International Journal of Computer Theory and Engineering, Vol. 1, No. 5, December, 2009
1793-8201

A Modified Playfair Cipher Involving Interweaving and Iteration

V. Umakanta Sastry, N. Ravi Shankar, and S. Durga Bhavani

***Abstract*— In this investigation, we have generalized and modified the Playfair cipher into a block cipher. Here, we have introduced substitution, interweaving and iteration. The cryptanalysis and the avalanche effect carried out in this analysis markedly indicate that the cipher is a strong one, and it cannot be broken by any cryptanalytic attack.**

***Index Terms*— interweaving, inverse interweaving, substitution matrix.**

I. Introduction

In all the classical ciphers, Playfair cipher [1] is a simple and interesting one. In this, every block consisting of two characters (digrams) is mapped into another block of two characters by applying a set of rules. Here, we use a square matrix of size 5x5 to accommodate all the 26 characters in the English alphabet, in an appropriate manner. Firstly, a chosen keyword (containing distinct characters) is placed, in the matrix, in a row wise manner. Then, excluding the characters in the keyword, the rest of the English characters are placed in the remaining places of the matrix, of course, by accommodating a pair of letters in the same place. Selecting MONARCHY as the keyword, a typical square matrix can be formed as follows:

$$\begin{bmatrix} M & O & N & A & R \\ C & H & Y & B & D \\ E & F & G & I/J & K \\ L & P & Q & S & T \\ U & V & W & X & Z \end{bmatrix}$$

A plaintext is encrypted, taking two letters at a time, according to the following rules.

1. Repeating plaintext letters that would fall in the same pair are separated with a filler letter, such as x, so that *balloo*n would be treated as *ba lx lo on*.
2. Plaintext letters that fall in the same row of the matrix are each replaced by the letter to the right with the first element of the row circularly following the last. For example, *AR* is replaced with *RM*.
3. Plaintext letters that fall in the same column are each replaced by the letter beneath with the top element of the column circularly following the last. For example, *MU* becomes *CM*.
4. Otherwise, each plaintext letter is replaced by the letter that lies in its own row and column occupied by the other plaintext letter. Thus, *HS* becomes *BP* and *EA* becomes *IM* or *JM* as the encipherer wishes.

Though, this cipher enjoyed its prominence up to the middle of the last century, subsequently, with the advent of computers, it was found to be breakable with some amount of computation, as the structure of the plaintext is not that much dissipated in the corresponding ciphertext.

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, we construct a substitution table in an appropriate manner (see section 2) and modify the rules 1 to 4, suitably, for encryption and decryption. Further, we introduce interweaving (explained later) and iteration which will lead to a lot of confusion and diffusion. 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.

In section II, we present the development of the cipher. We design the algorithms for encryption, decryption, interweaving, and inverse interweaving in section III. In section IV, we illustrate the cipher with an example. We discuss the cryptanalysis in section V, and mention the avalanche effect in section VI. Finally, in section VII, we draw conclusions.

II. 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

$P = [P_{ij}]$, i=1 to n, j=1 to 2.
(1)

Let us take a key K, consisting of 64 distinct numbers, denoted by K_i, i=1 to 64, where each number lies between 0 and 127. Excluding these numbers, from the ASCII codes 0 to 127, the remaining numbers, arranged in their ascending order, be represented as R_i, i=1 to 64.

Then, the substitution matrix is shown in (2).

Let us consider a pair of characters, denoted by P_1, P_2. Let them be represented in terms of their ASCII code, say A_1, A_2.

V. Umakanta Sastry is with the Department of Computer Science and Engineering, Sreenidhi Institute of Science and Technology, India. Phone:919985012707, fax:914027640394, e-mail: vuksastry@rediffmail.com.

N. Ravi Shankar is with the Department of Computer Science and Engineering, Sreenidhi Institute of Science and Technology, Hyderabad, India.

