ISSN: 0975-766X
CODEN: IJPTFI
Available Online through *Research Article*
www.ijptonline.com

SECURE CRYPTOSYSTEM BASED ON NON-DETERMINISTIC LINEAR TRANSFORMATION

Adi Narayana Reddy K*[a], Shyam Chandra Prasad G[b]
[a] Department of CSE, ACE Engineering College, Hyderabad, India.
[b] Department of CSE, Matrusri Engineering College , IS Sadan, Hyderabad.
Email: aadi.iitkgp@gmail.com

Received on 06-08-2016 *Accepted on 10-09-2016*

Abstract

The secure transmission of any form of data over a communication medium is primary important across the globe or in research arena. Cryptography is a branch of cryptology and it provides security for data transmission between any communicating parties. The Hill cipher is one of the symmetric key substitution algorithms. Hill Cipher is vulnerable to known plaintext attack. The randomized cryptosystem based on linear transformation is secure but it produces more cipher text than the plain text. The proposed technique shares a prime circulant matrix as a secret key and reduces the size of the cipher text. The security analysis and performance of the method are studied and presented

Keywords: Circulant Matrix, Probabilistic, Hill Cipher, Sub Key group, Substitution Cipher.

1. Introduction

Today, information is one of the most valuable assets. Information transmission across the network is of prime importance in the present age. Cryptography is the branch of cryptology and it provides security to the transmitted data between the communicating parties. There are various algorithms to provide security for the information. Traditional symmetric ciphers use substitution in which each character is replaced by other character. Lester S. Hill invented the Hill cipher in 1929. Hill cipher is a classical substitution technique that has been developed based on linear transformation. It has both advantages and disadvantages. The main advantages are disguising letter frequencies of the plaintext; high speed, high throughput, and the simplicity because of using matrix multiplication and inversion for enciphering and deciphering. The disadvantages are, it is vulnerable to known plaintext attack and the inverse of the shared key matrix may not exist always. To overcome the drawbacks of Hill cipher algorithm many modifications are presented. In our paper we present a modification to the Hill cipher by the utilization of special matrices called circulant matrices. A circulant matrix is a matrix where each row is rotated one element to the right

relative to the preceding row vector. In literature circulant matrices are used in many of the cryptographic algorithms. Advanced Encryption Standard (AES) uses circulant matrices to provide diffusion at bit level in mix columns step. Circulant matrices can be used to improve the efficiency of Lattice-based cryptographic functions. Cryptographic hash function Whirlpool uses circulant matrices. The paper is systematized accordingly: Section 2 presents an over view of Hill 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 on Hill Cipher Modifications

Many researchers improved the security of linear transformation based cryptosystem. Yeh, Wu et al. [17] presented an algorithm which thwarts the known-plaintext attack, but it is not efficient for dealing bulk data, because too many mathematical calculations. Saeednia [14] presented an improvement to the original Hill cipher, which prevents the known-plaintext attack on encrypted data but it is vulnerable to known-plaintext attack on permutated vector because the permutated vector is encrypted with the original key matrix. Ismail [5] tried a new scheme HillMRIV (Hill Multiplying Rows by Initial Vector) using IV (Initial Vector) but Rangel-Romeror et al. [11] proved that If IV is not chosen carefully, some of the new keys to be generated by the algorithm, may not be invertible over Z_m, this make encryption/decryption process useless and also vulnerable to known-plaintext attack and also proved that it is vulnerable to known-plaintext attack. Lin C.H. et al. [9] improved the security of Hill cipher by using several random numbers. It thwarts the known-plaintext attack but Toorani et al.[15, 16] proved that it is vulnerable to chosen ciphertext attack and he improved the security, which encrypts each block of plaintext using random number and are generated recursively using one-way hash function but Liam Keliher et al [8] proved that it is still vulnerable to chosen plaintext attack . Ahmed Y Mahmoud et al [1, 2, 3] improved the algorithm by using eigen values but it is not efficient because the time complexity is more and too many seeds are exchanged. Reddy, K.A. et al [12, 13] improved the security of the cryptosystem by using circulant matrices but the time complexity is more. Again Kaipa, A.N.R et al [6] improved the security of the algorithm by adding nonlinearity using byte substitution over GF (2^8) and simple substitution using variable length sub key groups. It is efficient but the cryptanalyst can find the length of sub key groups by collecting pair of same ciphertext and plaintext blocks. Again KANReddy et al [7] improved the security of linear transformation based cryptosystem but the size of the cipher text is three times more than the plain text. In this paper a non-deterministic linear transformation algorithm is proposed to improve the disadvantages of the "randomized cryptosystem based on linear transformation" [7].

