Available online at www.sciencedirect.com

SciVerse ScienceDirect

Procedia Technology 4 (2012) 114 – 118

Procedia Technology

C3IT-2012

A Modified Hill Cipher Based on Circulant Matrices

Adinarayana Reddy K[a], Vishnuvardhan B[b], Madhuviswanatham[c], Krishna A. V. N.[d]

[a]*Assoc.Prof, Hyderabad Institute of Technology and Management,Gowdavelli,Hyderabad-501401,India*
[b]*Professor, JNTU Jagityal,jagityal,Karimnagar-505327,India*
[c]*Assoc.Prof, VIT University,Vellore-632014,India*
[d]*. Professor, Pujyasri Madhavanji College of Engg.&Tech,Hyderabad-500709,india*

Abstract

Secured communication of text information is prime importance across the globe. Cryptography is one of the methods to attain security. The Hill cipher is a symmetric encryption algorithm vulnerable to the attack of known-plaintext. This paper proposes a modification to the Hill cipher. In the proposed cryptosystem, a prime circulant matrix is shared as a secret key and a non-singular matrix G is used as a public key such that the determinant of coefficient matrix G_c is zero. Which generates infinite solutions. This makes difficulty to find secret key matrix.

Keywords: circulant matrix; decryption; determinant; encryption; hill cipher; permutation; public key

1. Introduction

The Hill cipher algorithm [4, 5] is a polygraphic cipher algorithm based on linear transformation, and is invented by Lester S.Hill in 1929. Hill cipher is a block cipher algorithm where plaintext is divided into equal size blocks. In a Hill cipher, the key is a non-singular matrix of size n x n in which n is the size of the block. The plaintext P is encrypted as C = KP mod m in which C is the cipher text block and K is key matrix. The decryption of cipher text C produces plaintext as P = K^{-1} C mod m such that gcd (det (K) mod m, m) =1. Hill Cipher is no longer used due to the vulnerability against known-plaintext attack. It still serves an important pedagogical role in cryptology and linear algebra. Hill Cipher has resistant towards frequency analysis, high speed and high throughput. A circulant matrix [2] is matrix where each row is rotated one element to the right relative to the preceding row vector. A circulant matrix is used in the Mix Columns step of the Advanced Encryption Standard [11]. This mix column provides diffusion at the bit level. Circulant matrices can be used to improve the efficiency of Lattice-based cryptographic functions. Cryptographic hash function WHIRLPOOL uses circulant matrices. In our paper we focus on Hill cipher and circulant matrix combination. This paper proposes a modification to the Hill cipher based on circulant matrices. The paper is systematised accordingly: Section 2 presents an over view of Hill

2212-0173 © 2012 Published by Elsevier Ltd.
doi:10.1016/j.protcy.2012.05.016

cipher modifications. Section 3 presents a proposed Hill cipher modification. Section 4 explains security analysis. Conclusion of the proposal is in the section 5.

2. Literature Review

Hill cipher [4, 5] is a polyalphabetic block cipher algorithm based on linear algebra. The cipher text block is expressed by

C = KP mod m, where K is key matrix, P is plaintext and C is ciphertext

and the decryption process is expressed by

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

Where the multiplication of matrices are over Z_m. The value of modulus m was 26 in the original Hill cipher but its value can be optionally chosen. Many of square matrices, generally, are not invertible over Z_m. The key space of the Hill cipher is GL (n, Z_m), the group of n x n matrices that are invertible over Z_m. The probability of a randomly selected square matrix to be invertible is about one for any large prime modulus, while it is almost zero for a composite modulus with many different prime divisors, so the risk of determinant having common factors with the modulus can be reduced by taking a prime number as a modulus. Thus, a prime modulus generates large key space than a composite modulus. The Hill cipher security mainly based on confidentiality of the key matrix K and its rank n. The most important vulnerability of Hill cipher is known-plaintext attack.