S. Durga Bhavani is with the School of Information Technology, J.N.T. University, Hyderabad, India.

Then, the set of rules 1 to 4, mentioned in section I, can be modified as follows:

1. If $A_1=A_2$ (i.e. both the numbers are the same), then we replace both A_1 and A_2 by the number occurring in the same row and in the next column of A_1 in the substitution matrix. For example, K_{39}, K_{39} will be replaced by K_{40}, K_{40}.
2. If A_1 and A_2 are distinct and fall in the same row of the substitution matrix, then each of these numbers is replaced by the number that exists in the same row and in the next column of that number, with the first element of the row following, circularly, the last element of the row. For example, R_{31}, R_{32} is replaced by R_{32}, R_{17}.
3. If A_1 and A_2 are distinct and fall in the same column of the substitution matrix, then each of these numbers is replaced by the number that exists in the same column and in the next row of that number, with the first element of the column following.

Circularly, the last element of the column. For example, R_{45}, R_{61} is replaced by R_{61}, K_{13}.

4. If A_1 and A_2 are distinct and fall in different rows and columns of the substitution matrix, then A_1 is replaced by the number that exists in the same row as A_1 and in the column of A_2, and A_2 is replaced by the number that exists in the same row as A_2 and in the column of A_1. For example, K_{36}, R_{41} is replaced by K_{41}, R_{36}.

Now, let us consider the pair of numbers P_{11} and P_{12}, the first row of the plaintext matrix P. On adopting the rules 1 to 4, mentioned above, let us map these numbers (by using the substitution matrix) into a pair of numbers, denoted by P_{11}^1, P_{12}^1. Similarly, the elements of each row of the entire matrix P (row wise) are mapped into their corresponding numbers. Thus we get the new matrix

$P^1 = [\,P_{ij}^1\,]$, i = 1 to n, j = 1 to 2.

(3)

We now introduce the process of interweaving. On converting the elements of P^1 into their binary form, we get

$$b = \begin{bmatrix} b_{11} & b_{12} & \dots & b_{114} \\ b_{21} & b_{22} & \dots & b_{214} \\ . & . & \dots & . \\ . & . & \dots & . \\ b_{n1} & b_{n2} & \dots & b_{n14} \end{bmatrix}$$

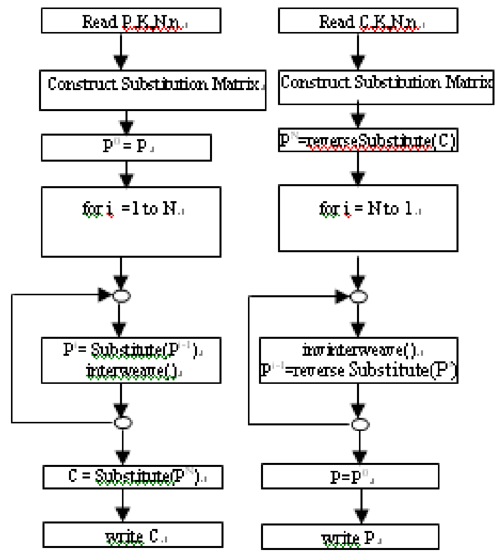
Let us rotate the first column so that it assumes the form $[b_{21},b_{31},\dots b_{n1},b_{11}]^T$, where T denotes the transpose of the vector. In view of this, all the elements of the first column are moved up by one step and the first element occupies the last position in the column. Same procedure is adopted on all the odd numbered columns. Let us now apply left circular rotation, by one position, on all the even numbered rows. Thus, the matrix assumes totally a modified form, given by

$$b = \begin{bmatrix} b_{21} & b_{12} & b_{23} & \dots & b_{213} & b_{114} \\ b_{22} & b_{33} & b_{24} & \dots & b_{214} & b_{31} \\ . & . & . & . & . & . \\ . & . & . & . & . & . \\ . & . & . & . & . & . \\ b_{n2} & b_{13} & b_{n4} & \dots & b_{n14} & b_{11} \end{bmatrix}$$

We now convert the binary bits into decimal numbers by taking seven bits at a time in a row wise manner. Thus we get the new P^1, having n rows and 2 columns. This completes the process of interweaving and ends up the first round of iteration. We denote the reverse process of interweaving as inverse interweaving and that of substitution as reverse substitution.

We repeat the above process and carryout the iteration.

We present the schematic diagram of the encryption and the decryption in Fig. 1.



a) Encryption b) Decryption

Fig. 1. Schematic diagram of the cipher

In this analysis, N denotes the number of iterations and it is taken as 16.

