IOSR Journal of Engineering
May. 2012, Vol. 2(5) pp: 1212-1216

Cryptography Playfair Cipher using Linear Feedback Shift Register

*Dr. Ashish Negi (Associate Professor), [1] Jayveer Singh Farswan (Scholar), [2]
V.M Thakkar (Assistant Professor), [3] Siddharth Ghansala (Assistant Professor) [4]

Department of MCA G.B Pant Engineering College Pauri Garhwal Uttrakhand, INDIA[1]
Department of CSE, G. B Pant Engineering College Pauri Garhwal Uttrakhand, INDIA[2]
Department of CSE, G. B Pant Engineering College Pauri Garhwal Uttrakhand, INDIA[3]
Department of MCA G.B Pant Engineering College Pauri Garhwal Uttrakhand, INDIA[4]

Abstract: In this paper we present a new approach for secure transmission of message by modified version of Play fair 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. Play fair cipher method based on poly alphabetic cipher. It is relatively easy to break because it still leaves much of the structure and a few hundred of letters of cipher text are sufficient. Here we are mapping random numbers to secret key of Play fair 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*:* Play fair cipher, Random number; Linear Feedback Shift Register; Poly alphabetic cipher.

I. 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, and 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 Play fair cipher. In Play fair cipher, the alphabets are arranged in 8X8 table based on secret key, even though it is very difficult to break the cipher text 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: 8 X 8. 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 8 X 8 table and cipher text will be produced based on Play fair cipher rules. And we are transmitting cipher text values to receiver instead of alphabets. Different encryption techniques should be used to protect the confidential data from unauthorized use and in the mean time we also ensure that the characteristic of data on the sender side is preserved at the receiver side.

II. THE PLAYFAIR CIPHER

The well known multiple letter substitution cipher is the Play fair cipher. It is relatively easy to break because it still leaves much of the structure and a few hundred of letters of cipher text are sufficient. In the 18th century, the Play fair cipher was first invented by Charles Wheatstone but it has heavily used and popular by Lord Play fair. This cipher mainly relied on poly alphabetic cipher. This method arranges the plaintext in table based on key value.
This is illustrated as follows with key.

Key: CIPHER

S	H	I	V	@	A	E	R
B	C	D	F	G	J	K	L
M	N	O	P	Q	U	W	X
Y	Z	T	0	1	2	3	4
5	6	7	8	9	!	#	$
%	^	&	*	(	)	-	+
=	{	}	[	]	\	|	:
;	‘	,	<	>	/	.	?

Table 1 showing the CIPHER

There are only 26 letters; there is 26 X 26 = 676 Table 1 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 cipher text are known [2, 4, and 7]. But today computer era, this method can be easily breakable by few seconds.

III. 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 simplest kind of feedback shift register is a linear feedback shift register, or LFSR (as shown in Figure 1). The feedback function is simply the XOR of certain bits in the register and the list of these bits is called a tap sequence. LFSRs are the most common type of shift registers used in cryptography because they can be used as random number generators. Cryptographers like to analyze sequences to convince themselves that they are random enough to be secure.

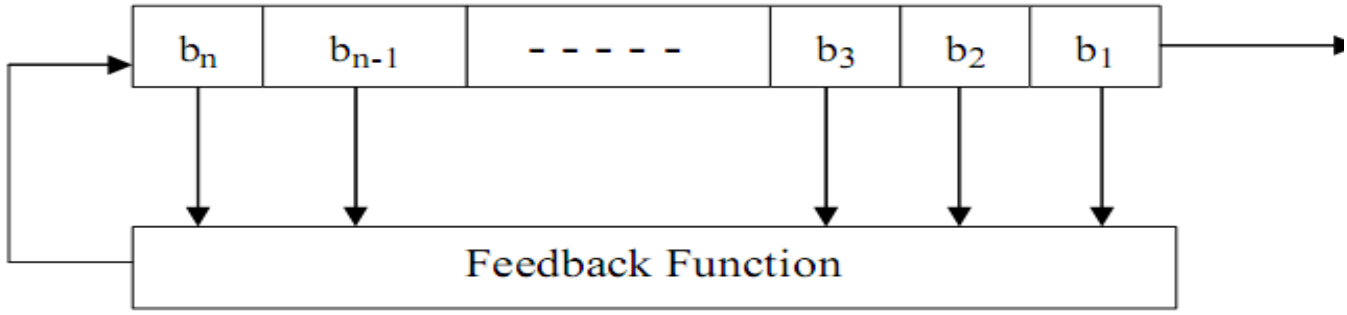

Figure 1 Feedback Shift Register

LFSRs are the most common type of shift registers used in Cryptography. 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

