Journal of Theoretical and Applied Information Technology
10th November 2013. Vol. 57 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

A DOUBLE GUARD HILL CIPHER SUITABLE FOR WIRELESS SENSOR NETWORKS

[1]C.BENNILA THANGAMMAL , [2]P.RANGARAJAN , [3]J.RAJA PAUL PERINBAM

[1] Assoc. Prof, Department of Information Technology, R.M.D Engineering College, Tamil Nadu, India.
[2] Professor, Department of Computer Science Engg , R.M.D Engineering College, Tamil Nadu, India .
3 Professor, Department of Electronics & Communication Engg, KCG Institute of Technology, Tamil Nadu , India.
E-mail: [1]cbt.it@rmd.ac.in, [2]rangarajan69@yahoo.com , [3]rajapaul51@gmail.com

ABSTRACT

A Classical Hill cipher breaks the plaintext into blocks and multiplies each block to a key matrix to obtain the cipher text. But it inclines to known plaintext. To strength the Hill cipher , a novel modification is performed in this paper. A double protection has been given for the Hill cipher with a single private key matrix. First protection is given by modified key matrix K_m , obtained from the private key matrix with some arithmetic operation and the second protection is given before transmitting the cipher text with respect to the 't' matrix. Without the private key matrix and the modified key matrix, cipher text cannot be decrypted. The proposed Double Guard Hill cipher is suitable for Wireless Sensor Networks as it is capable of encrypting 128 ASCII values.
Keywords: *Encryption, Decryption, Modulo-128 inverse, Private Key matrix and Modified Key matrix.*

1. INTRODUCTION

Data security is the major issue in data communication. The study of '*cryptology*' is called cryptography.(rewrite as Cryptology is a Greek word compounded by "*Kryptos*" meaning hidden and "*logos*" meaning word.) where cryptology is a Greek word compounded by "kryptos" means hidden and "logos" means word. The art of sending message secretly was in practice even before four thousand years as a safety measure in military and diplomatic communications. In cryptography and network security by William stallings, encryption and decryption are the two terms used for secured communication. In encryption, the information which is to be transmitted safely is converted to cipher text using any algorithm or logic. In decryption, the received cipher text is decrypted using the same algorithm or logic used during the encryption to obtain the original information. Nowadays, the computer ciphers substitute the mechanical cryptology techniques. Many ciphers are formulated with the help of substitution and transposition principles. All the ciphers depend on choosing a key either public or private. To propose a new cipher, three issues have to addressed,

- Operation used to convert plaintext to cipher text
- Keys used either private or public, number of keys etc.
- Processing of plain text.

Also, in the communication sector wireless communication segment gains the rapid growth. Inspite of many limitations such as battery operated sensors, security issues, low processing capability etc the Wireless Sensor Network (WSN) categorized under infrastructure-less wireless networks has advantages,. The wireless sensors were developed to save energy but the main concern then shifted in monitoring the energy consumption of individual sensor; as the lifetime of the WSN depends largely on the individual wireless sensors. Many protocols and algorithms were proposed for improving the routing of data packets by considering the factors which leads to waste of energy. Then, new sensors were designed to extend the sensing area of the WSN. Also, security issues in data transmission change the research path of energy efficiency in WSN. One of the major issues in WSN is to find the solution for secured energy efficient data transmission. By considering the same, an algorithm is proposed in this paper with the base of Hill cipher. In the rest of the paper, Hill cipher and various algorithm proposed with the base of Hill cipher are explained in section 2, a double guard Hill cipher algorithm is proposed in section 3 and illustrated with an example in section 4. The proposed algorithm is concluded with the future work in section 5.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

2. HILL CIPHER

(Laster S Hill, 1929,1931) formulated the Hill ciphers by using n x n matrix to encrypt and decrypt the messages. Algorithm used by the Hill given in Introduction to cryptography by Johannes A.Buchmann, was

- Alphabets were assigned with the values of 0 to 25 as given in table 1

Table : 1 Hill Cipher Substitution Of The Alphabets

A	B	C	D	E	F	G	H	I
0	***1***	***2***	***3***	***4***	***5***	***6***	***7***	***8***
J	K	L	M	N	O	P	Q	R
9	***10***	***11***	***12***	***13***	***14***	***15***	***16***	***17***
S	T	U	V	W	X	Y	Z	
18	***19***	***20***	***21***	***22***	***23***	***24***	***25***	

Hill ciphers use a private n x n key matrix [K] for encryption and decryption. Once the key matrix (n x n) was formed then the message was formulated into matrix of n x 1 vectors [A] .

