International Journal of Psychosocial Rehabilitation, Vol. 24, Issue 08, 2020
ISSN: 1475-7192

Application of Vigenere Cipher to Enhance the Playfair Cipher Security

[1]Ms. Prachi Gupta, [2]Dr. Manoj Kumar

***Abstract*: -**

We present a new approach for secure transmission of message by modified version of Playfair cipher with Random number generator methods combining with Vigenere cipher. To develop this method of encryption technique, one of the simplest methods of random number generator methods called linear congruential generator has been used. Playfair cipher method based on polyalphabetic cipher. It is relatively easy to break because it still leaves much of the structure and a few hundred of letters of ciphertext are sufficient. In this we used double encryption and decryption technique. For the encryption, first encrypt the plaintext by vigenere cipher, and then result encrypt by playfair cipher. And result is called ciphertext. After that we are mapping random numbers to ciphertext and corresponding numbers will be transmitted to the recipient instead of alphabetical letter. This method rapidly increases security of the transmission over an unsecured channel.

Keywords— *Playfair cipher, Vigenere Cipher, pseudorandom number, Linear Feedback Shift Register, polyalphabetic cipher.*

1. INTRODUCTION

The relationship of cryptography and random numbers are investigated. Linear Congruential generator method is a good candidate for generating random numbers . We can easily modify the congruential generator method and produce unique random numbers. So it provides very good security for transmission. And also implementation of congruential generator method is very easy . This paper presents a new approach, Encryption and Decryption using Playfair Cipher and Vigenere Cipher, if we get cipher text then find numbers corresponds to cipher text. In playfair cipher, the alphabets are arranged in 5x5 table based on secret key, even though it is very difficult to break the ciphertext but it can be breakable by few hundreds of letters. And also in this method we are transmitting alphabets to the receiver . In our approach, on key stream value only, alphabets and number are arranged in 6x6 table that is called playfair key matrix. The congruential generator method produce various random sequences, the number are filled in 6x6 table. We use Vigenere cipher, Playfair cipher and Linear congruential generator method to enhance the security of classical playfair cipher. First encrypt the plaintext by vigenere cipher with keyword and then result encrypt by playfair cipher with another keyword. We get the cipher text. Linear congruential generator method generate unpredictable sequence of number. This sequence of number depends on the multiplier and increment. We mapping the sequence number to cipher text and find corresponding sequence of number. We transmit sequence of number to the receiver instead of alphabets. At the receiver side, receiver receive the sequence of number, and find the cipher text corresponds to sequence of these numbers. First decrypt the cipher text by playfair cipher with same encryption keyword and then result decrypt by vigenere cipher with same encryption keyword. Then we get the original plaintext. This technique increases the security of playfair cipher.

2. Playfair Cipher

The Playfair cipher uses 5 x 5 table containing a key word or phrase. Memorization of the keyword and 4 simple rules are all that are required to create the 5 x 5 table and use the cipher. To generate the key table, one would first fill in the spaces in the table with the letters of the keyword (dropping and duplicate letters), then fill the remaining space with the rest of
letters of the alphabet in order (put both I and J in the same space). The key can be written in the top row of the table, from left to right. The keyword together with the conventions for filling in the 5 x 5 table constitutes the cipher key. To encrypt a message, one would break the message into digraphs(groups of 2 letters) such that, for example, ―NETWORK‖ becomes ―NE TW OR KX‖, and map them out on the key table. If needed, append an

[1] *Phd Schollar , Department of Computer Science, The School of Engineering & Technology, SVU Gajraula (UP) India.*
[2] *Assistant Professor, Department of Computer Science, The School of Engineering & Technology, SVU Gajraula (UP) India.*

—X‖ to complete the final digraph. Then apply the following 4 rule, in order, to each pair of letters in the plaintext:

1. If both letters are the same (or only one letter is left), add an —X‖ after the first letter. Encrypt the new pair and continue.
2. If the letter appear on the same row of the table, replace them with the letters to their immediate right respectively(wrapping around to the left side of the row if a letter in the original pair was on the right side of the row).
3. If the letters appear on the same column of the table, replace them with the letters immediately below respectively(wrapping around to the top side of the column if a letter in the original pair was on the bottom side of the column).
4. If the letters are not on the same row or column, replace them with the letters on the same row respectively but at the other pair of corners of rectangle defined by the original pair. The order is important –the first letter of the encrypted pair is the one that lies on the same row as the first letter of the plaintext pair.

