Journal of Computer Science of Newports Institute of Communications and Economics
Volume 6, Issue-2015, ISSN: 2226-3683

Advance Procedure Of Encryption And Decryption Using Transposition And Substitution

FOZIA HANIF KHAN[1], FARHEEN QAZI[2]

[1]Department of Mathematics, Sir Syed University of Engineering and Technology, Karachi, Pakistan, ms_khans2011@hotmail.com

[2]Department of Computer Engineering, Sir Syed University of Engineering and Technology, Karachi, Pakistan,engr.fq@gmail.com

ABSTRACT

It is very important in today's world to protect communication procedure from prying eyes, and is needed more than ever before. Cryptography plays a major role in mobile communication, sending emails, exchanging financial information, the security of ATM cards and in innumerable other ways in our daily lives. It is a well-known fact that Hill cipher succumbs to cryptanalysis relatively easily. In this paper the same effort has been made by using the orthogonal key matrix and presenting the new way of encryption and decryption to strengthen the security of Hill cipher against the known plain text-attack. The proposed scheme is based upon the transposition and then application of the Ceasr cipher substitution which makes it almost impossible to break the cipher text.

Key Words: *Cryptography, encryption, orthogonal key, decryption, transposition.*

1. Introduction

In a recent paper [3] we have presented a new a secure procedure for generating orthogonal key for Hill cipher by using the three dimensional equation. In the current paper, by using the same key we are proposing the new way of encryption and decryption to enhance the security of Hill cipher. We have adopted a procedure which is called transposition and substitution technique. During the encryption procedure the matrix of the plane text will be multiplied with the key matrix after its transposition. By choosing any arbitrary value '***a'*** it changes the plane text completely by adding this arbitrary value in each element of the transposed plane text. This procedure is called the Caesr cipher substitution.

The uniqueness of this paper is to overcome the drawback from the routine procedure of generating the random key in Hill cipher algorithm for encryption and decryption. The purpose for using the orthogonal matrix is definitely to reduce the computational complexity and avoiding the process of finding the inverse of the key in the decryption procedure. As described in [3] that, by using the orthogonal matrix, security will be sufficiently enhanced if we send the equation of plan instead of sending the complete key.

2. Literature review

Hill cipher is very well known and very eye-catching due to its simplicity and strong throughout [8, 9], but is can be broken by the attack called Plain Text Cipher attack (KPCA) [10]. Several modifications have made to secure the procedure and increase the strength of Hill cipher. In HC modification [9] HCM-PT random permutation of rows and column is used for generating the dynamic key from the master key. Efforts in [2] which works like HCM-PT but does not transfer permutations. Both techniques use pseudo random permutation generator, but only the selected number of permutations are transferred to the receiver. In symmetric cryptosystem the single key is used for sender and the recipient, which means the key used for the encryption will definitely be used for the decryption procedure [1]. In symmetric cryptosystem [11] substitution or transposition and merging of both can be used. In [4] there is a good effort to improve the security of Hill cipher by using the initial vector that multiplies with each row of the key matrix and generates a new key. Lin Ch [5] claimed that by using random number

and one way hash function will prevent the known plain text attack to Hill cipher. Mohsen Toorani [6, 7] proposed symmetric cryptosystem scheme which is based on affine transformation.

Our aim is to make a useful modification of Hill cipher by including both K and K^{-1} and by introducing a new way of encryption and decryption, instead of having only K in encryption and K^{-1} in the decryption. In the experimental analysis it has been observed that the strength of proposed procedure of Hill cipher is relatively more significant as compared to old one and it cannot be easily broken by other cryptanalytic attack.

3. Proposed Algorithm

As described in the earlier section we are using the orthogonal matrix for the proposed technique. Previously we have defined the complete procedure of generating orthogonal key [3]. After generating the orthogonal key which is,

$$k = \begin{bmatrix} k_{11} & k_{12} & k_{13} & k_{14} \\ k_{21} & k_{22} & k_{23} & k_{24} \\ k_{31} & k_{32} & k_{33} & k_{34} \\ k_{41} & k_{42} & k_{43} & k_{44} \end{bmatrix} \qquad (1)$$

there might be a chance of getting some negative values in the generated key; therefore, by taking additive inverse in mod 26 for converting the negative values in to positive and for further simplification also one by one as per the requirements. As a result of this, a secured key will be generated, and ***k*** will turn into ***k'***:

$$k' = \begin{bmatrix} k'_{11} & k'_{12} & k'_{13} & k'_{14} \\ k'_{21} & k'_{22} & k'_{23} & k'_{24} \\ k'_{31} & k'_{32} & k'_{33} & k'_{34} \\ k'_{41} & k'_{42} & k'_{43} & k'_{44} \end{bmatrix} \qquad (2)$$