Several researches have been done to improve the security of Hill cipher. Yi-Shiung Yeh [13] presented a new polygraph substitution algorithm based on different bases. Their algorithm uses two co-prime base numbers that are securely shared between the participants. Although their algorithm thwarts the known-plaintext attack, requires many mathematical manipulations. It is time consuming and is not efficient for dealing bulk data. Sadeenia [11] tried to make Hill cipher secure by using dynamic key matrix obtained 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 numbers of dynamic keys are generated n! where n refers 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. Chefranov [1] proposed a modification to [11] that works similar 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]. Ismail [6] tried to improve the security of Hill cipher by introduction of an initial vector that multiplies each row of the current key matrix to produce the corresponding key of each block but it has several inherent security problems. Lin Ch [7, 8] claimed that taking random numbers and using one-way hash function thwarts the known-plaintext attack to the Hill cipher but their scheme is vulnerable to choosen-ciphertext attack. Mohsen Toorani [9, 10] 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 [14, 15] proposed a modification to Hill cipher based on Eigen values HCM-EE. The HCM-EE generates dynamic encryption key matrix by exponentiation with the help of Eigen values but it is time consuming. In literature circulant matrices has been used in various cryptographic algorithms. Circulant matrices are used in AES and WHIRLPOOL to achieve diffusion. This paper proposes a modification to the Hill cipher based on circulant matrices.

3. Proposed Algorithm

3.1. Basic Concepts

Circulant Matrix: A circulant matrix is a matrix where each row rotates one element to the right relative to the preceding row vector. Thus a circulant matrix can be written as

$$\begin{bmatrix} c_0 & c_1 & c_2 & \cdots & c_{n-1} \\ c_{n-1} & c_0 & c_1 & \cdots & c_{n-2} \\ c_{n-2} & c_{n-1} & c_0 & \cdots & c_{n-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ c_1 & c_2 & c_3 & \cdots & c_0 \end{bmatrix}$$ and is denoted by $\text{circ}(c_0, c_1, c_2, \cdots c_{n-1})$

Prime circulant matrix: An n x n circulant matrix is prime circulant if gcd of row vector is 1. For example the 4 x 4 circulant matrix with row vector (a, b, c, d) is prime circulant if gcd (a, b, c, d) = 1.
Coefficient matrix: Let G be a matrix and the coefficient matrix of G is denoted as G_c and is defined as circ (circ (row 1), circ (row 2) . . . circ (row n)) where row 1, row 2. . . row n are row vectors of matrix G and circ (row i) is the circulant matrix of row i. For example if G is a 2 x 2 matrix then G_c is 4 x 4 matrix

$$G = \begin{bmatrix} g_1 & g_2 \\ g_3 & g_4 \end{bmatrix}$$

$$G_c = \begin{bmatrix} g_1 & g_2 & g_3 & g_4 \\ g_2 & g_1 & g_4 & g_3 \\ g_3 & g_4 & g_1 & g_2 \\ g_4 & g_3 & g_2 & g_1 \end{bmatrix}$$

3.2. Proposed Hill Cipher Algorithm

It proposes modification to Hill cipher based on circulant matrices, where a prime circulant matrix is shared as a secret key and a non-singular matrix G chosen as a public key such that the determinant of coefficient matrix G_c is zero. The algorithm as follows

- Select a n x n non-singular matrix G in GF (P) as a public key such that det (G_c) = 0.
- Select a n x n prime circulant matrix A in GF(P) as a secret key
- Calculate key K = AGA^{-1} mod P
- Encryption:
  - M_i is i^{th} plaintext block of size n
  - C_i is i^{th} cipher text block
  - $C_i = K M_i + V_i^T$ mod P, where V_i is i^{th} row of the prime circulant matrix A
- Decryption:
  - Calculate $K^{-1} = AG^{-1}A^{-1}$ mod P
  - $M_i = K^{-1}(C_i - V_i^T)$ mod P

Here V is the first row of the prime circulant matrix A. For each plaintext block encryption we use a different vector V by rotation. This thwarts known-plaintext attack. It also overcomes the ciphertexr-only attack, since the modulus is a prime number and chosen-plaintext attack. This algorithm is easily implementable. It reduces the key storage requirement from n^2 elements of Z_p to just n elements, because matrix is fully specified by its first row. It also reduces the running time required to compute matrix multiplication. Example is provided in the appendix A**.**

4. Security Analysis

Security of the proposed cryptosystem is based on the difficulty of solving multivariable polynomial equations i.e. $K = AGA^{-1} \bmod P$. This is a NP-hard problem. It is difficult to solve if the modulus is large prime number. After simplification this equation becomes

$$G_c X = Y \bmod P \qquad (1)$$

Where the elements of X are the elements of matrices A and A^{-1} and elements of Y are elements of matrix K. For example A is 2 x 2 prime circulant matrix, G is 2 x 2 non-singular matrix, and then the equation (1) becomes

$$\begin{bmatrix} g_1 & g_2 & g_3 & g_4 \\ g_2 & g_1 & g_4 & g_3 \\ g_3 & g_4 & g_1 & g_2 \\ g_4 & g_3 & g_2 & g_1 \end{bmatrix} \begin{bmatrix} ac \\ ad \\ bc \\ bd \end{bmatrix} = \begin{bmatrix} k_{11} \\ k_{12} \\ k_{21} \\ k_{22} \end{bmatrix}$$

This produces infinite solutions, since the numbers of equations are less than the number of unknowns.