To decrypt, use the INVERSE(opposite) of the last 3 rules, and the 1st as-it-is(dropping any extra —X‖s that don‘t make sense in the final message when finished).

Example:
Key: Playfair

P	L	A	Y	F
I/J	R	B	C	D
E	G	H	K	M
N	O	Q	S	T
U	V	W	X	Z

Table 2.1: playfair matrix

Encryption: From the matrix we find the digraph for plaintext as follows:
Plaintext in pairs: NE TW OR KX
Cipher text in pairs: UN QZ VG SY

3. LINEAR CONGRUENTIAL GENERATORS METHOD

The most widely used technique for pseudorandom number generator is the algorithm first proposed by Lehmer, which is known as the linear congruential method. The algorithm is parameterized with four numbers, as follows:

m the modulus m>0
a the multiplier 0<a<m
c the increment 0=<c<m
X0 the starting value or seed 0<= X0<m
The sequence of random number {Xn} is obtained via the following iterative equation:
Xn+1 = (aXn+c)modm
If m, a, c and X0 are integer, then this technique will produce a sequence of integer with each integer in the range 0<= Xn<m.

The selection of values for a, c, and m is critical in developing a good random number generator.
For example, consider a= c= 1. The sequence produced is obviously not satisfactory.
Now consider the values a= 7, c=0, m=32, and X0 =1.
This generates the sequence {7,17,23,1,7,etc}, which is also clearly unsatisfactory.
Of the 32 possible values, only 4 are used ;thus, the sequence is said to have a period of 4. If, instead, we change the value of a to 5, then the sequence is {5,25,29,17,21,9,13,1,5,etc}, which increase the period to 8.

The period of a Linear Congruential Generator method is at most *m*, and for some choices of factor *a* much less than that. Provided that the offset *c* is nonzero, the Linear Congruential Generator method will have a full period if and only if
a. c and m are relatively prime,
b. (a-1) is divisible by all prime factors of m.
c. (a-1) is a multiple of 4 if m is a multiple of 4.

Example: a=5,c=3, X0 =3 and m=32;
Then numbers are 18,29,20,7,6,1,8,11,26,5,28,15,14,9,16,19,2,13,4,23,22,17,24,27,10,21,12,31,30,25,0,3

4.Vigenere Cipher

A poly-alphabetic cipher is any cipher based on substitution, using multiple substitution alphabets. Mono-alphabetic Cipher can be broken. The reason: Same plain letters are encoded to same cipher letters; the underlying letter frequencies remain unchanged.

- Cryptographers have tried to overcome this dilemma simply by assigning various cipher letters or symbols to same plain letters. Such ciphers are called Poly-alphabetic Ciphers. The most popular of such ciphers is the ―Vigenere Cipher‖. The Vigenere Cipher is an improvement of the Caesar Cipher key is multiple letters long K=k1, K2, k3….kd. To encrypt a message, a key is needed that is long as message. Usually, the key is a repeating keyword and also requires a keyword that the sender and receiver known.

- Vigenere cipher starts with a 26 x 26 matrix of alphabets in sequence. First row starts with _A‘, second row starts with _B‘, etc.

- Each letter of the message is combined with the letter of the keyword to find the ciphertext letter.

- For example, if the keyword is deceptive, the message ―we are discovered save youself‖ is encrypted as follows:

