Modified Version of Playfair Cipher using Linear Feedback Shift Register

Packirisamy Murali[†] **and Gandhidoss Senthilkumar**[††],

[†]*Department of Computer Science and Engineering, Periyar Maniammai University, Thanjavur, 613403 India*
[††]*Department of Computer Applications, Periyar Maniammai University, Thanjavur, 613403 India*

Summary

In this paper we present a new approach for secure transmission of message by modified version of Playfair cipher combining with Random number generator methods. To develop this method of encryption technique, one of the simplest methods of random number generator methods called Linear Feedback Shift Register (LFSR) 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. Here we are mapping random numbers to secret key of Playfair cipher method 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, Random number, Linear Feedback Shift Register, Polyalphabetic cipher.

1. Introduction

The relationship of Cryptography and random numbers are investigated. Linear Feedback Shift Register is a good candidate for generating random numbers because logical circuit variations are high [1], [2], [3]. We can easily modify the LFSR and produce different random numbers. So it provides very good security for transmission. And also the software and hardware implementation of LFSR is very easy [9]. This paper presents a new approach with LFSR and Playfair cipher. 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 [4],[7]. In our approach, based on key stream value only, the plaintext is arranged in table ex: 5 X 5. The LFSR produce various random sequences, the bits are grouped ex: 5 or 4 or 6 bits and the table are filled with bits which are grouped previously. Finally the table values assigned to plaintext which is arranged in 5 X 5 tables and ciphertext will be produced based on Playfair cipher rules. And we are transmitting ciphertext values to receiver instead of alphabets.

2. The Playfair Cipher

In the 18th century, the Playfair cipher was first invented by Charles Wheatstone but it has heavily used and popular by Lord Playfair. This cipher mainly relied on polyalphabetic cipher. This method arranges the plaintext in table based on key value. This is illustrated as follows with key.

Key: CIPHER

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

There are only 26 letters; there is 26 X 26 = 676 diagrams will be produced so it was very difficult to identify the particular structure. It can be easily cracked if there is enough text. Calculating the key stream can be very easy if plaintext and ciphertext are known [2], [4], [7]. But today computer era, this method can be easily breakable by few seconds.

3. Linear Feedback Shift Register

A Linear Feedback Shift Register is a shift register whose input state is a linear function of its previous state.The only linear functions of single bits are XOR and inverse-XOR; thus it is a shift register whose input bit is driven by the exclusive-or (XOR) of some bits of the overall shift register value. The initial value of LFSR is called seed, the stream values produced by the register is completely determined by previous state. It can produce various random sequences by varying the taps [8],[11].The bit position that affects next state is called tap. This is illustrated as follows

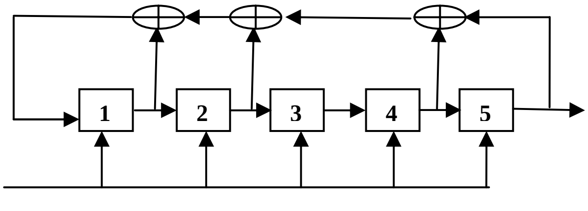

Fig 3.1 Feedback connections [5, 4, 2, 1], Feedback register of length m =5

In this circuit, at each pulse, the state of the flip-flop is shifted to the next one down the line and also computes Boolean function of the state of the flip-flops. The sequence produced by LFSR with m flip-flops cannot exceed 2^m-1. When the period is exactly 2^m-1, the sequence is called an m-sequence.

Feedback	**State of Shift Register**					**Output**
Symbol	**1**	**0**	**0**	**0**	**0**	**Symbol**
1	1	1	0	0	0	0
0	0	1	1	0	0	0
1	1	0	1	1	0	0
0	0	1	0	1	1	0
1	1	0	1	0	1	1
0	0	1	0	1	0	1
0	0	0	1	0	1	0
1	1	0	0	1	0	1
0	0	1	0	0	1	0
0	0	0	1	0	0	1

Table 3.2 maximal length sequence generated by the LFSR

Code: 0000110101.........................

LFSR can have multiple maximal length tap sequences. A maximal length tap sequence also describes the exponents in what is known as a primitive polynomial mod 2. For example, a tap sequence of 4, 1 describes the primitive polynomial x^4 + x^1 + 1. Modifying the taps and logical function in the Linear Feedback shift Register will produce the various random sequences.

4. Description of the New Algorithm

The new algorithm adds many advantageous over the normal Playfair cipher. It maps random sequences to plaintext in the secret key table before the message is encrypted by Playfair cipher. The amount of random sequences mapped to plaintext in the table is determined by how many bits are grouped. The output symbol code from above LFSR is 00001 10101 00100 01011 11101 10011 1 , m = 5. Increasing no of flip-flops can increase the cycle length. The output sequence bits are grouped, as follows; here 5 bits are grouped 00001, 10101, 00100, 01011, 11101, and 10011. The combined bits are filled in the table by using any rules followed in classical Playfair cipher.

