Proceedings of the 2009 International Conference on Security Management, SAM 2009, July 13-16, 2009, Las Vegas Nevada, USA, 2 Volumes 2009

Self generating multi keys cryptosystem model for non-invertible matrices based on hill cipher Algorithm

Mousa Farajallah
mousa_math@ppu.edu
College of Engineering and Technology
Palestine Polytechnic University,
Palestine

Rushdi Hamamreh
rhamamreh@eng.alquds.edu
Computer Engineering Department
AL-Quds University, Palestine

Abstract

Many cryptosystems were designed to prevent data from unauthorized access, and some are relatively secure but slow. Others are fast but relatively not secure enough. One of the most efficient cryptosystems is Hill Cipher algorithm which is classified as symmetric encryption. In this paper we provide a solution for the problem of non-invertible matrix by modifying the way of dealing with key matrix, and make all matrices; including not invertible ones, usable in modified Hill cipher system. Moreover, it will solve the known of pair plaintext and cipher text problem by generating new key matrix for each encrypted block of plaintext, using SHA-512. Since SHA-512 generates 64 integers we can manipulate these integers to become 128 different integers and use them as an input for the matrix; based on the concept that any acceptable data must not be prime.

1. Introduction

Hill Cipher algorithm is not widely used despite of its linear nature, simplicity and ease of use. Hill Cipher is not widely used since it is easy to know the secret key if pair of plaintext and a cipher text is known [1-3].

In addition, Hill Cipher has a problem of none-invertible matrices; not only the zero determinant Matrices but all none prime determinant matrices relative to modular value. Hence, the unreliability of the system, because of the two previous problems Hill Cipher not widely used [4]. In section four. Through this paper, we try to make Hill Cipher usable for all determinants in our system.

It's important to notice that we have two techniques to overcome all Hill Cipher problems. First solve the problem of none invertible matrices which enables us to use the second method.

The rest of this paper is organized as follows. Section two briefly discusses the difference between symmetric and asymmetric cryptosystem. Section three gives brief introduction about Hill Cipher. Section four introduces disadvantages of Hill Cipher through different examples. Section five explains the solution for the Hill Cipher main problem none invertible matrices. Section six explains how to create secret key for every encryption to prevent key discovery. We conclude our work in section seven.

2. Symmetric vs. Asymmetric Encryption

Encryption systems are divided into two main categories, symmetric and asymmetric.

Symmetric encryption, also known as secret key or single key, uses the same key that sender uses to encrypt the data and to decrypt it by the

receiver on the other side [5-7]. This system was the only system used earlier to the discovering and developing the public key [7-8]. In symmetric encryption, a safe way of data transfer must be used to move the secret key between the sender and the receiver [9]. Symmetric encryption occurs either by substitution or transposition technique, or by a mixture of both techniques [10].

Symmetric encryption has many advantages over asymmetric in many ways. First, it is faster since it doesn't consume much time in data encryption and decryption. Secondly, it is easier than asymmetric encryption in secret key generation [11-12]. However, it has some disadvantages, for example, key distribution between the sender and the receiver. Thus, symmetric encryption can achieve a good system performance while asymmetric encryption can provide a high level of security [13-14].

Asymmetric encryption is the opposite of symmetric encryption in safety, since it doesn't require the sharing of the secret key between the sender and the receiver. [12, 15]. But asymmetric encryption is slower and very complicated in calculations [14]. Therefore, the nature of the data determines the system of encryption.

3. Hill Cipher

Hill cipher is an application of modular linear algebra to cryptology [1] .Many researches and papers tried to use Hill Cipher algorithm to build a comprehensive cryptosystem, because it has many advantages; it's simple and easy since it uses multiplications of matrices. It's also fast and highly productive; also it is very strong substitution technique against a cipher-only attack [16-17].

However, it has two compound problems. The first one: is that Hill Cipher requires an inverse of each matrix, used in order to decrypt all the matrixes used in the encryption side. And many matrices have no inverse. In case the key remains constant during the encryption process, it will be easy for the hacker to get it; once he gets a pair of plaintext and cipher text [15].