3.1 Proposed Procedure for Encryption

Take some plain text ***p***:

$$p=\begin{bmatrix} p_1 \\ p_2 \\ p_3 \\ p_4 \end{bmatrix} \qquad (3)$$

Take the transpose of plaintext and change the actual position/location of the plain text, in the proposed algorithm, where we change the position of plaintext in reverse order

$$p'=\begin{bmatrix} p_4 \\ p_3 \\ p_2 \\ p_1 \end{bmatrix} \qquad (4)$$

Arbitrarily, we take an integer **"a"** and add in each element of $\boldsymbol{p'}$then $\boldsymbol{p}$"will become,

$$p"=\begin{bmatrix} p^4 + a \\ p^3 + a \\ p^2 + a \\ p^1 + a \end{bmatrix} \qquad (5)$$

And the Ceaser Cipher substitution technique generates newly secured plaintext:

by applying standard method of hill cipher encryption convert the plaintext $\boldsymbol{p'''}$similar to:

$$\begin{bmatrix} k'_{11} & k'_{12} & k'_{13} & k'_{14} \\ k'_{21} & k'_{22} & k'_{23} & k'_{24} \\ k'_{31} & k'_{32} & k'_{33} & k'_{34} \\ k'_{41} & k'_{42} & k'_{43} & k'_{44} \end{bmatrix} * \begin{bmatrix} p"_4 \\ p"_3 \\ p"_2 \\ p"_1 \end{bmatrix} = \begin{bmatrix} c^1 \\ c^2 \\ c^3 \\ c_4 \end{bmatrix} \qquad (6)$$

Where, c is the newly produced cipher text from the newly produced key $\boldsymbol{k'}$and plaintext $\boldsymbol{p'''}$

3.2 Procedure for the Decryption:

As we have discussed initially we are using orthogonal key therefore the inverse of the orthogonal key will be the transpose of k',

$$\boldsymbol{k' = k'^{t} = k'^{-1}} \qquad (7)$$

$$\boldsymbol{k'^{-1} = k'^{t} = I} \qquad (8)$$

Applying the standard procedure of decryption of hill cipher we obtain p''':

$$\begin{bmatrix} k'_{11} & k'_{12} & k'_{13} & k'_{14} \\ k'_{21} & k'_{22} & k'_{23} & k'_{24} \\ k'_{31} & k'_{32} & k'_{33} & k'_{34} \\ k'_{41} & k'_{42} & k'_{43} & k'_{44} \end{bmatrix} * \begin{bmatrix} c^1 \\ c^2 \\ c^3 \\ c_4 \end{bmatrix} = \begin{bmatrix} p''_4 \\ p''_3 \\ p''_2 \\ p''_1 \end{bmatrix} \qquad (9)$$

to obtain the real plaintext applying back substitution technique of Ceaser Cipher

$$\begin{bmatrix} p''_4 \\ p''_3 \\ p''_2 \\ p''_1 \end{bmatrix} = \begin{bmatrix} p_4 \\ p_3 \\ p_2 \\ p_1 \end{bmatrix} \qquad (10)$$

Furthermore, applying reverse procedure of transposition on plaintext, we produce real plaintext

$$\begin{bmatrix} p_4 \\ p_3 \\ p_2 \\ p_1 \end{bmatrix} = \begin{bmatrix} p_1 \\ p_2 \\ p_3 \\ p_4 \end{bmatrix} \qquad (11)$$

figure 3 shows the complete description of the algorithm.

