International Journal of Computer Engineering in Research Trends
Multidisciplinary, Open Access, Peer-Reviewed and fully refereed
Research Paper Volume-7, Issue-1,2020 Regular Edition E-ISSN: 2349-7084

A Novel Technique for Enhancement of the Security of Playfair Cipher

Sarita Singh*
Assistant professor, *Department of Computer Science and Engineering.*
Shri Ram Murti Smarak College of Engg & Tech, Bareilly AKTU, Luck now, India

er.sarita2014@gmail.com

Received: 06/01/2020, Revised: 10/01/2020, Accepted: 15/01/2020, Published: 28/01/2020

Abstract: - In today's world advancement of data transmission over the unsecured channel and data is not secure. In this scenario, data should be in encrypted form and that data transmitted over the network. In cryptography, have two methods to encrypt data are substitution and Transposition. Transposition is referring to changing the position of a character in the given text. On the other hand, Substitution is referring to replacing the character with another character in the given text. Play fair cipher is based on polyalphabetic substitution cipher; classical play fair cipher has a 5*5 matrix. To increase the security of play fair cipher, this paper presents a new approach to introducing double encryption in the sender side and double decryption in the receiver side approach by vigenere cipher, play fair cipher, and linear congruently method.

Keywords: play fair cipher, vigenere cipher, and linear congruential method.

1. Introduction

The relationship between 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 perfect security for transmission. And also, the implementation of the congruential generator method is straightforward. This paper presents a new approach, Encryption, and Decryption using Play fair Cipher and Vigenere Cipher; if we get ciphertext, then find numbers corresponds to ciphertext. In-play fair cipher, the alphabets are arranged in a 5x5 table based on a secret key, even though it is challenging 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 keystream value only, alphabets and numbers are arranged in a 6x6 table that is called play fair key matrix. The congruential generator method produces various random sequences; the number is filled in 6x6 tables. We use Vigenere cipher, Play fair cipher, and linear congruential generator method to enhance the security of classical play fair cipher. First, encrypt the plaintext by vigenere cipher with keyword and then result encrypt by play fair cipher with another keyword. We get the ciphertext. The linear congruential generator method generates an unpredictable sequence of numbers. This sequence of a number depends on the multiplier and increment. We were mapping the sequence number to ciphertext and find the corresponding sequence of numbers. We transmit a sequence of the number to the receiver instead of the alphabets.

At the receiver side, the receiver receives the sequence of numbers, and fined the ciphertext corresponds to a sequence of these numbers. First, decrypt the ciphertext by play fair cipher with the same encryption keyword and then result decrypt by vigenere cipher with the same encryption keyword. Then we get the original plaintext. This technique increases the security of play fair cipher. This sequence of the number depends on the multiplier and increment. We are

mapping the sequence number to ciphertext and find the corresponding sequence of numbers. We transmit a sequence of the number to the receiver instead of alphabets.

At the receiver side, the receiver receives the sequence of numbers, and fined the ciphertext corresponds to the sequence of these numbers. First, decrypt the ciphertext by play fair cipher with the same encryption keyword and then result decrypt by vigenere cipher with the same encryption keyword. Then we get the original plaintext. This technique increases the security of play fair cipher.

2. Play fair Cipher

The Play fair cipher uses a 5 x 5 table containing a keyword or phrase, as shown in Fig.1. 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 a ―*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 a ―*X*‖ after the first letter. Encrypt the new pair and continue.

2. If the letter appears 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 the 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).

3. 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 the 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 as long as the message. Usually, the key is a repeating keyword and also requires a keyword that the sender and receiver are known.

	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
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	P	Q
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

Figure 1:Vigenere Cipher

4. Linear Congruential Generators Method

The most widely used technique for the pseudo-random 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*
the multiplier *0<a<m*
c the increment 0=<c<m
X_0 the starting value or seed *0<= X_0<m*

The sequence of random number $\{X_n\}$ is obtained via the following iterative equation:

$X_n+1 = (aX_n+c) \text{mod} m$

If *m*, *a*, *c* and X_0 are integer, then this technique will produce a sequence of an integer with each integer in the range.

$0 <= X_n < m$.

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 X_0 *=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*.

5. Working of New Algorithm

The flowchart of the proposed approach is shown in the Fig. 2.