Hill Cipher was invented by Lester S. Hill in 1929 [18-19]. The idea of Hill Cipher is matrices multiplications in which every character or group of characters in the plaintext is substituted by a character or a group of characters in the ciphertext. Each character is assigned to a numerical value [2-5].

To encrypt a block consists of n characters, we need $n \times n$ matrix. During the decryption process, we need the inverse of the matrix. It's important to notice that the inverse of the matrix is calculated depending on modular value of the system (P) [2-5, 20].

The encryption and decryption model are:

$$c = k \times x \bmod p$$

Where c is the cipher text, x is the plaintext, k is the key matrix, and p is the modular value.

$$x = k \times c \bmod p$$

4. Hill Cipher Problems

The first problem of Hill cipher is none invertible matrices; since the encrypted text can't be decrypted [13, 8]. Also when the matrix not invertible, two plaintext vector will be mapped into the same cipher text vector.

A second problem of Hill Cipher is the known-plaintext attack. Due to Hill Cipher linear nature, the cryptosystem can be broken through the known plaintext attack [21-22]. An analyzer knows only two pairs of plaintext-cipher text, and

then the key matrix can be calculated, from the following equations.

$$\begin{bmatrix} p_{11} & p_{21} \\ p_{12} & p_{22} \end{bmatrix} \times \begin{bmatrix} k_{11} & k_{12} \\ k_{21} & k_{22} \end{bmatrix} \bmod 26 = \begin{bmatrix} c_{11} & c_{21} \\ c_{12} & c_{22} \end{bmatrix}$$

5. All Matrices invertible

To make all matrices invertible there are two chooses. First proposed method depend on convert every two characters in encryption side, into three characters in decryption side. At encryption side, the key matrix is used, while at decryption side the normal inverse of key matrix is used. This technique requires some restriction on the maximum value allowed in the key matrix. The second method does not have any restriction on the values of key matrix, but every two characters at the encryption side will convert into four characters in the decryption side.

5.1 First Technique Algorithm

1. Check if the determinant of the key matrix is zero. If so, add identity matrix, else do nothing. Convert the two vector of plaintext into one numerical value.

2. Calculate the three cipher text vectors from the following equations:

$$c_T = k \times (p_1 \times n + p_2)$$

$$c_1 = c_T \mod n$$

$$c_2 = \text{int}(c_T / n) \bmod n$$

$$c_3 = \text{int}(c_T / n^2) \bmod n$$

3. Convert the numerical values into characters.

At the decryption side:

1. Check if the determinant of the key matrix is zero. If so, add identity matrix, else do nothing.

2. Convert the three vectors of cipher text into numerical values.

3. Calculate the two plaintext vectors from the following equations.

$$c_T = c_1 + (n \times (c_2 + (n \times c_3)))$$

$$x = k^{-1} \times c_T$$

$$p_1 = \frac{x}{n}$$

$$p_2 = x \mod n$$

4. Convert the numerical values into characters.

In this method, numerical values of key have small restriction which is discussed in the following section.

5.1.1 Key space of matrix of first technique

Let $k = \begin{bmatrix} k_{11} & k_{12} & \cdots & \cdots & k_{1n} \\ k_{21} & k_{22} & \cdots & \cdots & k_{2n} \\ \vdots & \vdots & & & \vdots \\ \vdots & \vdots & & & \vdots \\ k_{n1} & k_{n2} & \cdots & \cdots & k_{nn} \end{bmatrix}$

$$p_1 = \begin{bmatrix} p_{11} \\ p_{12} \\ \vdots \\ p_{1n} \end{bmatrix}, \quad p_2 = \begin{bmatrix} p_{21} \\ p_{22} \\ \vdots \\ p_{2n} \end{bmatrix}.$$

And the modular value is p.