3.3 Example

Consider an orthogonal key which we have generated through the previous defined procedure in [3].

$$k = \begin{bmatrix} 77 & -14 & -42 & -56 \\ -14 & 98 & -21 & -28 \\ -42 & -21 & 42 & -84 \\ -56 & -28 & -84 & -7 \end{bmatrix}$$

After taking additive inverse in mod 26,***k*** will become ***k'***:

$$k'=\begin{bmatrix}25 & 12 & 10 & 22\\ 12 & 20 & 05 & 24\\ 10 & 05 & 16 & 20\\ 22 & 24 & 20 & 19\end{bmatrix}$$

3.4 Encryption:

Consider any plaintext:

Plaintext = SECURITY

$$p=\begin{bmatrix}S\\ E\\ C\\ U\end{bmatrix}=\begin{bmatrix}18\\ 4\\ 2\\ 20\end{bmatrix}$$

Applying transposition

$$p'=\begin{bmatrix}U\\ C\\ E\\ S\end{bmatrix}=\begin{bmatrix}20\\ 2\\ 4\\ 18\end{bmatrix}$$

Applying Ceaser Cipher Substitution by considering any arbitrary value which is 7 here.

$$p"=\begin{bmatrix}20+7\\ 2+7\\ 4+7\\ 18+7\end{bmatrix}$$

$$p'''=\begin{bmatrix}27\\ 9\\ 11\\ 25\end{bmatrix}(\text{mod } 26)=\begin{bmatrix}1\\ 9\\ 11\\ 25\end{bmatrix}$$

By applying the regular procedure of encryption regarding to hill cipher we convert the plaintext ***p'''***like this:

$$\begin{bmatrix} 25 & 12 & 10 & 22 \\ 12 & 20 & 05 & 24 \\ 10 & 05 & 16 & 20 \\ 22 & 24 & 20 & 19 \end{bmatrix} * \begin{bmatrix} 1 \\ 9 \\ 11 \\ 25 \end{bmatrix} = \begin{bmatrix} 793 \\ 847 \\ 731 \\ 933 \end{bmatrix} (\text{mod } 26)$$

$$c = \begin{bmatrix} 13 \\ 15 \\ 3 \\ 23 \end{bmatrix}$$

Where, c is the newly produced cipher text

3.5 Decryption:

After the regular procedure of decryption of hill cipher we produce the plain text $\boldsymbol{p'''}$:

$$\begin{bmatrix} 25 & 12 & 10 & 22 \\ 12 & 20 & 05 & 24 \\ 10 & 05 & 16 & 20 \\ 22 & 24 & 20 & 19 \end{bmatrix} * \begin{bmatrix} 13 \\ 15 \\ 3 \\ 23 \end{bmatrix} = \begin{bmatrix} 1041 \\ 1023 \\ 713 \\ 1143 \end{bmatrix} (\text{mod } 26)$$

$$p''' = \begin{bmatrix} 1 \\ 9 \\ 11 \\ 25 \end{bmatrix}$$

Applying back substitution

$$p'' = \begin{bmatrix} 20 - 7 \\ 2 - 7 \\ 4 - 7 \\ 18 - 7 \end{bmatrix} = \begin{bmatrix} -6 \\ 2 \\ 4 \\ 18 \end{bmatrix} (\text{mod } 26)$$

$$p' = \begin{bmatrix} 20 \\ 2 \\ 4 \\ 18 \end{bmatrix}$$

Applying back transposition we get the original plane text which is,

$$p = \begin{bmatrix} 20 \\ 2 \\ 4 \\ 18 \end{bmatrix} = \begin{bmatrix} 18 \\ 4 \\ 2 \\ 20 \end{bmatrix} = \begin{bmatrix} S \\ E \\ C \\ U \end{bmatrix}$$

4. Experimental Setup

Elapsed time is basically measures the amount of time that MATLAB takes to complete one or more operations and displays the time in seconds. For the experimental setup we have done our simulation on Pentium IV. The MATLAB version 7.3 coding is given below which is calculating the elapsed time of encryption and decryption process separately. The graphical representation is showing in figure 1which is the simulation time of our proposed algorithm. The graph has been plotted between number of iterations (which is 50 in this case) and elapsed time.