III. Algorithms

A. Algorithm for Encryption

1. read n,N,K,P;
2. Construct Substitution matrix
3. $P^0 = P$;
4. for i=1 to N {
   P^i = Substitute(P^{i-1});
   interweave();
   }
5. C = Substitute(P^N);
6. write C;

B. Algorithm for Decryption

1. read n,N,K,C;
2. Construct Substitution matrix
3. P^N =reverse substitute(C);
4. for i=N to 1 {
   invinterweave();

```
        P^(i-1) = reverse substitute(P^i);
    }
5. P=P^0;
6. write P;
```

C. Algorithm for Interweave

```
1.construct [b_ij],i=1ton,j=1to14 from P;
2. for j=1 to 14 in step 2 {
    k=b_1j;
        for i=1 to n-1{
            b_ij=b_(i+1)j;
        }
        b_nj=k;
    }
3. for i=2 to n in step 2 {
        k=b_i1;
        for j=1 to 13 {
            b_ij=b_i(j+1);
        }
        b_i14=k;
    }
4. Construct P from b_ij;
```

D. Algorithm for Invinterweave

```
1. construct [b_ij], i=1ton, j=1to14 from P;
2. for i= n to 2 in step 2 {
        k=b_i14;
        for j= 14 to 2{
            b_ij=b_i(j-1);
        }
        b_i1=k;
    }
3. for j = 13 to 1 in step 2{
    k=b_nj;
    for i= n to 2 {
        b_ij=b(_(i-1)j);
    }
    b_1j=k;
    }
4. Construct P^i from b_ij;
```

IV. Illustration of the Cipher

Let us consider the plaintext, given below.

I do not Know why the rich people do not care our voices and heart burnings. They will come to know only when their stomachs flare up with hunger. It wont happen! Let us dig graves for all those rich in all parts of the country. Then only we will have peace.

(4)

To have a simple illustration, let us focus our attention on the first sixteen characters given by

I do not Know wh

(5)

On substituting the ASCII codes for these characters, and arranging them in the form of a matrix of size 8x2, we get

$$P = \begin{bmatrix} 73 & 32 \\ 32 & 75 \\ 100 & 110 \\ 111 & 111 \\ 32 & 119 \\ 110 & 32 \\ 111 & 119 \\ 116 & 104 \end{bmatrix} \qquad (6)$$

The substitution matrix, described in section II, is given in (7).

On applying the substitution process (see section II) on the elements of P, we get the modified P, denoted by P^1, as

$$P^1 \begin{bmatrix} 32 & 34 \\ 75 & 92 \\ 101 & 123 \\ 83 & 83 \\ 67 & 8 \\ 92 & 70 \\ 18 & 37 \\ 113 & 96 \end{bmatrix} \qquad (8)$$

On converting the elements of P into their binary representation, we get

$$b=\begin{bmatrix} 0&1&0&0&0&0&0&0&1&0&0&0&1&0 \\ 1&0&0&1&0&1&1&1&0&1&1&1&0&0 \\ 1&1&0&0&1&0&1&1&1&1&1&0&1&1 \\ 1&0&1&0&0&1&1&1&0&1&0&0&1&1 \\ 1&0&0&0&0&1&1&0&0&0&1&0&0&0 \\ 1&0&1&1&1&0&0&1&0&0&0&1&1&0 \\ 0&0&1&0&0&1&0&0&1&0&0&1&0&1 \\ 1&1&1&0&0&0&1&1&1&0&0&0&0&0 \end{bmatrix} \quad (9)$$

On applying the process of interweaving described in section 2, we get the modified b. Thus we have

$$b=\begin{bmatrix} 0&0&1&0&1&0&1&1&1&0&1&1&0&0 \\ 1&1&0&0&0&0&1&1&0&1&1&0&0&1 \\ 0&0&0&1&1&1&1&1&1&1&0&1&1&1 \\ 1&0&1&0&0&1&1&0&0&0&0&0&1&0 \\ 0&0&1&0&0&1&1&0&0&1&1&0&0&1 \\ 1&0&1&0&1&1&0&0&0&0&0&1&1&1 \\ 1&1&0&0&0&0&1&1&0&0&0&0&0&0 \\ 1&1&1&0&0&0&1&0&1&0&0&0&0&0 \end{bmatrix} \quad (10)$$