- Key: deceptivedeceptivedeceptive

- Plaintext: wearediscoveredsaveyourself

- Ciphertext: ZICVTWQNGRZGVTWAVZHCQYGLMGJ

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
A A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
B B C D E F G H I J K L M N O P Q R S T U V W X Y Z A
C C D E F G H I J K L M N O P Q R S T U V W X Y Z A B
D D E F G H I J K L M N O P Q R S T U V W X Y Z A B C
E E F G H I J K L M N O P Q R S T U V W X Y Z A B C D
F F G H I J K L M N O P Q R S T U V W X Y Z A B C D E
G G H I J K L M N O P Q R S T U V W X Y Z A B C D E F
H H I J K L M N O P Q R S T U V W X Y Z A B C D E F G
I I J K L M N O P Q R S T U V W X Y Z A B C D E F G H
J J K L M N O P Q R S T U V W X Y Z A B C D E F G H I
K K L M N O P Q R S T U V W X Y Z A B C D E F G H I J
L L M N O P Q R S T U V W X Y Z A B C D E F G H I J K
M M N O P Q R S T U V W X Y Z A B C D E F G H I J K L
N N O P Q R S T U V W X Y Z A B C D E F G H I J K L M

Received: 18 Apr 2020 | Revised: 16 May 2020 | Accepted: 21 Jun 2020

O O P Q R S T U V W X Y Z A B C D E F G H I J K L M N

P P Q R S T U V W X Y Z A B C D E F G H I J K L M N O

Q Q R S T U V W X Y Z A B C D E F G H I J K L M N O P

R R S T U V W X Y Z A B C D E F G H I J K L M N O PQ

S S T U V W X Y Z A B C D E F G H I J K L M N O P Q R

T T U V W X Y Z A B C D E F G H I J K L M N O P Q R S

U U V W X Y Z A B C D E F G H I J K L M N O P Q R S T

V V W X Y Z A B C D E F G H I J K L M N O P Q R S T U

W W X Y Z A B C D E F G H I J K L M N O P Q R S T U V

X X Y Z A B C D E F G H I J K L M N O P Q R S T U V W

Y Y Z A B C D E F G H I J K L M N O P Q R S T U V W X

Z Z A B C D E F G H I J K L M N O P Q R S T U V W X Y

Table 4.1 26x26 vigenere cipher matrix

Decryption is equally simple. The key letter again identifies the row. The position of the cipher text letter in that row determines the column, and the plaintext letter is at the top of the column.

For example:

Ciphertext: ZICVTWQNGRZGVTWAVZHCQYGLMGJ
Key: deceptivedeceptivedeceptive
Plaintext: wearediscoveredsaveyourself

5. DESCRIPTION OF NEW ALGORITHM

5.1 Introduction:

This technique enhance the security of Playfair cipher to use the double encryption at the sender side and double decryption technique at the receiver side. At the sender side, First encrypt the message using vigenere cipher with key k1 and then result encrypt using playfair cipher with key k2, then result is called ciphertext . At the receiver side, this ciphertext is decrypt using the double decryption, first using the Playfair cipher with the key k2, and then using the vigenere cipher with key k1, and get the original message.

5.2 Steps for Encryption

1. The alphabets and numbers are arranged in 6x6 Playfair key matrix based on keyword.
2. Generate 6x6 unique random number matrix using the linear congruential generator methods.
3. Map the Playfair key matrix with the random number matrix.
4. Encrypt the plaintext P using Vigenere cipher with key k1 and get intermediate result X.
5. Then this result encrypt using Playfair cipher with keyword k2 and get ciphertext C.
6. Find the corresponding number to ciphertext C, the sequence of these number is transmit to receiver.

5.3 Steps for Decryption

1. Receiver receive the sequence of numbers.
2. Find the ciphertext C corresponding to sequence of number.
3. Decrypt the ciphertext C using the Playfair cipher with keyword k2 and get intermediate result X.
4. And then X is decrypted by vigenere cipher with key k1 and get plaintext P.

Received: 18 Apr 2020 | Revised: 16 May 2020 | Accepted: 21 Jun 2020

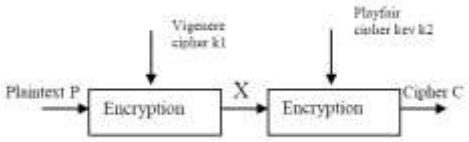
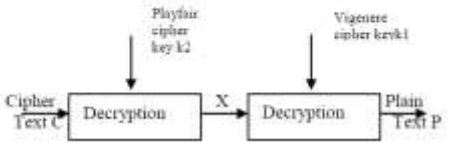