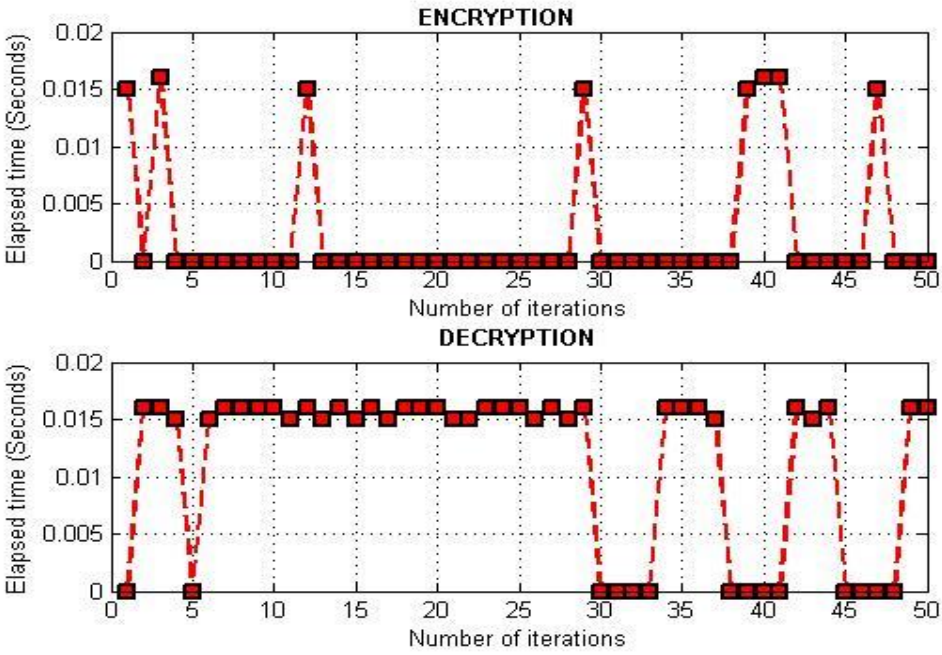

Figure 1: Showing the elapsed time with number of iteration for the encryption and decryption

The elapsed time of complete algorithm is plotted in figure 2 in which the graph was plotted between number of iterations (which is 50 in this case) and elapsed time

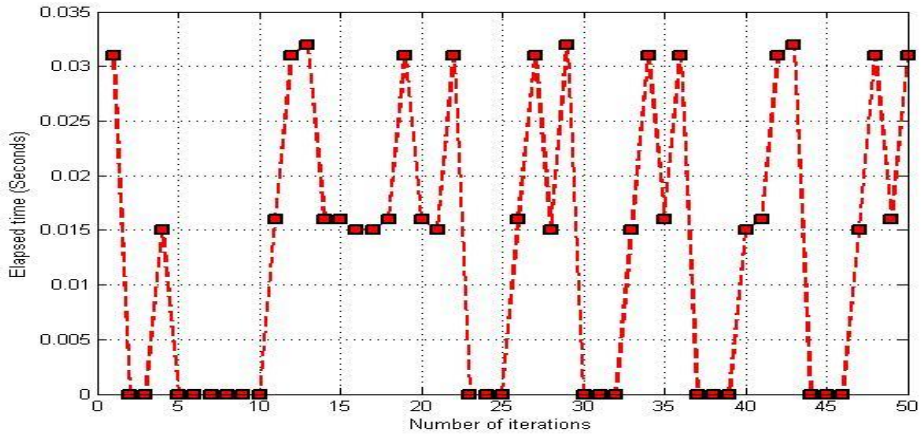

Figure 2: Showing the elapsed time with number of iterations

4.1 Pseudo code of the algorithm:

```
%--------ENCRYPTION----------

%input a key vector
key=input('Enter values for key:');
%input plaintext
plaintext=input('Enter values for plaintext:');
%input the value of ceasar cipher substitution key
subk=input ('input value:');
%apply transposition on plaintext
p1=flipud ([plaintext])
%apply ceasar cipher substitution on p1
p2=p1+subk
p3=mod(p2,26)
%p3 is the newly generated plain test
%for cipher text
Cipher text=key*p3
c=mod(ciphertext,26)

%--------DECRYPTION-----------
```

```
%taking transpose of key
k=transpose(key)
%for obtaining p3
plaintext3=key*c
pltxt3=mod(plaintext3,26)
%applying back ceasar cipher substitution
plaintext2=pltxt3-subk
pltxt2=mod(plaintext2,26)
%apply back transposition
plaintext1=flipud([pltxt2])
%now plaintext1 is the original plaintext
```