We now convert these binary numbers into their corresponding decimal numbers, and construct the modified P^1, as

$$P^1 \begin{bmatrix} 21 & 108 \\ 97 & 89 \\ 15 & 119 \\ 83 & 2 \\ 19 & 25 \\ 86 & 7 \\ 97 & 64 \\ 113 & 32 \end{bmatrix}$$

(11)

After carrying out all the sixteen iterations, we get the ciphertext in the form

$$C = \begin{bmatrix} 114 & 50 \\ 118 & 110 \\ 127 & 21 \\ 119 & 23 \\ 7 & 73 \\ 10 & 45 \\ 76 & 66 \\ 111 & 5 \end{bmatrix}$$

(12)

Now, let us consider the process of decryption.

On taking the C given in (12), and applying the reverse substitution process, we get

$$P^N = \begin{bmatrix} 4 & 83 \\ 60 & 97 \\ 106 & 25 \\ 99 & 18 \\ 25 & 48 \\ 114 & 33 \\ 84 & 34 \\ 44 & 18 \end{bmatrix}$$

(13)

On applying the inverse interweaving process, we get the transformed P^N as

$$P^N = \begin{bmatrix} 104 & 56 \\ 22 & 33 \\ 125 & 73 \\ 97 & 6 \\ 38 & 24 \\ 88 & 112 \\ 34 & 1 \\ 46 & 19 \end{bmatrix}$$

(14)

Following the same procedure, after carrying out all the sixteen iterations, we get the plaintext P in the form

$$P = \begin{bmatrix} 73 & 32 \\ 32 & 75 \\ 100 & 110 \\ 111 & 111 \\ 32 & 119 \\ 110 & 32 \\ 111 & 119 \\ 116 & 104 \end{bmatrix} \qquad (15)$$

This is the same as the plaintext given in (6).

The ciphertext corresponding to the entire plaintext given in (4), in its hexadecimal notation, can be obtained as
E5DBFF70E2A66F65B8A9792B6105FC8FB3097ACCA93
8982C3B6437A57299E6A042AB38AA02E70162EB2F5F2
7038A0F9AE25CBE667984B998D37C4BDDBC1F18795B
9F159FD4AF99D38A62DAB5660A5CA65FEA72F7D49C
044CCE5F989620392A1B033D5C055EE9591CD3C4DAE
9B8A2AAC8394FE29A84C62C2BE2BE5170841B310653
E04C496F456C132B76AAA2.

V. Cryptanalysis

In the science of cryptology, 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 of this block cipher, as the length of the ciphertext block is 112 bits, the length of the plaintext block is also 112 bits. Thus, in order to arrive at the cipher text, the size of the plaintext space which is to be searched is 2^{112}($\approx 10^{33.6}$), i.e., we have to carryout computation with 2^{112} plaintext blocks. The time required for this is enormously large. Hence, this sort of ciphertext only attack is ruled out.

As the key is chosen to contain 64 distinct numbers between 0 and 127, the number of possible keys is ${}^{128}P_{64}$. As the rest of the numbers (between 0 and 127, excluding the numbers in the key) are arranged in their ascending order, the possible number of substitution matrices is ${}^{128}P_{64}$. As this number is also very large, finding the substitution matrices in all these cases is a formidable task. Hence, brute force attack of this type also is impossible.

We know the plaintext at the beginning of the iterative procedure, and the ciphertext at the end of the iteration. And in between, as we have several transpositions on account of substitution and interweaving, correlating directly the plaintext and the ciphertext is no way a possible job. Thus, breaking the cipher in the case of the known plaintext attack also is impossible.

Lastly, we envisage that no special choice of the plaintext or the ciphertext will help the cryptanalyst to break the cipher.

VI. Avalanche Effect

The plaintext P given in (6), in its binary representation, assumes the form
1001001010000011001001101111010000011011101101111
1111010001000000100101***1101110***1101111111011101000
0011101111101000.
(16)

On changing the eleventh character in the above plaintext from **n** to **o** (i.e., from the ASCII code 110 to 111), the plaintext takes the form
1001001010000011001001101111010000011011101101111
1111010001000000100101***1101111***1101111111011101000
0011101111101000.
(17)

It may be noted that the plaintexts given in (16) and (17) differ by one bit. The ciphertexts corresponding to the above plaintexts are
111001011101101111111111011100001110001010100110
011011110110010110111000101010010111100100101011

0110000100000101
(18)

and

110110001001110111100101110000001001110001011100
110001101011100001011010110110010011110110001011
0100100111110110.
(19)

It can be readily noticed that the ciphertexts given in (18) and (19) differ by 55 bits, which is quite significant.