Assume we have the worst case; in this case the values of plaintext vectors are $p-1$. The problem is to find the values accepted to act as key matrix element. Also assume these elements are also at the worst case scenario; are equal to each other and are equal to y.

$$c_T = k \times (p_1 \times n + p_2)$$

$$c_T = \begin{bmatrix} y & y & \cdots & \cdots & y \\ y & y & \cdots & \cdots & y \\ \vdots & \vdots & & & \vdots \\ \vdots & \vdots & & & \vdots \\ y & y & \cdots & \cdots & y \end{bmatrix} \times \left(\begin{bmatrix} p-1 \\ p-1 \\ \vdots \\ p-1 \end{bmatrix} \times p + \begin{bmatrix} p-1 \\ p-1 \\ \vdots \\ p-1 \end{bmatrix} \right)$$

$$c_T = n \times y \times (p^2 - 1)$$

To use the previous technique, the following equation must hold:

$$c_T < p^3$$

So we can calculate the maximum value of y.

$$n \times y \times \left(p^2 - 1\right) < p^3$$

$$y < \frac{p^3}{n \times \left(p^2 - 1\right)}.$$

5.2. Second Technique Algorithm

The second technique is similar to the first one, except that every two characters from encryption side convert into four characters in the decryption side, but no restriction on the key space values.

At the encryption side the equations are:

$$c_T = k \times \left(p_1 \times n + p_2\right)$$

$$c_1 = c_T \mod n$$

$$c_2 = \text{int}(c_T / n) \mod n$$

$$c_3 = \text{int}(c_T / n^2) \mod n$$

$$c_4 = \text{int}(c_T / n^3)$$

At the decryption side the equations are:

$$c_T = c_1 + (n \times (c_2 + (n \times (c_3 + n \times c_4))))$$

$$x = k^{-1} \times c_T$$

$$p_1 = \frac{x}{n}$$

$$p_2 = x \mod n$$

To change data entry of matrix, we can choose any numbers that make the determinant not prime relative to the modular value, but less than or equal the maximum value y accept.

6. Multi key Generation

Generating new key steps

1. *Send secure 128 bit using secure channel.*
2. *Use this secret key to generate 128 integers using SHA-512, and save the result in array.*
3. *Check if use all elements of the array matrix, then merge the element of array to generate new 128 bit secrete key and call SHA -512 using this new secret key, else use the reset of element to generate the new key matrix.*
4. *Check if the determinant of the key matrix zero, if so, adds the identity matrix.*
5. *If using the first technique develop the following equation*

$$k = k \mod \left(y + 1\right)$$

6. *Repeat steps 3 through 7 for each block(s), if required.*

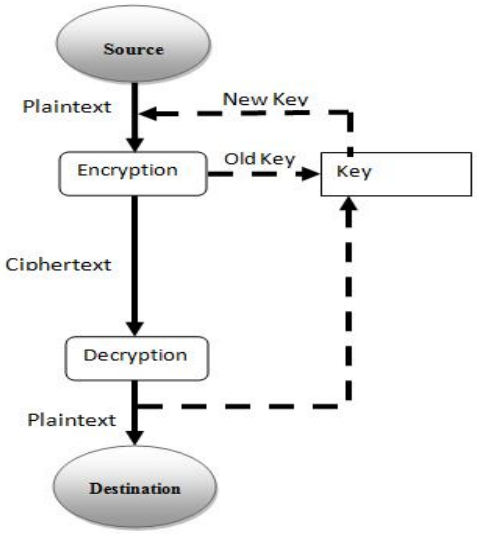

Figure1: Generation multi key algorithm

7. Results and Comparison

We make three comparisons between original Hill cipher, second technique of modified Hill Cipher (MRHC) and AES. Figure 2 is when key matrix size is 2x2 and data of plaintext ranged from 12 KB into 58 KB. Figure 3 is when key matrix size is 4x4. Figure 4 is when key matrix size 9x9. From size 9x9 and up, the MRHC take time more than AES.