Fig5.1 Encryption using Vigenere cipher and Playfair cipher



Fi5.2 Decryption using Vigenere cipher and Playfair cipher

EXAMPLE :

1. Generate 6x6 playfair key matrix with keyword = CIPHER

C	I	P	H	E	R
0	1	2	3	4	5
6	7	8	9	A	B
D	F	G	J	K	L
M	N	O	Q	S	T
U	V	W	X	Y	Z

TABLE 5.1 6X6 PLAY FAIR MATRIX

2. GENERATE 6X6 UNIQUE RANDOM NUMBER MATRIX USING LINEAR CONGRUENTIAL METHOD.

20	57	15	10	35	49
56	30	19	50	39	37
31	7	3	60	18	33
42	17	62	61	11	44
55	6	36	23	59	13
8	41	47	2	34	25

TABLE5.2 6X6 RANDOM NUMBER MATRIX

3. MAP 6X6 PLAYFAIR KEY MATRIX WITH THE 6X6 RANDOM NUMBER MATRIX.

C-20	I-57	P-15	H-10	E-35	R-49
0-56	1-30	2-19	3-50	4-39	5-37
6-31	7-7	8-3	9-60	A-18	B-33
D-42	F-17	G-62	J-61	K-11	L-44
M-55	N-6	O-36	Q-23	S-59	T-13
U-8	V-41	W-47	X-2	Y-34	Z-25

TABLE5.3 MAPPING TABLE

4. **Encryption:**
   Encryption rule is same as exiting playfair cipher, First encrypt the message using Vigenere cipher with key HELLO and then Playfair cipher with key CIPHER.

- Plaintext: CRYPTOGRAPHY

Received: 18 Apr 2020 | Revised: 16 May 2020 | Accepted: 21 Jun 2020

- Vigenere cipher key = HELLO
- Encrypt the plaintext using Vigenere cipher

  H E L L O H E L L O H E
  C R Y P T O G R A P H Y
  RESULT X = J V J A H Y K C L D H C

- Then encrypt result using Playfair cipher with key CIPHER.

  JV JA HY KC LD HC
  Ciphertext C = FX K9 EX DE DF EI

The transmitted ciphertext is {(17,2),(11,60),(35,2),(42,35),(42,17),(35,57)} instead of alphabetical letter.

5. Decryption:

- Receive ciphertext is {(17,2),(11,60),(35,2),(42,35),(42,17),(35,57)}

  17,2= FX
  11,60= K9
  35,2 = EX
  42,35= DE
  42,17= DF
  35,57= EI

- Ciphertext C = FX K9 EX DE DF EI decrypt using playfair cipher with key CIPHER.
- Ciphertext C = FX K9 EX DE DF EI
  get result X = JV JA HY KC LD HC

  Decrypt the result using Vigenere cipher with key = HELLO

  H E L L O H E L L O H E
  X = JV JA HY KC LD HC
  Plaintext P= C R Y P T O G R A P H Y

6. Analysis of proposed method

The classical Playfair cipher is not secure because it produces only 676 structures. This proposed methodology rapidly increases the security of the ciphertext because we use double encryption and double decryption. And also the inner structure of this method is very simple. Currently many algorithms are available for encryption but it requires many complex rounds like DES, AES etc. AES and DES use two concepts for security, confusion and Diffusion. Confusion means relationship between plaintext and ciphertext as complex as possible. Diffusion means mask the statistical properties of data in the ciphertext. Our approach allows confusion and diffusion can be easily incorporated to Vigenere cipher and Playfair Cipher. The linear congruential generator method can be used to generate random number sequences. Unpredictable different random sequences can be produced from linear congruential generator method by varying multiplier and increment. Increasing modulus value can increase the cycle length. It can be easily implemented with advent of new computer. The implementation of linear congruential generator method in hardware and Software is very easy. The cost is very less and also speed is considerably very high compare to other methods. This method of encryption does not increase size of the ciphertext. For areas with low bandwidth or very less memory storage this method can be used. The classical Playfair cipher is relatively easy to break because it still leaves much of the structure of the plaintext language. This method of incorporating random sequences can also be applied to other ciphers.

