A Novel Approach to Security using Extended Playfair Cipher

Shiv Shakti Srivastava
Department of Computer Science and Engineering
National Institute of Technology
Hamirpur, India

Nitin Gupta
Department of Computer Science and Engineering
National Institute of Technology
Hamirpur, India

ABSTRACT
The well known multiple letter encryption cipher is the Playfair cipher. Here the digrams in the plaintext are treated as single units and converted into corresponding cipher text digrams. However because of the drawbacks inherent in the 5*5 Playfair cipher which adversely affects the security we proposed an 8*8 Playfair cipher. For details one can refer to [1]. This paper analyses the new proposed system. For this we have carried out cryptanalysis and through the avalanche effect we find out that the proposed cipher is a strong one.

Keywords
Playfair cipher, matrices, Special symbols, Random number, crptanalysis,brute force, Polyalphabetic cipher.

1. INTRODUCTION
The Playfair cipher shows a great advancement over the monoalphabetic ciphers. The identification of digrams is more difficult than individual letters. In the Monoalphabetic cipher, the attacker searches in 26 letters only. But by using the Playfair cipher, the attacker has to search in 26 x 26 = 676 diagrams. The relative frequencies of individual letters exhibit a much greater range than that of digrams, making frequency analysis much more difficult.

Some of the peculiarities of Playfair cipher can be-

- No plaintext letter can be represented in the cipher by itself.
- Any given letter can be represented by 5 other letters.
- Any given letter can represent 5 other letters.
- Any given letter cannot represent a letter that it combines with diagonally.
- It is twice as probable that the two letters of any pair are at the corners of a rectangle, than as in the same row or column.
- When a cipher letter has once been identified as a substitute for a plaintext letter, their is a 20% chance that it represents the same plaintext letter in each other appearance.

These peculiarities make the cryptanalysis of Playfair cipher an easy task. The cryptanalysis of the Playfair cipher is also aided by the fact that a diagram and its reverse will encrypt in a similar fashion. That is, if AB encrypts to XY, then BA will encrypt to YX [2][5]. So by looking for words that begin and end in reversed diagrams, one can try to compare them with plaintext words that are similar.

In recent investigation[1] we have modified the Playfair cipher by using 8*8 matrix along with LFSR for random number generation. In the present paper, we assume that the characters of the plaintext belong to the set of ASCII characters denoted by the codes 0 to 127. Here, our interest is to see that the strength of the cipher enhances significantly and no cryptanalytic attack would be possible on account of the modifications. For this we try to analyze all the drawbacks and security loopholes and provide a new cipher which is a strong one.

The section II of the paper deals with the related work where details of 8*8 matrix has been depicted. Section III shows the development of the cipher. Section IV gives a brief illustration of the cipher, section V involves with the cryptanalysis, section VI involves the Avalanche effect and finally in section VII we conclude.

2. RELATED WORK
In recent times [1] we extended the playfair cipher using 8*8 matrix and hence it would be using 64 grids. The proposed system not only encrypts the alphabets but also the numerals and special characters. It also shows space between words where required. The system uses different blocks for different alphabet, numerals and symbols. In Proposed System, | is used at the time of encryption to provide space between two words, ^ is 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 playfair cipher.

Selecting SHIV@SHAKTI as keyword we can have the matrix as follows.

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

We can now use this matrix for encryption and decryption purpose. Instead of having 26*26 digrams the attacker has to now search in 64*64=4096 digrams. This surely increases the resistance to brute force attack.

Frequency Analysis-

On an average,the probability of occurrence of any particular element in 5*5 Playfair matrix is 1/26=0.0384.Whereas the probability of occurrence of an element in 8*8 playfair matrix is 1/64=0.0156. This value is far less when compared and frequency analysis is now a tougher job.

3. DEVELOPMENT OF THE CIPHER

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.

$$P = \begin{bmatrix} P11 & P12 \\ P21 & P22 \\ . & . \\ . & . \\ Pn1 & Pn2 \end{bmatrix}$$

Using the 8*8 matrix and the defined keyword we can convert this plaintext matrix(P) into corresponding cipher text matrix taking each row elements together as digrams. Let us call this matrix as C.

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

Now we convert each of these matrix elements into their corresponding ASCII values in decimal. Lets 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.