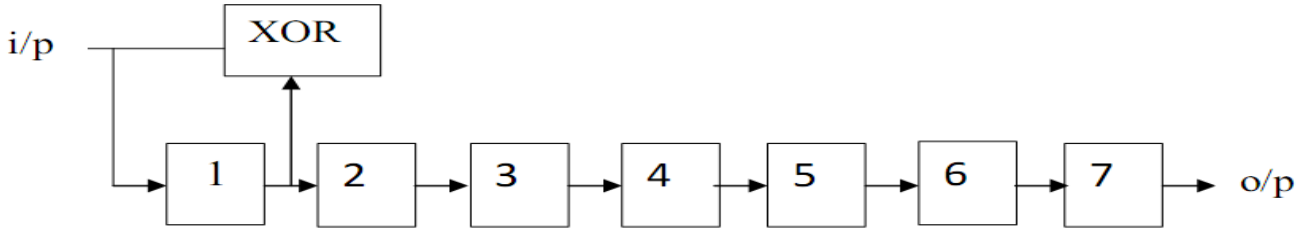

Figure 2 Feedback Shift Register

LFSR design used for implementation Feedback register of length m =8

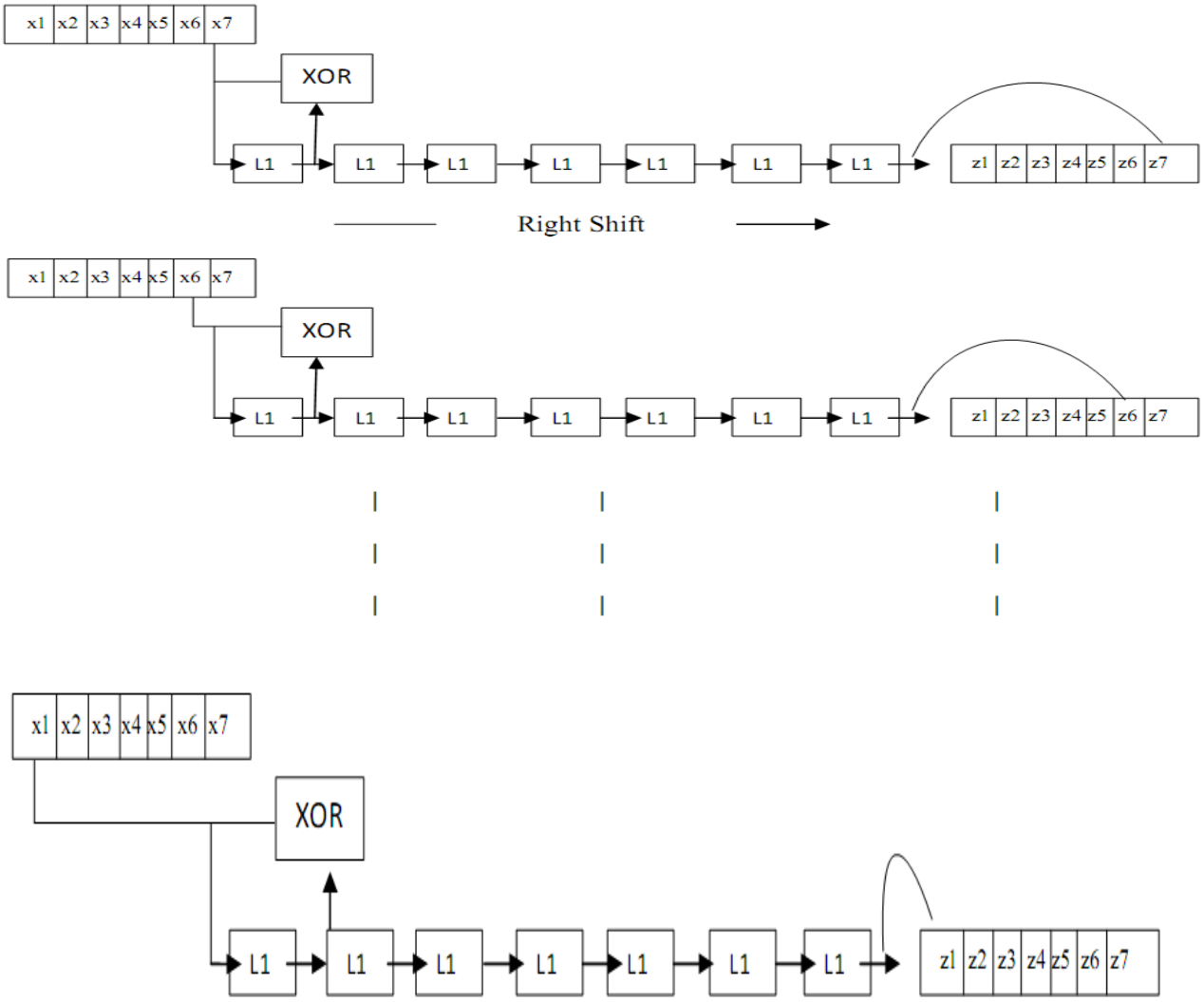

Figure 3 Feedback Shift Register

LFSR mechanisms for each of the 7-bits in this circuit, at each pulse, the state of the flip-flop is 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 2m-1. When the period is exactly 2m-1, the sequence is called an m-sequence.

IV. Proposed Cryptographic Algorithm

Encryption and Decryption algorithm play crucial role in cryptography. Strength of the security technique depends on the algorithm used for encryption and decryption. The well known multiple letter substitution cipher is the Playfair cipher. It is relatively easy to break because it still leaves much of the structure and a few hundred of letters of cipher text are sufficient. Here the diagrams in the plaintext are treated as single units and converted into corresponding cipher text diagrams. However because of the drawbacks inherent in the 8x8 Play fair cipher which adversely affects the security we propose an 8x8 Play fair cipher and then couple it with LFSR (Linear Feedback Shift Register) to make the traditional Play fair cipher at par with the advanced ciphers available like AES and DES. Now for all practical applications, performance and speed are also prime concerns besides security. The LFSR not only enhances the security up to a considerable level by generating random sequences but also provides a much faster rate of encryption and decryption. 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 cipher-text has to be as complex as

