Randomized Cryptosystem Based on Linear Transformation

K. Adi Narayana Reddy, B. Vishnuvardhan and G. Shyama Chandra Prasad

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. This paper presents randomized cryptosystem based on linear transformation using variable length sub key groups. The proposed technique shares a prime circulant matrix as a secret key. The security analysis and performance of the method are studied and presented.

Keywords Circulant matrix · Determinant · 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

K.A.N. Reddy (✉)
Department of CSE, ACE Engineering College, Hyderabad, India
e-mail: aadi.iitkgp@gmail.com

B. Vishnuvardhan
Department of IT, JNTU, Jagityala, Karimanagar, India
e-mail: mailvishnu@yahoo.co.in

G.S.C. Prasad
Department of CSE, Matrusri Engineering College, Saidabad, Hyderabad, India

S.C. Satapathy et al. (eds.), *Information Systems Design and Intelligent Applications*, Advances in Intelligent Systems and Computing 434,
DOI 10.1007/978-81-322-2752-6_10

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: Sect. 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 Sect. 5.

2 Literature Review on Hill Cipher Modifications

Many researchers improved the security of linear transformation based cryptosystem. Yeh et al. [14] presented an algorithm which thwarts the known-plaintext attack, but it is not efficient for dealing bulk data, because too many mathematical calculations. Saeednia [11] 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 [4] tried a new scheme HillMRIV (Hill Multiplying Rows by Initial Vector) using IV (Initial Vector) but Rangel-Romeror et al. [8] 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 et al. [7] improved the security of Hill cipher by using several random numbers. It thwarts the known-plaintext attack but Toorani et al. [12, 13] 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 Keliher et al. [6] proved that it is still vulnerable to chosen plaintext attack. Ahmed and Chefranov [1–3] 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 et al. [9, 10] improved the security of the cryptosystem by using circulant matrices but the time complexity is more. Again Kaipa et al. [5] 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. In this paper randomness will be included to the linear transformation based cryptosystem to overcome chosen-plaintext and chosen-ciphertext attacks and to reduce the time complexity.

3 Proposed Cryptosystem

In this paper an attempt is made to propose a randomized 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 ith partitioned block (i = 1, 2, … m) and size of each M_i is 'n'. Let C_i be ciphertext of the ith block corresponding to the ith of block plaintext. In this paper the randomness is added to the linear transformation based cryptosystem. Each element of the plaintext block is replaced by a randomly selected element from the corresponding indexed sub key group. The randomly selected element will not be exchanged with the receiver. In this method key generation and sub key group generation is similar to hybrid cryptosystem [3]. Choose a prime number 'p'. The following steps illustrate the algorithm.

1. **Step 1: Key Generation**. Select randomly 'n' numbers (k_1, k_2, … k_n) such that GCD (k_1, k_2, … 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 $K_{n\times n}$. The generated key matrix is called prime circulant matrix.
2. **Step 2: Sub Key Group Generation**. Let $r = \sum_{i=1}^{n} k_i \bmod p$. A sequence of 'p' pseudo random numbers S_i (i = 0, …, p − 1) are generated with initial seed as r. The sub key groups are generated with following steps as

   Step 1: initialize i = 0
   Step 2: j = i + S[i] % b
   Step 3: $S_G[j] = \{i\}$
   Step 4: i ++
   Step 5: goto step 2

3. **Step 3: Encryption**. The encryption process encrypts each block of plaintext using the following steps.
   3.1. Initially the transformation is applied as Y = KM mod p.
   3.2. Convert each element of the block into base b number system
   3.3. Replace each digit of the element by a randomly chosen element from the corresponding sub key group.
   3.4. Transmit the ciphertext block to the other end user
4. **Step 4: Decryption.** The encryption process encrypts each block of plaintext using the following steps
   4.1. Replace each element by an index of the sub key group which it belongs
   4.2. Convert the base b number system into equivalent decimal number system
   4.3. The inverse linear transformation is applied as $M = K^{-1}Y \bmod p$
   4.4. 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 [4, 11]. Generate shared key matrix $K_{3\times3}$. Assume the plaintext block M = [3, 10, 12]. Generate a sequence of 'p' pseudo-random number with seed value as r = 45. Assume b = 5 and generate five sub-key groups (S_G) from the random number sequence. The sub key groups are random and of variable length.

$$S_G[0] = \{0, 6, 17, 21, 24, 25, 31, 38, 50\}$$
$$S_G[1] = \{1, 4, 9, 12, 16, 29, 30, 34, 39, 40, 43, 44, 46, 48, 49\}$$
$$S_G[2] = \{2, 3, 13, 22, 23, 26, 37, 45, 51, 52\}$$
$$S_G[3] = \{7, 10, 15, 19, 20, 27, 33, 42\}$$
$$S_G[4] = \{5, 8, 11, 14, 18, 28, 32, 35, 36, 41, 47\}$$
$$Y = KM \bmod p = KM \bmod 53 = [0, 42, 44]$$
$$0 \rightarrow 0.000\left(0.5^2 + 0.5^1 + 0.5^0\right)$$
$$42 \rightarrow 132\left(1.5^2 + 3.5^1 + 2.5^0\right)$$
$$44 \rightarrow 134\left(1.5^2 + 3.5^1 + 4.5^0\right)$$

Each of the digits is replaced by an element from the corresponding sub key group

The possible ciphertext pairs are presented in Table 1.

