \\ R3=R_3/23 \end{matrix}$$

The plaintext characters are P1=8, P2=9 and P3=10

6. Conclusion

This paper recommends that the same non-singular key square matrix can be used at both encryption and decryption end. Inverse matrix is not necessary at the decryption end. The key matrix can contain both *positive* and *negative* numbers. Moreover, this proposed method eradicates the computational complexity involved in finding the inverse of the matrix at decryption end.

References

1. Yeh YS, Wu TC, Chang CC, Yang WC. "A New Cryptosystem Using Matrix Transformation". 25th IEEE International Carnahan Conference on Security Technology 1991: 131-138
2. Saeednia S. "How to Make the Hill Cipher Secure", J. Cryptologia 2000; 24 353-360
3. Lin CH, Lee CY, Lee CY. "Comments on Saeednia's improved scheme for the Hill cipher". Journal of the Chinese institute of engineers 2004; 27: 743-746
4. William Stallings Cryptography and Network Security Principles and Practices. Printice Hall, 2006
5. Ismail IA, Amin M, Diab H. "How to repair the Hill cipher". Journal of Zhejiang University-Science A 2006, 7: 2022-2030
6. Chefranov A. G., "Secure Hill Cipher Modification SHC-M" Proc. Of the First International Conference on Security of Information and Network (SIN2007) 7-10 May 2007, Gazimagusa (TRNC) North Cyprus, Elci, A., Ors, B., and Preneel, B (Eds) Trafford Publishing, Canada, 2008: pp 34-37, 2007
7. B Acharya, Saroj kumar, Sarat Kumar, Ganapati Panda, "Novel Methods of Generating Self-Invertible Matrix for Hill Cipher Algorithm" International Journal of Security, Vol. 1, Issue 1,, 2007, pp. 14-21.
8. Mohsen Toorani, Abolfazl Falahati. "A secure variant of the Hill cipher". IEEE 2009. 313-316
9. Y. Mahmoud Ahmed, Alexander G. Chefranov. "Hill Cipher Modification Based on Eigen values HCM-EE". In Proc. Of the First International Conference on Security of Information and Network (SIN2009) Gazimagusa (TRNC), North Cyprus, Elci, A., Orgun, M., and Chefranov, A. (Eds), ACM NewYork, USA, pp. 164-167, 2009.
10. B Acharya, Saroj kumar, Sarat Kumar, Ganapati Panda., "Image Encryption Using Advanced Hill Cipher Algorithm", Int. Journal on Signal and Image Processing, ACEEE, Vol 1, No. 1, 2010
11. Y. Mahmoud Ahmed, Chefranov A. G., " Hill Cipher Modification Based on Pseudo-Random Eigen values HCM-PRE" Submitted to Turkish Journal of Electrical Engineering & Computer Science on 2-03-2010
12. Mohsen Toorani, Abolfazl Falahati. "A Secure Cryptosystem based on Affine Transformation". Journal of Security and Communication Networks 2011. 2:207-215