In this paper we have used the following LFSR design-

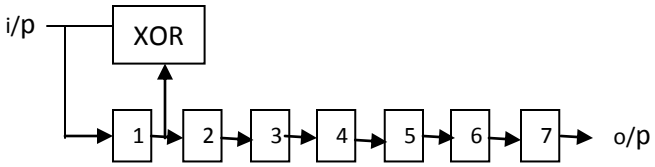

Fig 1. LFSR Design

Description of the LFSR mechanism-

Since we are using seven bit LFSR so let us name each bit in LFSR(L) as l1,l2,l3,l4,l5,l6,and l7. Each of the element in matrix A when converted to equivalent binary assumes the form given in matrix B. We take these binary equivalents for all the elements as the input sequence to the LFSR and name it X where

X{x1,x2,x3,x4,x5,x6,x7} = binary equivalent for every Aij .

Since LFSR only shifts the bits and there is no change in the number of output bits therefore we can store output sequences for each 7 bit input into Z where

Z = {z1,z2,z3,z4,z5,z6,z7}.

Procedure followed for each element Aij goes like-

Initially i=1
While(i<=7)
{
z[8-i]=l[7];
Shift bits in L to right directions i.e. l7=l6,l6=l5,…….,l2=l1.
l[1]=l[1] xor x[8-i]
increment i
}

Once we are finished with this LFSR process we get the corresponding 7 bit permuted binary sequences for each of the seven bit binary input. These binary sequences when converted to decimal give us the final cipher text which is represented as matrix CT, shown below.

$$CT = \begin{bmatrix} ct11 & ct12 \\ ct21 & ct22 \\ . & . \\ . & . \\ ctn1 & ctn2 \end{bmatrix}$$

We present the schematic diagram of the encryption and decryption. OPOL is the overall process of LFSR and has been

illustrated at the end of the paper. The overall process of encryption goes like-

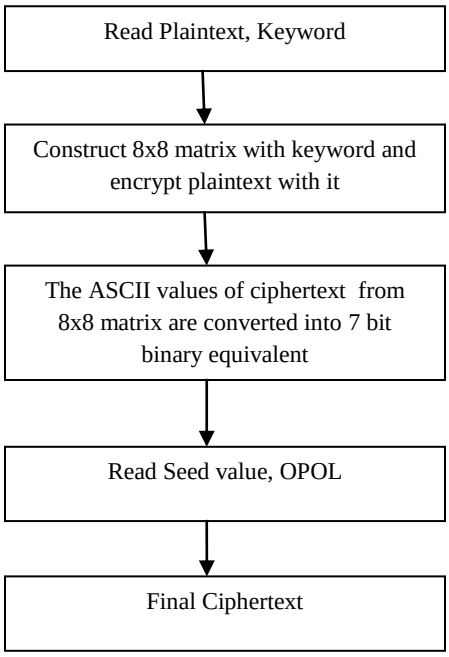

Fig 2: Encrytion

The process of decryption is the reverse of encryption and it goes like-

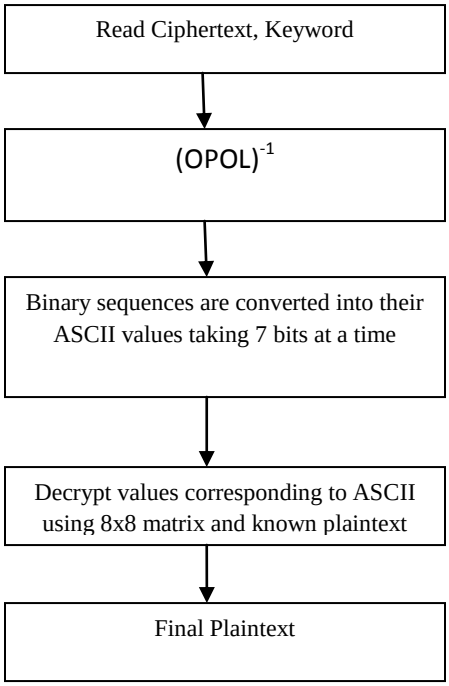

Fig 3: Decrytion

4. ILLUSTRATION OF THE CIPHER

Consider the following plaintext.

The man who acquires the habit of reading when he is young is happy.

Firstly we have to append |symbol at blank spaces.

T he plaintext becomes

The| man| who |acquires| the| habit| of| reading| when |he |is| young| is| happy.