3. Proposed Cryptosystem

In this paper an attempt is made to propose a non-deterministic encryption algorithm which produces more than one ciphertext for the same plaintext. The following sub sections explain the proposed method.

3.1 Algorithm

Let M be the message to be transmitted. The message is divided into 'm' blocks each of size 'n' where 'm' and 'n' are positive integers and pad the last block if necessary. Let M_i be the i^{th} partitioned block (i = 1, 2, ... m) and size of each M_i is 'n'. Let C_i be ciphertext of the i^{th} block corresponding to the i^{th} of block plaintext. In this paper the non-deterministic is added to the linear transformation based cryptosystem. Choose a prime number 'p'. The following steps illustrate the algorithm.

1. **Step 1: Key Generation.** Select randomly 'n' numbers ($k_1, k_2, \ldots k_n$) such that GCD ($k_1, k_2, \ldots k_n$) = 1. Assume $k_i \in Z_p$. Rotate each row vector relatively right to the preceding row vector to generate a shared key matrix K_{nxn}. The generated key matrix is called prime circulant matrix. Select randomly another vector e =($e_1, e_2, ..e_n$). Choose a secret shared value d such that 1<d<p. Now calculate s as

   $$s=d*e \bmod p$$

   The inverse of the key K and d shared with the receiver.

2. **Step 2: Encryption.** The encryption process encrypts each block of plaintext using the following steps.

   2.1. Initially the transformation is applied as Y = KM mod p.

   2.2. Choose a random value r

   2.3. Compute the cipher text pair

   $$C_1 = r*e \bmod p$$

   $$C_2 = Y^T + r * s \bmod p$$

   Where Y^T is transpose of Y

   2.4. Transmit the cipher text pair (C_1, C_2) to the other end user

3. **Step 4: Decryption.** The encryption process encrypts each block of plaintext using the following steps

   3.1. Compute Y from cipher text pair (C_1 , C_2) and shared value d as

   $$Y = C_2 – d * C_1 \bmod p$$

   3.2. The inverse linear transformation is applied as $M = K^{-1}Y \bmod p$

   3.3. This produces the plaintext corresponding to ciphertext

3.2 Example

Consider a prime number p as 53 and the set of relatively prime numbers as [5, 27, 13]. Generate shared key matrix K_{3x3}. Assume the plaintext block M= [12, 14, 3]. Assume random vector e = [15, 25, 8] and shared random value d = 18. Choose random number r = 36

Compute s as s = d * e mod p = 18 *[15, 25, 8] mod 53 = [5, 26, 38]

Y^T = KM mod p = KM mod 53 = [0, 42, 44]

Compute cipher text pair

C_1 = r * e mod p = 36 * [15, 25, 8] mod 53 = [10, 52, 23]

C_2 = (Y^T+ r * s) mod p = [0, 42, 44] + 36 * [5, 26, 38] mod 53 = [21, 24, 34]

The pair C_1 and C_2 is transmitted to the receiver.

Decryption:

Compute Y^T as Y^T = (C_2 – d * C_1) mod p = [21, 24, 34] – 18 * [10, 52, 23] mod 53 = [0, 42, 44]

Compute inverse linear transformation P = K^{-1} Y mod p = [12, 14, 3]

4. Performance Analysis

The performance analysis is carried out by considering the computational cost and security analysis which are to show the efficiency of the algorithm.