Each n x 1 vectors were multiplied with the private key matrix to obtain the encrypted message vector. If the values of the encrypted vectors were greater than 26 alphabets cannot be substituted so, find modulo 26 to bring the encrypted vector less than or equal to 25.

$$\text{Encrypted message vector, } [AE] = AK$$

To decrypt, modular inverse matrix of the private key $[K^{-1}]$ was calculated and multiplied with $[A_E]$.

$$\text{Original message, } A = K^{-1}[A_E]$$

The major advantage of the Hill cipher was, to calculate the suitable key matrix and its modular inverse matrix. Unless the key matrix was available, the messages cannot be decrypted. But the major disadvantages of the Hill cipher was that

1. Hill ciphers encrypt the alphabets that too, only uppercase (or lowercase). In this, special characters and numerals cannot be encrypted.

2. With some of the hacked $[A_E]$ and A it was possible to hack all the messages by obtaining the private key matrix using the matrix theorem

$$K = A_E A^{-1}$$

The Hill cipher was modified by (V.U.K.Sastry,2011) using EBCDIC (Extended Binary Coded Decimal Interchange Code) This code was framed to support IBM mainframes. In this approach the iteration process, mixing process were done bit wise, which was not suitable for the battery operated networks where the energy was a main constraint. The Hill cipher was modified by (Ismail et. Al, 2006) using one-time-one key matrix to improve the security of Hill cipher. Current key is multiplied with a secret initial vector to compute this one-time-one key, but it is inclined to known plain text attack (Romero, 2008). Using Maximum Distance Separable (MDS) master key matrix , a variable length key matrix ,the Hill cipher is modified to strength its security by (Magamba, 2012) using many matrix operations.

3. A DOUBLE GUARDED HILL CIPHER

The disadvantages of Hill cipher are concentrated in the proposed algorithm. In the proposed algorithm instead of 26 alphabets, ASCII values – lowercase, uppercase alphabets, numerals, special characters are considered for encryption. To avoid the known plaintext attack , the key matrix are permutated. So the key matrix cannot be obtained easily without the permutation vector. In the proposed algorithm, novel modifications are performed to strengthen the security of the cipher. An invertible n x n triangular matrix, whose determinant is one, be the private key matrix [K]. A modified n x n key matrix $[K_m]$ is obtained by performing some arithmetic operations whose determinant is also one to strengthen the key matrix. The encryption (figure 1a) and decryption (figure 1b) algorithm of the proposed cipher is

3.1 Encryption Algorithm

The algorithm of proposed cipher to encrypt the message is

1. A n x n invertible triangular matrix is chosen as private key matrix [K] whose determinant is one.

2. According to the key matrix [K], the message matrix [M] is obtained as n x m matrix.

3. Modified n x n key matrix $[K_m]$ whose determinant is one can be obtained by performing some arithmetic operations in the private key matrix [K] (First protection).

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

4. Permutated [P_t] and inverse permutated [P_t^{-1}] is obtained with the help of n x 1‘t’ matrix.
   Note: The values of‘t’ matrix may be programmed as fixed or randomly generated values, ranges in between 1 to n.

5. Key matrix [K] is permutated to strengthen the security .

$$[K_t] = [P_t] [K] [P_t^{-1}]$$

6. Obtain the encrypted n x m matrix, E by multiplying key matrix [K] with message matrix [M].

$$[E] = [K] [M]$$

7. The rows of the encrypted matrix, E are rearranged according to the ‘t’ matrix to obtain [C]to obtain the cipher text and U_m is generated by multiplying modified key matrix [K_m] with ‘t’ matrix.

$$[U_m] = [K_m] [t]$$

   Now transmit the modified encrypted matrix, cipher text [C] along with the U_m matrix.(Second protection).