5. Conclusion

This paper presents a symmetric substitution cipher that is actually a secure variant of the Hill cipher. This algorithm uses secret prime circulant matrix key and a public key matrix, such that the determinant of the coefficient matrix is zero. The proposed algorithm has matrix inverse and multiplication as the only operation which does not require any additional operations other than the original Hill cipher. The proposed cryptosystem overcomes the known-plaintext attack, and chosen-plaintext attacks. It also overcomes the ciphertexr-only attack, since the modulus is a prime number.

References

1. 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
2. D. Kalman and J.E. White, “Polynomial equations and circulant matrices”, Amer. Math. Monthly 108 (2001), 821–840.
3. Daniele Micciancio, Oded Regev. “Lattice-based Cryptography”. July 22 2008
4. Hill LS Cryptography in an Algebraic Alphabet. American Mathematical Monthly 1929; 36: 306-312
5. Hill LS Concerning Certain Linear Transformation Apparatus of cryptography. American Mathematical Monthly 1931; 38: 135-154
6. Ismail IA, Amin M, Diab H. “How to repair the Hill cipher”. Journal of Zhejiang University- Science A 2006, 7: 2022-2030
7. 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

8. Li C, Zhang D, Chen G. “Cryptanalysis of an image encryption scheme based on the Hill cipher”. Journal of Zhejiang University - Science A 2008; 9: 1118-1123
9. Mohsen Toorani, Abolfazl Falahati. “A Secure Cryptosystem based on Affine Transformation”. Journal of Security and Communication Networks 2011. 2:207-215
10. Mohsen Toorani, Abolfazl Falahati. “A secure variant of the Hill cipher”. IEEE 2009. 313-316
11. Saeednia S. How to Make the Hill Cipher Secure. Cryptologia Journal 2000; 24: 353-360
12. William Stallings Cryptography and Network Security Principles and Practices. Printice Hall, 2006
13. 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
14. Y.Mahmoud Ahmed, Alexander G. Chefranov. “Hill Cipher Modification Based on Eigenvalues 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.
15. Y. Mahmoud Ahmed, Chefranov A. G., “ Hill Cipher Modification Based on Pseudo-Random Eigenvalues HCM-PRE” Submitted to Turkish Journal of Electrical Engineering & Computer Science on 2-03-2010
16. Y Muhammad Malik, Jong-Seon no. “ Dynamic MDS Matrices for Substantial Cryptographic Strength”

Appendix A. An example

Choose P = 29

Secret key A = $\begin{bmatrix} 3 & 4 \\ 4 & 3 \end{bmatrix}$

Public key G = $\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$ and $\det(G_c) = 0$

Key K = AGA^{-1} **mod P**

$$= \begin{bmatrix} 3 & 4 \\ 4 & 3 \end{bmatrix}\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}\begin{bmatrix} 12 & 13 \\ 13 & 12 \end{bmatrix} \bmod 29 = \begin{bmatrix} 2 & 24 \\ 10 & 3 \end{bmatrix}$$

and Plaintext is M = “AD” and create a vector corresponding to letters (replace ‘A’ with 1, ‘B’ with 2 . etc) to get M = [1, 4]. The ciphertext corresponding to plaintext M is calculated as

$$C = \begin{bmatrix} 2 & 24 \\ 10 & 3 \end{bmatrix}\begin{bmatrix} 1 \\ 4 \end{bmatrix} + \begin{bmatrix} 3 \\ 4 \end{bmatrix} \bmod 29 = \begin{bmatrix} 14 \\ 26 \end{bmatrix}$$

The ciphertext C is “MZ” corresponding to plaintext “AD”.
The plaintext corresponding to ciphertext is calculated as

$M = K^{-1}(C - V^T) \bmod P$

$$M = \begin{bmatrix} 13 & 12 \\ 5 & 28 \end{bmatrix}\left(\begin{bmatrix} 14 \\ 26 \end{bmatrix} - \begin{bmatrix} 3 \\ 4 \end{bmatrix}\right) \bmod 29$$

$$M = \begin{bmatrix} 1 \\ 4 \end{bmatrix}$$

After decryption the plaintext is “AD”.