29	1	11	4	1
11	19	4	29	21
4	29	1	21	19
29	21	19	4	11
1	19	11	1	21

Table 4.1: arrangement of code sequence from LFSR

Here m = 5, the initial state is 10000, so it will generate sequence 2^m-1. Here again, the generator returns to the initial state 10000 after 31 iterations. Next, plaintext filled in the table based on the key value. The code sequences from LFSR are mapped to plaintext in the table.

29	1	11	4	1
11	19	4	29	21
4	29	1	21	19
29	21	19	4	11
1	19	11	1	21

⇨

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

Table 4.2: Mapping of code sequence from LFSR to plaintext

Now the values of alphabets as follows

{C, I, P, H, E}	=	{29,1,11,4,1},
{R,A,B,D,F}	=	{11,19,4,29,21},
{G,K,L,M,N}	=	{4,29,1,21,19},
{O,Q,S,T,U}	=	{29,21,19,4,11},
{V,W,X,Y,Z}	=	{1,19,11,1,21}

Here, Encryption based on classical Playfair cipher. The proposed method follows the same rules and regulations.

Example:

Plaintext: hello

he → EC, lx → SP, lo → GS

Ciphertext:

{(E, C), (S, P), (G, S)} = {(1, 29), (19, 11), (4, 19)}
The transmitted ciphertext is {(1, 29), (19, 11), (4, 19)} instead of alphabetical letter. Decryption processes reverse of Encryption process.

5. Analysis of proposed method

This proposed methodology rapidly increases the security of the ciphertext. 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 [1],[2]. Our approach allows confusion and diffusion can be easily incorporated to Playfair Cipher. The LFSR can be used to generate random sequences. Unpredictable different random sequences can be produced from LFSR by varying logic functions and taps. Increasing no of registers can increase the cycle length. It can be easily implemented with advent of new computer. The implementation of LFSR 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.

6. Conclusion

This paper has attempted to implement modified Playfair cipher using Linear Feedback Shift Register. The classical Playfair cipher is not secure because it produces only 676 structures. With mapping of random sequences to classical Playfair cipher, increases the security of the transmission by many folds. Another approach to further enhance the security is to use high-dimensional chaotic or hyperchaotic systems such as the Rössler or the Lorenz systems.

References:

[1] Schnier B.”*Applied cryptography: protocols”, algorithms and source code in C.* New York: John Wiley and sons; 1996.

[2] Menezes AJ, Oorschot PCV , Vanstone SA . “*Handbook of applied cryptography”* . Boca Raton , Florida , USA : CRC Press ; 1997.

[3] Johannes A.Buchmann . *Introduction to Cryptography,* Second Edition 2001, Springer –Verlag NY, LLC

[4] Behrouz A. Forouzan. *Cryptography and Network Security,* Special Indian Edition 2007, The McGraw- Hill companies, New Delhi

[5] Dhiren R.Patel *“Information Security Theory and Practice”* First Edition,2008, Prentice-Hall of India Private Limited.

[6] Keith Harrison, Bill Munro and Tim Spiller “Security *through uncertainty “HP* Laboratories, February 2007.

[7] William Stallings, “ *Cryptography and Network Security Principles and Practice* “ Second edition, Pearson Education.

[8] Simon Haykin , “ *Communication Systems* “ , 4th Edition , Willey.

[9] Wayne Tomasi “Electronic *Communications System Fundamentals through Advanced* “, 5th edition, Pearson Education, 2008.

[10] http://en.wikipedia.org/wiki/Linear_feedback_shift_ register.html.

[11] http://homepage.mac.com/afj/lfsr.html.

PACKIRISAMY MURALI Murali P is a Senior Lecturer and Secretary E-GovPMU at Periyar Maniammai University, Thanjavur, India. He received a B.E degree in Computer science and Engineering from Bharathidasan University, Tamilnadu, India. And also received a M.Tech in Computer Science and Engineering from SASTRA, Tamilnadu, India . He presented many papers in National and International conferences and recently received a Best paper award in an International conference (ICDF2008) held at CIT, Coimbatore.

GANDHIDOSS SENTHIL KUAMR Senthilkumar G is a Senior Lecturer and Web Administrator at Periyar Maniammai University, Thanjavur, India. He received a M.C.A in Computer

Applications, from Bharathidasan University, TamilNadu, India. He presented many papers in National and International conferences and recently received a Best paper award in an International conference (ICDF2008) held at CIT, Coimbatore.