3.2 Decryption Algorithm

The algorithm of the proposed cipher to decrypt the cipher text is

1. Received U_m matrix is multiplied with inverse modified key matrix [K_m^{-1}] to obtain ‘t’ matrix.

$$[t] = [U_m][K_m^{-1}]$$

2. The rows of the cipher text is rearranged according to the ‘t’ matrix obtained.

3. Construct the permutated [P_t] and it inverse matrix [P_t^{-1}] from‘t’ matrix.

4. Permutated mod-128 inverse key [K_t^{-1}] is obtained by

$$[K_t^{-1}] = [P_t][K^{-1}][P_t^{-1}]$$

5. Plain text is obtained by multiplying the permutated mod-128 inverse key [K_t^{-1}] with the cipher text [C].

$$[M] =[K_t^{-1}][C]$$

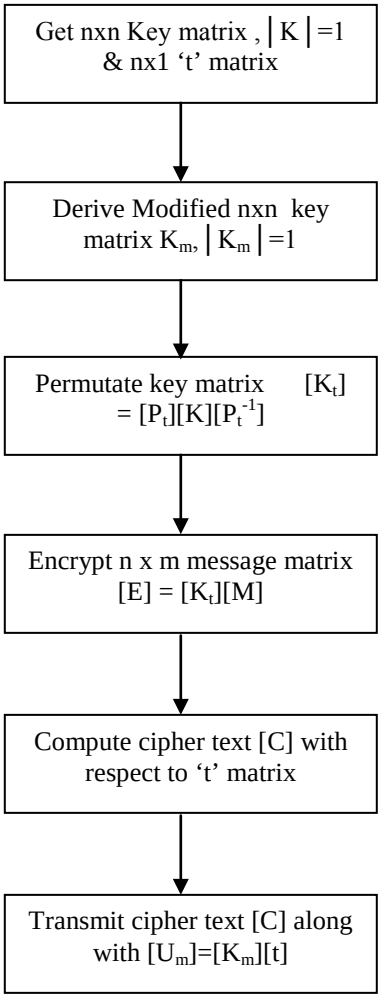

Figure 1a Encryption Algorithm Of Double Guard Hill Cipher

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

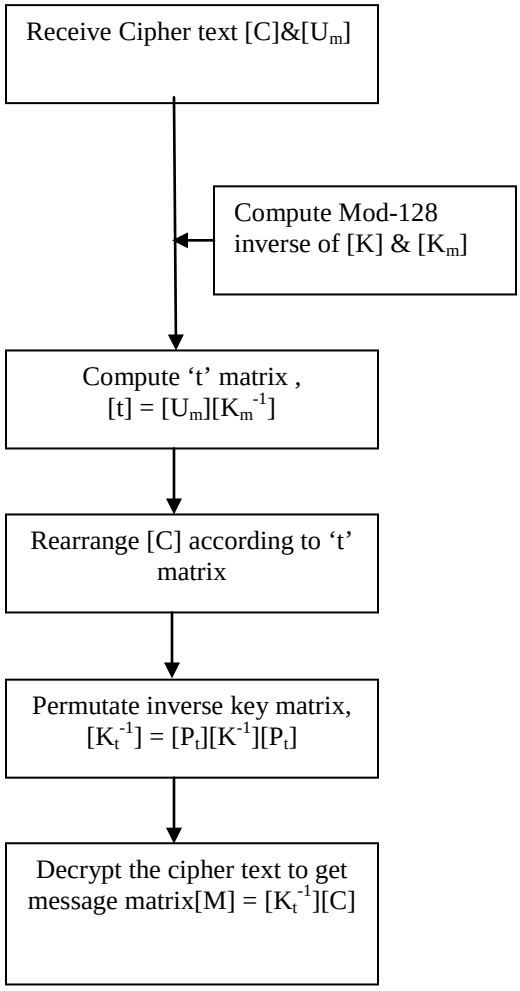

Figure 1b Decryption Algorithm Of Double Guard Hill Cipher

4. ILLUSTRATION OF PROPOSED DOUBLE GUARD HILL CIPHER USING 4 X 4 KEY MATRIX

The proposed Double Guard Hill cipher is illustrated with 4 x 4 invertible triangular key matrix.