3.1 Computational Cost

The time complexity measures the running time of the algorithm. The time complexity of the proposed algorithm to encrypt and to decrypt the text is O (mn^2) which is shown in the equation (2), where 'm' is number of blocks and 'n' is size of each block, which is same as that of original Hill cipher. In this process T_{Enc} and T_{Dec} denote the running time for encryption and decryption of 'm' block of plaintext respectively.

$$T_{Enc}(m) \cong m(n^2)T_{Mul} + m(n^2)T_{Add} + mnT_{AddV}$$
$$T_{Dec}(m) \cong m(n^2)T_{Mul} + m(n^2)T_{Add} + mnT_{AddV} \quad (1)$$

In which T_{Add}, T_{Mul}, and T_{AddV} are the time complexities for scalar modular addition, multiplication, and addition of vector respectively.

$$T_{Enc}(m) \cong m(n^2)c_1 + m(n^2)c_2 \cong O(mn^2)$$
$$T_{Dec}(m) \cong m(n^2)c_1 + m(n^2)c_2 + mnc_3 \cong O(mn^2) \quad (2)$$

Where c_1,c_2 and c_3 are the time constants for addition, multiplication and index search respectively. The running time

of proposed randomized LTCM and other methods are analysed and presented in the Fig 1. The running time of proposed randomized LTCM method is equal to the linear transformation based cipher. The proposed method is better than other methods.

3.2 Security Analysis

The key matrix and secret value d are shared secretly by the participants. The attacker tries to obtain the key by various attacks but it is difficult because the non-deterministic nature of the algorithm. The sender encrypts the message by a random value which is not shared with the receiver. This makes the algorithm more secure and produces different cipher text block for the same plain text block. The proposed cryptosystem overcomes all the drawbacks of linear transformation based cipher and symmetric key algorithms. This is secure against known-plaintext, chosen-plaintext and chosen-cipher text attacks because one plaintext block is mapped to many cipher text blocks. This is due to the non-deterministic nature of the algorithm. Therefore, the cryptanalyst can no longer encrypt a random plaintext looking for correct cipher text. To illustrate this assume that the cryptanalyst has collected a cipher text C_i and guessed the corresponding plaintext M_i correctly but when he/she encrypt the plaintext block M_i the corresponding cipher text block C_j will be completely different. Now he/she cannot confirm M_i is correct plaintext for the cipher text C_i.

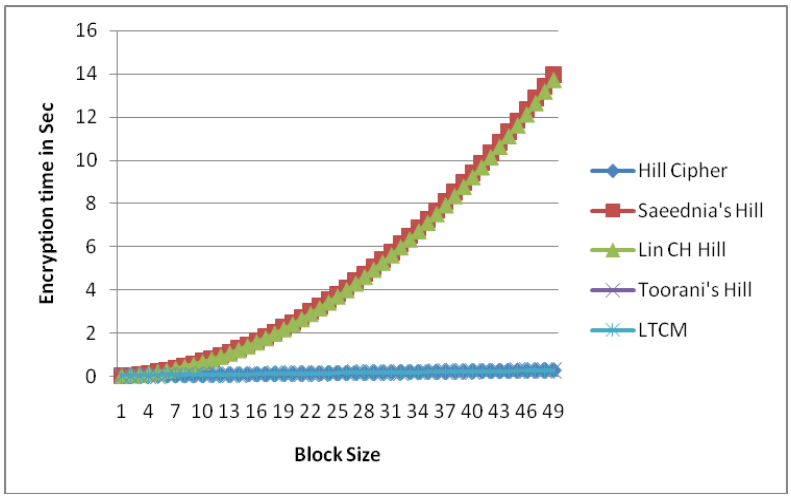

Fig 1 Encryption Time.

5. Conclusion

The structure of the proposed cryptosystem is similar to substitution ciphers i.e. initially the linear transformation is applied on the original plaintext block then a pair of cipher text block is generated using random vectors and a random value. The random value is not shared with the receiver. Without random value the receiver decrypts the

cipher text using key inverse and shared secret value. For every block the sender uses new random value. This makes the algorithm secure against known-plaintext, chosen plaintext and chosen cipher text attacks.