For simple illustration we have focused on the first sixteen characters of plaintext, i.e.

The|man|who| acqu

Encrypting this plaintext using the proposed 8*8 Playfair cipher and using the keyword SHIV@SHAKTI, (consider the table in section II),we get.

SIJ[RSU{NTO}HGRW

Arranging this into 8*2 matrix we get

$$C = \begin{bmatrix} S & I \\ J & [\\ R & S \\ U & \{ \\ N & T \\ O & \} \\ H & G \\ R & W \end{bmatrix}$$

Replacing elements of C with corresponding ASCII codes we get.

$$A = \begin{bmatrix} 83 & 73 \\ 74 & 91 \\ 82 & 83 \\ 85 & 123 \\ 78 & 84 \\ 79 & 125 \\ 72 & 71 \\ 82 & 87 \end{bmatrix}$$

Replacing elements of A with their equivalent binary value we get the matrix B as

$$B = \begin{bmatrix} 1&0&1&0&0&1&1&1&0&0&1&0&0&1 \\ 1&0&0&1&0&1&0&1&0&1&1&0&1&1 \\ 1&0&1&0&0&1&0&1&0&1&0&0&1&1 \\ 1&0&1&0&1&0&1&1&1&1&1&0&1&1 \\ 1&0&0&1&1&1&0&1&0&1&0&1&0&0 \\ 1&0&0&1&1&1&1&1&1&1&1&1&0&1 \\ 1&0&0&1&0&0&0&1&0&0&0&1&1&1 \\ 1&0&1&0&0&1&0&1&0&1&0&1&1&1 \end{bmatrix}$$

After applying LFSR (shown in section III) the permuted values of B are

$$B' = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Converting this matix element into binary equivalent we get the 8*2 matrix as-

$$CT = \begin{bmatrix} 85 & 78 \\ 56 & 70 \\ 54 & 73 \\ 68 & 76 \\ 86 & 69 \\ 51 & 65 \\ 84 & 71 \\ 66 & 49 \end{bmatrix}$$

CT is the final cipher text. Decryption process is just the reverse of the encryption and we get back to the plaintext easily.

5. CRYPTANALYSIS

In cryptolography, the different types of cryptanalytic attacks are (1) Ciphertext only (Brute force) attack, (2) Known plaintext attack and (3) Chosen plaintext/ciphertext attack.

In the example illustrated in section IV of this paper, the length of the ciphertext in is 16*7=112 binary bits and the length of the plaintext is also 112 bits. Thus, in order to arrive at the cipher text, thesize of the plaintext space which is to be searched is$2^{112}(\approx 10^{33.6})$. The time required for this is enormously large. Hence, this sort of ciphertext only attack is ruled out.

The plaintext is known at the beginning whereas the ciphertext at the end and in the between we have the procedure which not only includes substitution through 8*8 cipher but also randomization through LFSR.Therefore thecorrelation between plaintext and ciphertext is not possible. Thus,breaking the cipher in the case of the known plaintext attackalso is impossible.

We may therefore conclude that no combination of the plaintext or the ciphertext will help the cryptanalyst to break the cipher.

6. AVALANCHE EFFECT

The input given to LFSR in the example assumes the following binary representation.

10100111001001100101010111011101001010100111010101111
1011***1001110***10101001001111111111011001000100011110100101010111 . (X)

Now we simply change the ninth character in C1 (which acts as plaintext to LFSR) from N to O.This results in a one bit change in the input to LFSR.

The binary representation now assumes the form-

10100111001001100101110110111010010101001110101011111
1011***1001111***10101001001111111111011001000100011110100101010111. (Y)

The output sequence corresponding to (X) and (Y) are –

10101011001110011100010001100110110100111010011101001
10011001011010001010110011100000110101001000111100001
00110001.

And

10101011001110011100010001100110110100111010011101001
10011001011001110101001100011101001010110111000011110
11001110.

These output sequences differ by 48 bits which is quite substantial. This shows and proves that the cipher is a strong one.

7. CONCLUSION

In this paper, we have analyzed the modifications made in Playfair cipher. The modifications firstly include going for 8*8 matrix to overcome the problems in traditional Playfair cipher and then using LFSR to make use of the concept of random numbers. In the case of the traditional Playfair cipher, while each two characters undergo transformation into two characters only, in the present analysis we find out that now there is a lot of confusion and diffusion inherent. The algorithms governing the encryption and the decryption are implemented in C++ language.