$$K = \begin{bmatrix} 1 & 37 & 16 & 8 \\ 0 & 1 & 24 & 82 \\ 0 & 0 & 1 & 76 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

Let the message to be transmitted is **"PW JAson~*^# cvv 264" .** The message has 20 characters , so the message matrix is

$$M = \begin{bmatrix} P & A & \sim & \flat & \flat \\ W & s & * & c & 2 \\ \flat & o & \wedge & v & 6 \\ J & n & \# & v & 4 \end{bmatrix}$$

With the ASCII table, the message matrix [M] be

$$M = \begin{bmatrix} 80 & 65 & 126 & 32 & 32 \\ 87 & 115 & 42 & 99 & 50 \\ 32 & 111 & 94 & 118 & 54 \\ 74 & 110 & 35 & 118 & 52 \end{bmatrix}$$

Modified key matrix [K_m] whose determinant is one is obtained by performing arithmetic operations in key matrix [K].Keep the first row unchanged, add the second, third and fourth row to the first row,

$$\begin{bmatrix} 1 & 37 & 16 & 8 \\ 1 & 38 & 40 & 90 \\ 1 & 37 & 17 & 84 \\ 1 & 37 & 16 & 9 \end{bmatrix}$$

Again keep the first and second row unchanged, subtract the third from second to get third row , subtract fourth row from third to get fourth row.

$$K_m = \begin{bmatrix} 1 & 37 & 16 & 8 \\ 1 & 38 & 40 & 90 \\ 0 & 1 & 23 & 6 \\ 0 & 0 & 1 & 75 \end{bmatrix}$$

Let the't' matrix be chosen in 4 x 1 matrix to enhance the security f the key matrix such as,

$$t = \begin{bmatrix} 4 \\ 1 \\ 3 \\ 2 \end{bmatrix}$$

Let its corresponding permutation [P_t] and inverse permutation [P_t^{-1}] matrix be,

$$P_t = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \text{ and } P_t^{-1} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}$$

The permutated key matrix [K_t] is obtained by multiplying P_t, P_t^{-1} and key matrix,

$$K_t = [P_t][K][P_t^{-1}] = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 8 & 1 & 16 & 37 \\ 76 & 0 & 1 & 0 \\ 82 & 0 & 24 & 1 \end{bmatrix}$$

Journal of Theoretical and Applied Information Technology
10th November 2013. Vol. 57 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Encrypted matrix is obtained by multiplying the permutated key matrix [K_t] and message matrix [M].

$$E = [K][M] = \begin{bmatrix} 80 & 65 & 126 & 32 & 32 \\ 9 & 81 & 9 & 81 & 22 \\ 96 & 59 & 70 & 118 & 54 \\ 106 & 40 & 79 & 70 & 4 \end{bmatrix}$$

Rows of the [E] is rearranged with respect to 't' matrix.

$$C = \begin{bmatrix} 106 & 40 & 79 & 70 & 4 \\ 80 & 65 & 126 & 32 & 32 \\ 32 & 111 & 94 & 118 & 54 \\ 9 & 81 & 9 & 81 & 22 \end{bmatrix}$$

U_m is obtained by multiplying modified key matrix [K_m] with't' matrix.

$$U_m = [K_m][t] = \begin{bmatrix} 105 \\ 86 \\ 82 \\ 25 \end{bmatrix}$$

Now, the cipher text [C] is transmitted to the receiver along with the [U_m]

Receiver who has the exact private key matrix [K] along its modified key matrix [K_m] can only decrypt the cipher text. In the receiver side mod-128 inverse of modified key matrix [K_m^{-1}] is obtained initially.

$$K^{-1} = \begin{bmatrix} 1 & 91 & 104 & 114 \\ 0 & 1 & 104 & 78 \\ 0 & 0 & 1 & 52 \\ 0 & 0 & 0 & 1 \end{bmatrix} and$$

$$K_m^{-1} = \begin{bmatrix} 76 & 53 & 38 & 14 \\ 73 & 55 & 74 & 50 \\ 75 & 53 & 75 & 76 \\ 127 & 1 & 127 & 127 \end{bmatrix}$$