References:

1. Ahmed, Y.M. and A.G. Chefranov, 2009. Hill cipher modification based on eigenvalues hcm-EE. Proceedings of the 2th International Conference on Security of Information and Networks, Oct. 6-10, ACM Press, New York, USA., pp: 164-167. DOI: 10.1145/1626195.1626237
2. Ahmed, Y.M. and Alexander Chefranov, 2011. Hill cipher modification based on pseudo-random eigen values HCM-PRE. Applied Mathematics and Information Sciences (SCI-E) 8(2), pp. 505-516.
3. Ahmed, Y.M. and Alexander Chefranov. Hill cipher modification based generalized permutation matrix SHC-GPM, Information Science letter, 1, pp. 91-102
4. Hill, L.S., 1929. Cryptography in an Algebraic Alphabet. Am. Math. Monthly, 36: 306-312. http://www.jstor.org/discover/10.2307/2298294?uid=3738832&uid=2129&uid=2&uid=70&uid=4&sid=21102878411191
5. Ismail, I.A., M. Amin and H. Diab, 2006. How to repair the hill cipher. J. Zhej. Univ. Sci. A., 7: 2022-2030. DOI: 10.1631/jzus.2006.A2022
6. Kaipa, A.N.R., V.V. Bulusu, R.R. Koduru and D.P. Kavati, 2014. A Hybrid Cryptosystem using Variable Length Sub Key Groups and Byte Substitution. J. Comput. Sci., 10:251-254
7. KAN Reddy, Vishnuvardhan B, Shyam Chandra Prasad G. "Randomized Cryptosystem Based on Linear Transformation", Adavances in Intelligent Systems and Computing , pp 113-119
8. Keliher, L. and A.Z. Delaney, 2013. Cryptanalysis of the toorani-falahati hill ciphers. Mount Allison University. http://eprint.iacr.org/2013/592.pdf
9. Lin, C.H., C.Y. Lee and C.Y. Lee, 2004. Comments on Saeednia's improved scheme for the hill cipher. J. Chin. Instit. Eng., 27: 743-746. DOI: 10.1080/02533839.2004.9670922
10. Overbey, J., W. Traves and J. Wojdylo, 2005. On the keyspace of the hill cipher. Cryptologia, 29: 59-72. DOI: 10.1080/0161-110591893771
11. Rangel-Romeror, Y., R. Vega-Garcia, A. Menchaca-Mendez, D. Acoltzi-Cervantes and L. Martinez-Ramos *et al*., 2008. Comments on "How to repair the Hill cipher". J. Zhej. Univ. Sci. A., 9: 211-214. DOI: 10.1631/jzus.A072143

12. Reddy, K.A., B. Vishnuvardhan, Madhuviswanath and A.V.N. Krishna, 2012. A modified hill cipher based on circulant matrices. Proceedings of the 2nd International Conference on Computer, Communication, Control and Information Technology, Feb. 25-26, Elsevier Ltd., pp: 114-118. DOI: 10.1016/j.protcy.2012.05.016
13. Reddy, K. A., B. Vishnuvardhan, Durgaprasad, 2012. Generalized Affine Transformation Based on Circulant Matrices. Internatonal Journal of Distributed and Parallel Systems, Vol. 3, No. 5, pp. 159-166
14. Saeednia, S., 2000. How to make the hill cipher secure. Cryptologia, 24: 353-360. DOI: 10.1080/01611190008984253
15. Toorani, M. and A. Falahati, 2009. A secure variant of the hill cipher. Proceedings of the IEEE Symposium on Computers and Communications, Jul. 5-8, IEEE Xplore Press, Sousse, pp: 313-316. DOI: 10.1109/ISCC.2009.5202241
16. Toorani, M. and A. Falahati, 2011. A secure cryptosystem based on affine transformation. Sec. Commun. Netw., 4: 207-215. DOI: 10.1002/sec.137
17. Yeh, Y.S., T.C. Wu, C.C. Chang and. W.C. Yang, 1991. A new cryptosystem using matrix transformation. Proceedings of the 25th IEEE International Carnahan Conference on Security Technology, Oct. 1-3, IEEE Xplore Press, Taipei, pp: 131-138. DOI: 10.1109/CCST.1991.202204.

Corresponding Author:
Adi Narayana Reddy K*,
Email: *aadi.iitkgp@gmail.com*