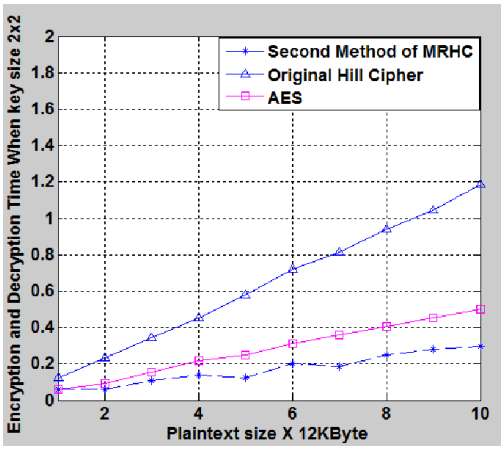

Figure2. time for encryption and decryption when matrix size2x2

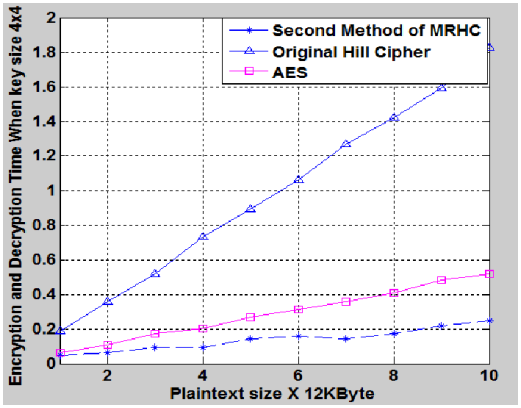

Figure3: time for encryption and decryption when matrix size4x4

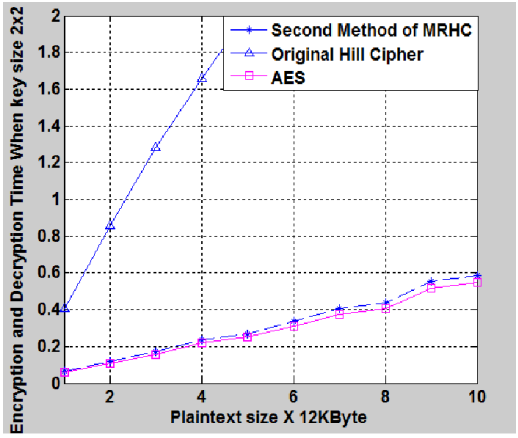

Figure4: time for encryption and decryption when matrix size 9x9

7. Conclusion

This paper introduced a new method to overcome the non-invertible matrices problem in Hill Cipher. Through the introduced solution, it will be possible to overcome the known plaintext attack.

One of the main advantages for our work is the capability of using any matrices as a key to Hill Cipher algorithm including zero determinant matrices. So, there will be no restriction on key selection. The process of generating a new key for every transmitted block of data, makes the algorithm more secure. As generating a new key doesn't have a mathematical inverse method, ; using SHA-512, it's extremely difficult for the hacker to calculate the key.

When using SHA-512 for generating new key matrix, if the key matrix is less than or equal to 8x8, then the modified Hill Cipher MRHC takes less time than AES and for all matrices size less than original Hill Cipher,, otherwise the time on MRHC will increase over AES.

References:

[1] B. N. Tran, T. D. Nguyen, " Modular matrix cipher and its application in authentication protocol", Proceedings of the 2008 Ninth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, August 6 - 8, 2008, Phuket, Thailand, pp. 318-323.

[2] S. K. Panigrahy, B. Acharya, " Image encryption using self-invertible key matrix of Hill cipher algorithm" 1st International Conference on Advances in Computing, February 21-22, 2008, Chikhli, India, pp.1-4.

[3] Y. S. Yeh, T. C. Wu, C. C. Chang, W. C. Yang " A new cryptosystem using matrix transformation", 25th Annual 1991 IEEE International Carnahan Conference on Security Technology. , October1-3, 1991, Taipei , Taiwan, pp. 131-138.