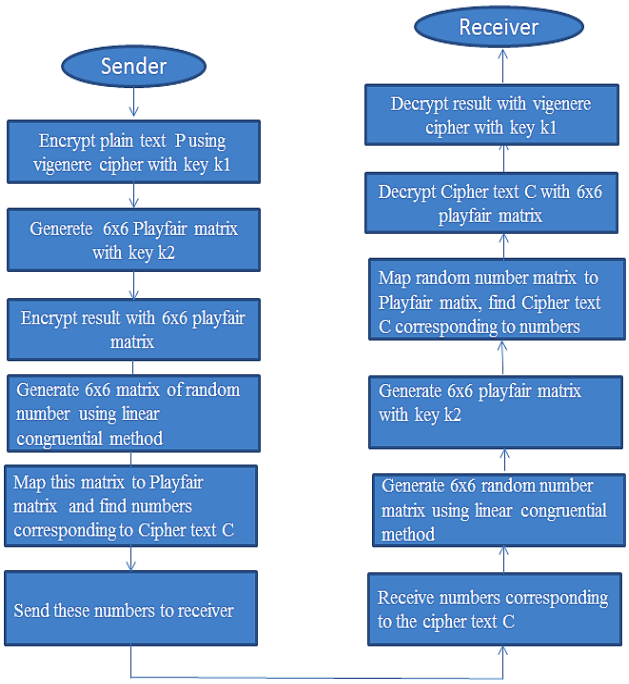

Figure 2: Flow Chart of the proposed methodology

5.1 Snapshot of the proposed methodology

The snapshot of the proposed approach is shown in Fig. 3-Fig.7.