The same plaintext is mapped to many ciphertext pairs

After communicating the ciphertext pair (C_1, C_2) to the receiver, the decryption process outputs the plaintext as [3, 10, 12].

Table 1 Ciphertext corresponding to plaintext

Plaintext	Base b number system	Ciphertext 1	Ciphertext 2	Ciphertext
12	000	6	17	50
14	132	4	15	23
3	134	30	42	5

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.

4.1 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 Eq. (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.

$$\begin{aligned} T_{Enc}(m) &\cong m(n^2)T_{Mul} + m(n^2)T_{Add} \\ T_{Dec}(m) &\cong m(n^2)T_{Mul} + m(n^2)T_{Add} + mnT_s \end{aligned} \tag{1}$$

In which T_{Add}, T_{Mul}, and T_s are the time complexities for scalar modular addition, multiplication, and search for the index respectively.

$$\begin{aligned} T_{Enc}(m) &\cong m(n^2)c_1 + m(n^2)c_2 \cong O(mn^2) \\ T_{Dec}(m) &\cong m(n^2)c_1 + m(n^2)c_2 + mnc_3 \cong O(mn^2) \end{aligned} \tag{2}$$

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.

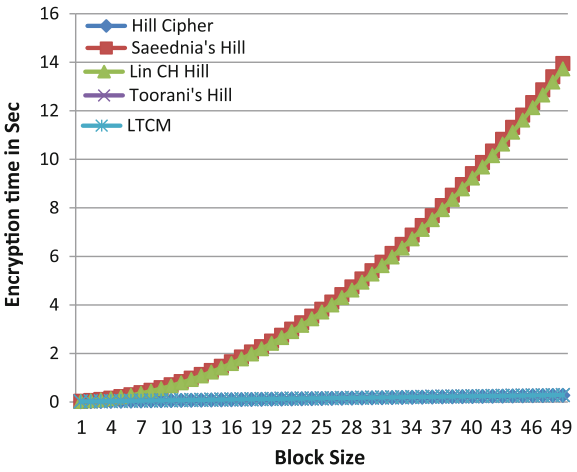

Fig. 1 Encryption time

4.2 Security Analysis

The key matrix is shared secretly by the participants. The attacker tries to obtain the key by various attacks but it is difficult because the random selection of elements from sub key groups. It is difficult to know the elements of the sub key groups because each sub key group is of variable length and generated by modulo which is an one-way function.

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-ciphertext attacks because one plaintext block is mapped to $(b*l_1*\ldots*l_n)^n$ ciphertext blocks where l_i is the length of the corresponding ith sub key group and these groups are variable length. This is due to the random selection of element from the corresponding sub key group. Therefore, the cryptanalyst can no longer encrypt a random plaintext looking for correct ciphertext. To illustrate this assume that the cryptanalyst has collected a ciphertext C_i and guessed the corresponding plaintext M_i correctly but when he/she encrypt the plaintext block M_i the corresponding ciphertext block C_j will be completely different. Now he/she cannot confirm M_i is correct plaintext for the ciphertext C_i.

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 the result is replaced by a randomly selected element from the corresponding sub key group. The sub key groups are of variable length and each sub key group is

generated randomly using one-way modulo function. The proposed randomized encryption algorithm produces more than one ciphertext for one plaintext because each element of the block is replaced by a randomly selected element from the corresponding sub key group. The proposed cryptosystem is free from all the security attacks and it has reduced the memory size from n^2 to n, because key matrix is generated from the first row of the matrix and is simple to implement and produces high throughput.

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. 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.
5. 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.
6. Keliher, L. and A.Z. Delaney, 2013. Cryptanalysis of the toorani-falahati hill ciphers. Mount Allison University. http://eprint.iacr.org/2013/592.pdf.
7. 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.
8. 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.
9. 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.
10. 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.
11. Saeednia, S., 2000. How to make the hill cipher secure. Cryptologia, 24: 353–360. DOI: 10.1080/01611190008984253.
12. 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.
13. Toorani, M. and A. Falahati, 2011. A secure cryptosystem based on affine transformation. Sec. Commun. Netw., 4: 207–215. DOI: 10.1002/sec.137.
14. 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.