Received: 18 Apr 2020 | Revised: 16 May 2020 | Accepted: 21 Jun 2020

7.CONCLUSION

To implement modified Playfair cipher using random number generation. We use linear congruential generator method, that can be used to generate unpredictable different random sequences by varying increment and multiplier. The classical Playfair cipher is not secure because it produces only 676 structures. We use vignere cipher and Playfair cipher for encryption and decryption. We are mapping random number sequence to ciphertext and corresponding number will be transmitted to the recipient instead of alphabetical letter. This method increases security of the transmission over unsecured channel. Because we use 6x6 matrix that produces 1296 structures and also use vigenere cipher that produces 456976.The total structures produces will be 1296*456966 = 592240896. The future work shall consider, to increases the size of matrix to include the special character.

REFERENCES

1) William stalling, ―Cryptography and Network Security : Principals and Practice,‖ Pearson Education, Edition Fifth, 2011.

2) Behrouz A. Frouzan, ―Cryptography and Network Security,‖ Tata McGraw Hill, Edition Second, 2010.

3) V. Umakanta Sastry, N. Ravi Shankar and S. Durga Bhavani, ―A Modified Playfair Cipher Involving Interweaving and Iteration,‖ International Journal of Computer Theory and Engineering, vol. 1,no. 5, Dec. 2009.

4) Dr. Ashish Negi, Jayveer Singh Farswan, V.M Thakkar and Siddharth Ghansala, ―Cryptography Playfair Cipher Using Linear Feedback Shift Register, ‖ IOSR Journal of Engineering, vol. 2(5), pp. 1212-1216, May 2012.

5) Rishi Dutt Sharma, ―Quantum Cryptography: a New Approach to Information Security,‖ International Journal of Power System Operation and Energy Management (IJPSOEM), vol. 1, Issue. 1, 2011.

6) Vishwa gupta , Gajendra Singh and Ravindra Gupta, ―Advance cryptography algorithm for improving data security,‖ International Journal of Advance Research in Computer Science and Software Engineering, vol. 2, Issue 1, Jan. 2012.

7) Shiv Shakti Srivastava and Nitin Gupta, ―A Novel Approach to Security using Extended Playfair Cipher,‖ International Journal of Computer Application, ISSN 0975-8887, vol. 20, no. 6, Apr. 2011.

8) Harinnandan Tunga and Soumen Mukherjee, ―A New Modified Playfair Algorithm Based on Frequency Analysis,‖ International Journal of Emerging Technology and Advanced Engineering, ISSN 2250- 2459, vol. 2, Issue 1, Jan. 2012.

9) Packirisamy Murali and Gandhidoss Senthikumar, ―Modified version of Cipher using Linear Feedback Shift Register,‖ International Journal of Computer Science and Network Security, IJCSNS, vol.8 No.12, December 2008.

10) Amandeep Kaur, Harish Kumar Verma And Ravindra Kumar Singh, ―Playfair Cipher using LFSR based Unique Random Number Generation,‖

11) S.S.Dhennakaran and M.Ilayaraja, ―Extension of Playfair Cipher using 16x16 Matrix,‖ International Journal of Computer Application(0975-888), vol.48- No.7, June 2012.

12) Harinnandan Tunga and Soumen Mukherjee, ―A New Modified Playfair Algorithm Based on Frequency Analysis,‖ International Journal of Emerging Technology and Advanced Engineering, ISSN 2250- 2459, vol. 2, Issue 1, Jan. 2012.

13) S.S.Dhennakaran and M.Ilayaraja, ―Extension of Playfair Cipher using 16x16 Matrix,‖ International Journal of Computer Application(0975-888), vol.48- No.7, June 2012.

14) Mohit Kumar, Reena Mishra, Rakesh Kumar Pandey and Poonam Singh ―Comparing Classical Encryption With Modern Techniques‖in proceedings of S-JPSET, Vol. 1, Issue 1,2010.

15) A. Alam, S. Khalid, & M. Salam, ―A Modified Version of Playfair Cipher Using 7x4 Matrix,‖ (October 17-19, 2010) IEEE International Conference on Software and Computing Technology (ICSCT2010), vol. 2, pp. 36-38, Kunming, Chi