Considering the analysis made, we find that the proposed cipher is a very strong one and it cannot be broken by any cryptanalytic attack. The analysis can be verified on plaintext of any size. For areas with low bandwidth or very less memory storage this method would be very effective.

8. REFERENCES

[1] Shiv Shakti Srivastava, Nitin Gupta and Rajaram jaiswal *"Modified Version of Playfair Cipher by using 8x8 Matrix and Random Number Generation"* in Proceedings of IEEE 3rd International Conference on Computer Modeling and Simulation (ICCMS 2011), Mumbai, pages 615-617, January, 2011.

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

[3] 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

[4] Packirisamy Murali and Gandhidoss Senthilkumar, Modified version of Playfair cipher using Linear Feedback Shift Cipher, International Conference on Information Management and Engineering ICIME,pp.488-490,2009.

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

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

[7] Dhiren R.Patel, Information Security Theory and Practice. First Edition, Prentice-Hall of India Private Limited, 2007

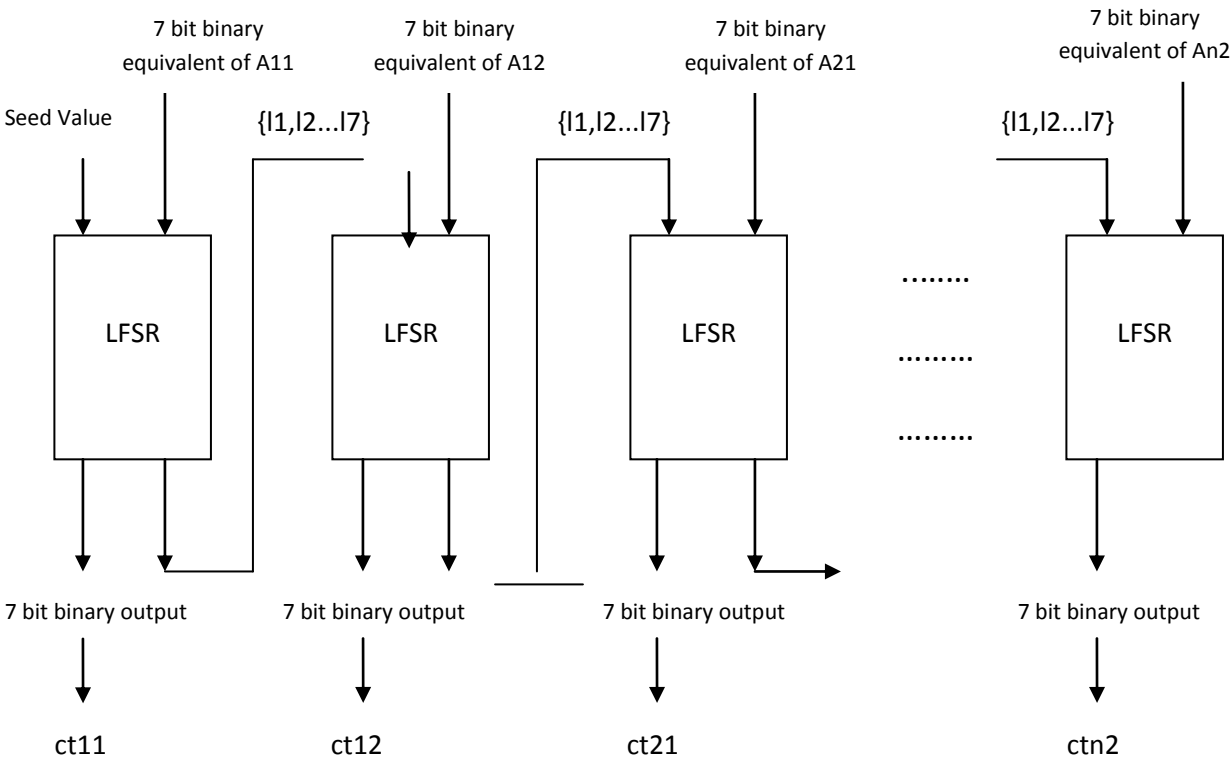

Fig 4: OPOL (Overall Process of LFSR)