[4] B. Acharya, D. Jena, "Invertible, involuntary and permutation matrix generation methods for Hill cipher system", Proceedings of the 2009 International Conference on Advanced Computer Control, January22-24, 2009, Singapore, Singapore pp. 410-414.

[5] B. Acharya, S. K. Patra, "A novel cryptosystem using matrix transformation", First International Conference on Emerging Trends in Engineering and Technology, July16-18, 2008, Nagpur , Maharashtra, India pp.77-81.

[6] A. D. Gordon, A. Jeffrey, "Types and effects for asymmetric cryptographic protocols", Journal of Computer Security, vol. 12, pp. 435 - 483, May. 2004.

[7] G. J. Simmons, "Symmetric and Asymmetric Encryption" ACM Computing Surveys, vol. 11, pp. 305 - 330, December 1979.

[8] C. Obimbo, B. Salami, "A Parallel Algorithm for determining the inverse of a matrix for use in block cipher encryption/decryption", The Journal of Supercomputing, Springer Netherlands, vol.39, no.2, February 2007.

[9] D. Dzung, M. Crevatin, "Security for Industrial Communication Systems", Proceedings of the IEEE Special Issue on Industrial Communication Systems vol. 93, no.6, June 2005.

[10] Bruce Schneier, "Applied Cryptography", Second Edition, USA, John Wiley & Sons, Inc, 1996.

[11] A. J. Elbirt, C. Paar, " An Instruction-Level Distributed Processor for Symmetric-Key Cryptography ", IEEE Transactions on Parallel and Distributed Systems, vol.16, May 2005.

[12] B. A. Forouzan, "Cryptography and Network Security", First edition, USA, McGraw Hill Higher Education, 2007.

[13] B. Acharya, G. S. Rath, "Novel Modified Hill Cipher Algorithm", International Conference on Emerging Technologies and Applications in Engineering, Technology and Sciences, January 13-14 2008, Rajkot, Gujarat, India, pp126-130.

[14] S. H. Lee, L. Choi "Accelerating Symmetric and Asymmetric Ciphers with Register File Extension for Multi-word and Long-word Operation", Proceedings of the 2008 International Conference on Information Science and Security, January 10-12 2008, Seoul, Korea, pp.102-107.

[15] Ismail I.A, Amin Mohammed, Diab Hossam, " How to repair the Hill cipher", Journal of Zhejiang University SCIENCE A, Zhejiang University Press, co-published with Springer vol.7, no.12, pp.2022-2030, January 2007.

[16] A. S. Hadi, A. H. Mahdi, "Encrypted Block Code", Australian Journal of Basic and Applied Sciences, vol.10, pp.1315-1318, June 2009.

[17] V. U. K. Sastry, N. R. Shankar "Modified Hill Cipher with Interlacing and Iteration", Journal of Computer Science, vol.3, pp.854-859, November 2007.

[18] L. S. Hill, "Cryptography in an algebraic alphabet", The American Mathematical Monthly, vol.36, no.6, pp.306-312, July 1929.

[19] L. S. Hill, "Concerning certain linear transformation apparatus of cryptography", The American Mathematical Monthly, vol.38, no.3, pp.135-154, March 1931.

[20] W. Stallings, "Cryptography and Network Security Principles and Practices", Fourth edition, USA, Prentice Hall, 2006.

[21] C. H. Lin, C. Y. Lee, " Comments On Saeednia's Improved Scheme For The Hill Cipher", Journal of the Chinese Institute of Engineering, vol.27, no.5, pp.743-746, 2004.

[22] Y. R. Romero, R. V. Garcia, "Comments on "How to repair the Hill cipher", Journal of Zhejiang University SCIENCE A, vol.9, no.2, pp.221-214, February 2008.

[23] M. Passing , F. Dressler, " Practical Evaluation of the Performance Impact of Security Mechanisms in Sensor Networks", The 31st Annual IEEE Conference on Local Computer Networks, November 14-16, 2006, Tampa, Florida, USA, pp.623-629.