5. Flow Chart of the proposed Algorithm

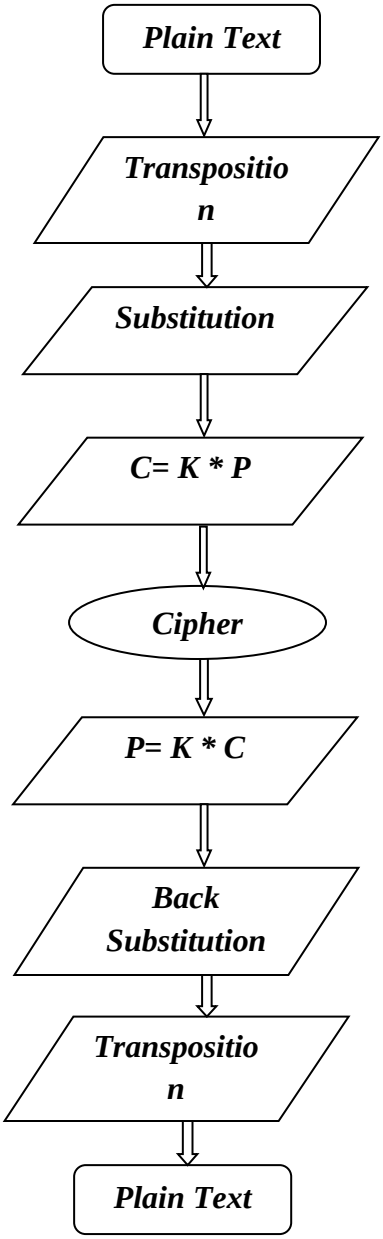

Figure 3: showing the complete procedure of the proposed algorithm

6. Conclusion

This study has made an effort for generating a secure and strong procedure for Hill cipher. The object of this study is to increase the strength and security of Hill cipher together with a technique which is not complicated in term of application but, as much as stronger for the security point of view. The proposed methodology not only use the transposition technique but also used the Ceaser cipher substitution. Our experimental setup has shown the performance of our algorithm. Therefore a considerable contribution has been made for the security of Hill cipher.

References

[1] Bibhudendra A., (2008), **"**Invertible, Involuntary and Permutation Matrix Generation Methods for Hill Cipher System" IEEE International Conference on Advanced Computer Control.

[2] Chefranov, A. G.,(2008), "Secure Hill Cipher Modification SHCM", Proc. of the First International Conference on Security of Information and Networks (SIN2007) 7-10 May 2007, Gazimagusa (TRNC) North Cyprus, Elçi, A., Ors, B., and Preneel, B. (Eds.) Trafford Publishing, Canada. 34-37.

[3] F. Hanif Khan, R. Shams, F. Qazi, and D. Agha, (2015), "Hill Cipher Key Generation Algorithm by using Orthogonal Matrix", International Journal of Innovative Science and Modern Engineering (IJISME). Vol. 3, issue 3, pp. 5-7.

[4] [6]. Hill LS, 1929 "Cryptography in an Algebraic Alphabet", American Mathematical Monthly; 36: 306-312.

[5] Lin CH, Lee CY, Lee CY., (2004), "Comments on Saeednia's improved scheme for the Hill cipher", Journal of the Chinese institute of engineers, pp.; 27: 743-746.

[6] Li C, Zhang D, Chen G., (2008), "Cryptanalysis of an image encryption scheme based on the Hill cipher", Journal of Zhejiang University - Science A , pp; **9**: 1118-1123.

[7] Mohsen T., Abolfazl F., (2011), "A Secure Cryptosystem based on Affine Transformation", Journal of Security and Communication Networks, pp. 207-215.

[8] Overbey, J. Traves, W. and Wojdylo, J.,(2005), "On the Key Space of the Hill Cipher", Cryptologia, 29(1), 59-72.

[9] Saeednia, S.,(2000), "How to Make the Hill Cipher Secure", Cryptologia, 24(4), 353-360.

[10] Stallings, W., (2006), "Cryptography and Network Security", 4th Edition. Prentice Hall, Upper Saddle River.

[11] Simmons, (1979), G**.** J, **"**Symmetric and Asymmetric Encryption", ACM Computing Surveys,