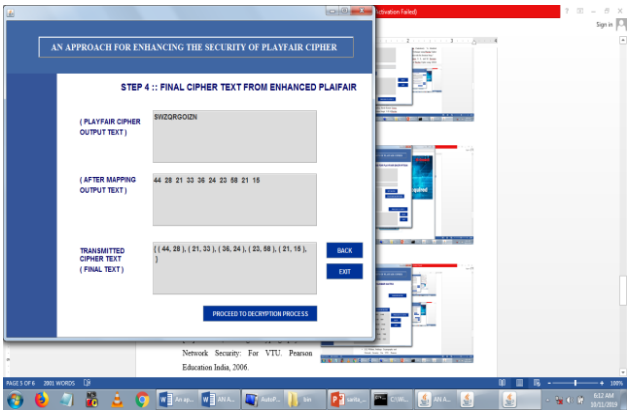

Figure 3. Final Ciphertext from Enhanced Playfair

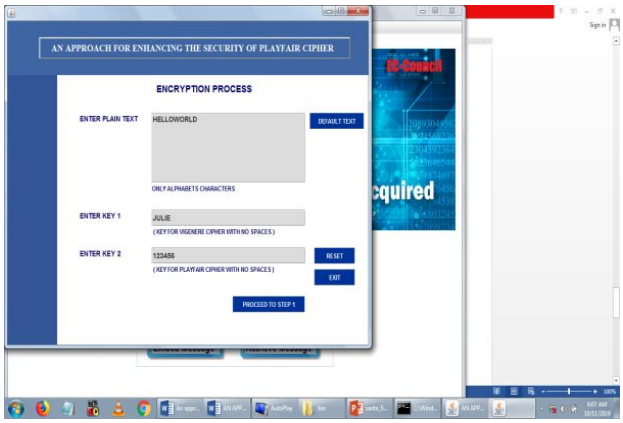

Figure 4. Encryption Process

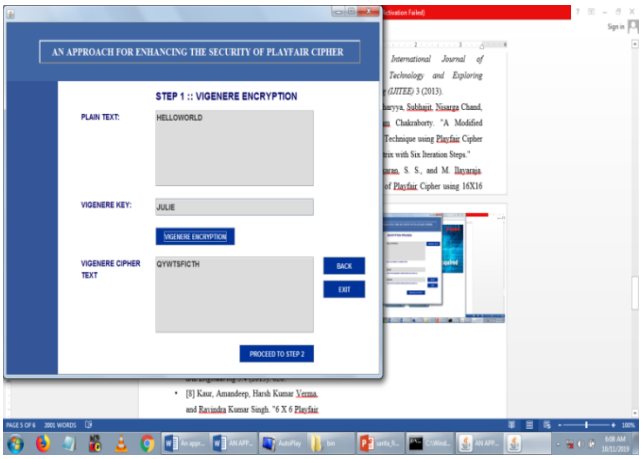

Figure 5. Vigenere Encryption

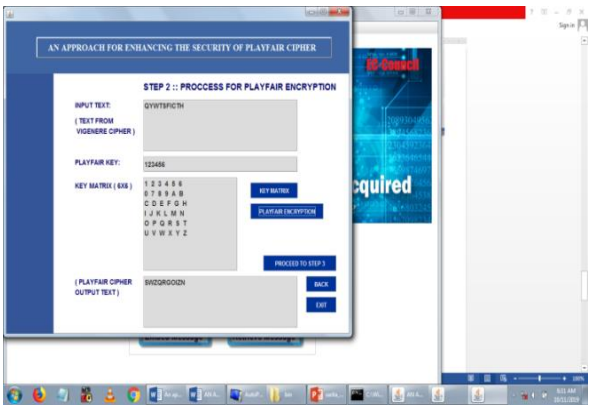

Figure 6. Processes for Playfair Encryption

Figure 7. Random Number matrix

6. Analysis of Proposed Method

The classical Play fair 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 the relationship between plaintext and ciphertext as complex as possible. Diffusion means to mask the statistical properties of data in the ciphertext. Our approach allows confusion, and diffusion can be easily incorporated into Vigenere cipher and Play fair Cipher. The linear congruential generator method can be used to generate random number sequences. Unpredictable different random sequences can be produced from a linear congruential generator method by varying multiplier and increment. Increasing modulus value can increase the cycle length. It can be easily implemented with the advent of a new computer. The implementation of the linear congruential generator method in hardware and software is very easy. The cost is very less, and also the speed is considered very high compared to other methods. This method of encryption does not increase the 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.

7. Conclusion

To implement modified Playfair cipher using random number generation. We use the linear congruential generator method that can be used to generate unpredictable

different random sequences by varying increments and multipliers. The classical Playfair cipher is not secure because it produces only 676 structures. We use vignette cipher and Playfair cipher for encryption and decryption. We are mapping random number sequences to ciphertext, and the corresponding number will be transmitted to the recipient instead of an alphabetical letter. This method increases the security of the transmission over the unsecured channel. Because we use 6x6 matrixes that produce 1296 structures and also use vigenere cipher that produces 456976. The total structures will be 1296*456966 = 592240896. The future work shall consider, to increases the size of the matrix to include the special character.

References:

[[1]Bhowmick, Anirban, Anand Vardhan Lal, and Nitish Ranjan. "Enhanced 6x6 Playfair Cipher using Double Myszkowski Transposition."*International Journal of Engineering Research and Technology*. Vol. 4. No. 07, July-2015. IJERT, 2015.

[2] Negi, Ashish, et al. "Cryptography Playfair Cipher using Linear Feedback Shift Register."*IOSR Journal of Engineering* 2.5 (2012): 1212-1216.

[3] Kumar, Vinod, et al. "Modified Version of Playfair Cipher Using Linear Feedback Shift Register and Transpose Matrix Concept'."*International Journal of Innovative Technology and Exploring Engineering (IJITEE)* 3 (2013).

[4] Bhattacharyya, Subhajit, Nisarga Chand, and Subham Chakraborty. "A Modified Encryption Technique using Playfair Cipher 10 by 9 Matrix with Six Iteration Steps."

[5] Dhenakaran, S. S., and M. Ilayaraja. "Extension of Playfair Cipher using 16X16 Matrix."*International Journal of Computer Applications* 48.7 (2012). [6] Basu, Sanjay, and Utpal Kumar Ray. "Modified Playfair Cipher using Rectangular Matrix."*IJCA (0975-8887) Volume* (2012)

[7]. Alam, A. Aftab, B. Shah Khalid, and C. Muhammad Salam. "A Modified Version of Playfair Cipher Using 7? 4 Matrix."*International Journal of Computer Theory and Engineering* 5.4 (2013): 626.

[8] Kaur, Amandeep, Harsh Kumar Verma, and Ravindra Kumar Singh. "6 X 6 Playfair Cipher using LFSR based Unique Random Number Generator."*International Journal of Computer Applications* 51.2 (2012).

[9] Murali, Packirisamy, and Gandhidoss Senthilkumar. "Modified version of Playfair cipher using a linear feedback shift register."*Information Management and Engineering, 2009. ICIME'09. International Conference on*. IEEE, 2009.

[10] Srivastava, Shiv Shakti, and Nitin Gupta. "Security Aspects of the Extended Playfair cipher."*Communication Systems and Network Technologies (CSNT), 2011 International Conference on*. IEEE, 2011.

[11] https://en.wikipedia.org/wiki/Pseudorandom_number_generator

[12] William, Stallings. Cryptography and Network Security: For VTU. Pearson Education, India, 2006.