Rows of the received cipher text [C] is rearranged according to the 't' matrix

$$C = \begin{bmatrix} 80 & 65 & 126 & 32 & 32 \\ 9 & 81 & 9 & 81 & 22 \\ 96 & 59 & 70 & 118 & 54 \\ 106 & 40 & 79 & 70 & 4 \end{bmatrix}$$

Compute the permutated [P_t] and inverse permutated matrix [P_t^{-1}] from the obtained 't' matrix. Permutated inverse key matrix [K^{-1}] is obtained as

$$K_t^{-1} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 114 & 1 & 104 & 91 \\ 52 & 0 & 1 & 0 \\ 78 & 0 & 104 & 1 \end{bmatrix}$$

Plain text is obtained multiplying the inverse key matrix [K^{-1}] with cipher text [C].

$$M = K_t^{-1} C = \begin{bmatrix} 80 & 65 & 126 & 32 & 32 \\ 87 & 115 & 42 & 99 & 50 \\ 32 & 111 & 94 & 118 & 54 \\ 74 & 110 & 35 & 118 & 52 \end{bmatrix}$$

Convert this matrix into its corresponding alphabets

$$M = \begin{bmatrix} P & A & \sim & \flat & \flat \\ W & s & * & c & 2 \\ \flat & o & \wedge & v & 6 \\ J & n & \# & v & 4 \end{bmatrix}$$

"PW JAson~*^# cvv 264", thus the original message has been retrieved. In the proposed Double Guard Hill cipher, key matrix is strengthen by creating the modified key matrix[K_m], again the cipher text is rearranged according to the 't' matrix so that it is prone to 'known plaintext attack', 'chosen plain text attack' ,'cipher text attack' as well as 'chosen cipher text attack'. Since the [U_m] is transmitted along with the cipher text and the cipher text is rearranged with respect to 't' matrix , the key matrix cannot be retrieved using 'meet in the middle attack'. Thus the proposed algorithm is very strong as it is not vulnerable to various attacks.

5. CONCLUSION

The proposed cipher is very strong as the key matrix cannot be broken easily by the various attacks. The proposed algorithm uses modular arithmetic and permutation. As the proposed Double Guard Hill cipher provide double protection than the Hill cipher and capable of encrypting 128 ASCII characters it is suitable for WSNs. In future , the proposed algorithm can be refined to suit the energy efficient WSNs for increasing the network's lifetime.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

REFERENCE

[1] William stallings, cryptography and network security, 3rd edition, Pearson education.

[2] Lester S. Hill, Cryptography in an Algebraic Alphabet, The American Mathematical Monthly Vol. 36, June-July 1929, pp. 306-312

[3] Lester S. Hill, Concerning Certain Linear Transformation Apparatus of Cryptography, TheAmerican Mathematical Monthly Vol. 38, 1931, pp.135-154

[4] http://en.wikipedia.org/wiki/Hill_Cipher

[5] Johannes A.Buchmann, Introduction to cryptography,2nd edition , Springer-Verlag, Chapter:3

[6] V.U.K.Sastry Aruna Varanasi and S.Udaya Kumar ,A Modern Advanced Hill Cipher Involving a Permuted Key and Modular Arithmetic Addition Operation, Journal of Global Research in Computer Science,Volume 2, No. 4, April 2011 ISSN : 2229-371X, 92-96

[7] Ismail I A, Amin Mohammed, Diab Hossam, "How to Repair the Hill Cipher," Journal of Zhejiang University Science, 7(12), pp. 2022-2030, 2006.

[8] Romero, Y. R. Garcia, R. V. et al., "Comments on How to Repair the Hill Cipher," J. Zhejiang Univ. Sci. A 9(2): pp. 211-214, 2008

[9] Kondwani Magamba , Solomon Kadaleka ,Ansley Kasambara, " Variable length Hill Cipher with MDS key matrix " , Cornell university 2012, DOI- arXiv:1210.1940v1.