possible. Diffusion means mask the statistical properties of data in the cipher text. Our approach allows confusion and diffusion to be easily incorporated to Play fair Cipher. We have used LFSR to generate random sequences. Varying initial conditions with same LFSR can also increase the confusion in the encryption process. 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 compared to other methods. This method of encryption does not increase size of the cipher-text. For areas with low bandwidth or very less memory storage this method can be used.

V. ANALYSIS OF PROPOSED MODEL

In our model we will use 8x8 matrixes and hence, would use 64 grids. The proposed system would encrypt alphabets, numeral and special characters. It would also show space between words where required. This would use different blocks for different alphabet, numerals and symbols. In Proposed System, || will be used at the time of encryption to provide space between two words, ^ will be used for stuffing between two alphabets if they are repeated in a pair and ^ will also be used to put at the end to get the last alphabet in pair if the total length at comes out to be odd. At the time of decryption || will be
Replaced by blank space of one alphabet and the symbol ^ will be discarded. Rules for encoding and decoding will be same as that for existing play fair cipher.
Selecting JAY@FARSWAN as keyword we can have the matrix as follows.

S	H	I	V	@	A	E	R
B	C	D	F	G	J	K	L
M	N	O	P	Q	U	W	X
Y	Z	T	0	1	2	3	4
5	6	7	8	9	!	#	$
%	^	&	*	(	)	-	+
=	{	}	[	]	\	|	:
;	‘	,	<	>	/	.	?

Table 2 showing the matrix for selecting keywords

Consider a plaintext P consisting of 2n characters. By using the ASCII code, let us represent P in the form of a matrix given by P = [Pij], i=1 to n, j=1 to 2. Using the 8x8 matrix and the into corresponding cipher text us call this matrix as C.

$$C = \begin{bmatrix} C11 & C12 \\ C21 & C22 \\ . & . \\ . & . \\ Cn1 & Cn2 \end{bmatrix}$$

Now we convert each of these matrix els decimal. Let’s name this matrix as A.

$$A = \begin{bmatrix} A11 & A12 \\ A21 & A22 \\ . & . \\ . & . \\ An1 & An2 \end{bmatrix}$$

Now we convert each of these matrix elements into their corresponding binary values consisting of 7 bits as ASCII values range from 0 to 127. Let’s name this matrix as B.

$$B = \begin{bmatrix} b11 & b12 & . & . & b114 \\ b21 & b22 & . & . & b214 \\ . & . & . & . & . \\ . & . & . & . & . \\ bn1 & bn2 & . & . & bn14 \end{bmatrix}$$

Now for these binary sequences we have to apply LFSR in order to get the permuted sequence of bits. LFSR 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 [4, 7]. Initially we have to decide a seed value for the LFSR. Seed value is basically the initial values held in the register design. The seed value can even act as the secondary key in the cipher because any change in its value results in the change of overall output sequence. We make use of 7 bit LFSR with tapping applied at preferred places. The design of the LFSR and the seed value being known to the designer only, it adds another security parameter to our cipher.

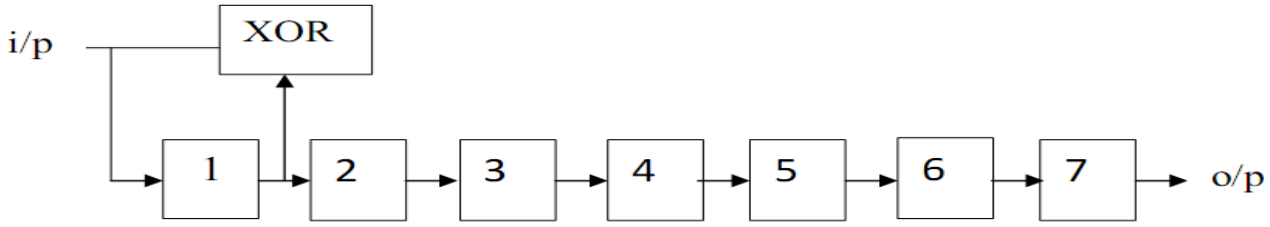

Figure 4 LFSR design used for implementation

VI. Conclusion

In this article we analysis and to develop this method of encryption technique for Cryptography Play fair Cipher using Linear Feedback Shift Register. one of the simplest methods of random number generator methods. It is relatively easy to break because it still leaves much of the structure and a few hundred of letters of cipher text are sufficient. Here we are mapping random numbers to secret key of Play fair 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. In this article gives effective result as compared to other shift register with new modified encryption cryptographic techniques.

References

[1] *William Stallings, Cryptography and Network Security Principles and Practice Fifth edition, Pearson Education. .*

[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, Springer –Verlag NY, LLC, 2001.*

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

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

[6] *Keith Harrison, Bill Munro and Tim Spiller, Security throughuncertainty. P Laboratories, February, 2007.*

[7] *William Stallings, Cryptography and Network Security Principles and Practice. Second edition, Pearson Education. Simon Haykin , Communication Systems. , 4th Edition, Willey.*

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

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

[10] *Samir Kumar Bandyopadhyay, Tuhin Utsab Paul and Avishek Raychoudhury,Genetic Algorithm Based Substitution Technique of Image Steganography. Volume1, No. 5, December 2010. Journal of Global Research in Computer Science Research Paper.*

[11] *V. Umakanta Sastry, N. Ravi Shankar, and S. Durga Bhavani, Modified Playfair Cipher Involving Interweaving and Iteration. International Journal of Computer.*