We now change the key element K_{45} from 3 to 2. With this change, the key under consideration changes by one bit. If we apply the modified key on the plaintext given in (6), we get the corresponding ciphertext as

111011110111111110110010111101111110101100000111
100111111100111010010110101001111001101011010100
1000100000010110.
(20)

It can be seen that the ciphertexts given in (18) and (20) differ by 55 bits, which is a large departure.

From the above analysis, we conclude that the cipher is a strong one.

VII. Conclusions

In this paper, we have devoted our attention to a modification of the Playfair cipher by introducing interweaving and iteration. In the case of the Playfair cipher, while each two characters undergo transformation into two characters only, in the present analysis as the substitution, interweaving and iteration cause a lot of confusion and diffusion, the plaintext gets modified as a whole as a block.

The algorithms governing the encryption and the decryption are implemented in C language.

The time required for the encryption of the entire plaintext given in (4) is 10.3×10^{-3} seconds and time for the decryption is 10.3×10^{-3} seconds.

In the light of this analysis, we find that the block cipher under consideration is a very strong one and it cannot be broken by any cryptanalytic attack.

This analysis can be extended to the case of a plaintext block of any size.

References

[1] 1. William Stallings, "Cryptography and Network Security: Principles and Practices", Third edition, Chapter 2, pp.35.

[2] Biographical notes:

[3] V. Umakanta Sastry was formerly a professor at Indian Institute of Technology, Kharagpur, India. Presently he is the Director, School of Computer Science and informatics and Dean (R&D) at Sree Nidhi Institute of Science and Technology, Hyderabad, India. He is currently guiding a number of Research Scholars for Ph.d in the areas of Information Security and Image Processing.

[4] N. Ravi Shankar is a Professor and is currently heading the department of Computer Science and Engineering, Sree Nidhi Institute of Science and Technology, Hyderabad, India. He is actively engaged in research in the area of Information Security.

[5] S. Durga Bhavani obtained her Ph.D from University of Hyderabad, India in the area of Evidential Reasoning. She is presently a Professor in Computer Science & Engineering, School of Information Technology, JNT University, Hyderabad, India. Her research interests are applications of uncertain reasoning techniques and Information Security.

$$\begin{bmatrix} K_{1} & K_{2} & K_{3} & K_{4} & K_{5} & K_{6} & K_{7} & K_{8} & K_{9} & K_{10} & K_{11} & K_{12} & K_{13} & K_{14} & K_{15} & K_{16} \\ K_{17} & K_{18} & K_{19} & K_{20} & K_{21} & K_{22} & K_{23} & K_{24} & K_{25} & K_{26} & K_{27} & K_{28} & K_{29} & K_{30} & K_{31} & K_{32} \\ K_{33} & K_{34} & K_{35} & K_{36} & K_{37} & K_{38} & K_{39} & K_{40} & K_{41} & K_{42} & K_{43} & K_{44} & K_{45} & K_{46} & K_{47} & K_{48} \\ K_{49} & K_{50} & K_{51} & K_{52} & K_{53} & K_{54} & K_{55} & K_{56} & K_{57} & K_{58} & K_{59} & K_{60} & K_{61} & K_{62} & K_{63} & K_{64} \\ R_{1} & R_{2} & R_{3} & R_{4} & R_{5} & R_{6} & R_{7} & R_{8} & R_{9} & R_{10} & R_{11} & R_{12} & R_{13} & R_{14} & R_{15} & R_{16} \\ R_{17} & R_{18} & R_{19} & R_{20} & R_{21} & R_{22} & R_{23} & R_{24} & R_{25} & R_{26} & R_{27} & R_{28} & R_{29} & R_{30} & R_{31} & R_{32} \\ R_{33} & R_{34} & R_{35} & R_{36} & R_{37} & R_{38} & R_{39} & R_{40} & R_{41} & R_{42} & R_{43} & R_{44} & R_{45} & R_{46} & R_{47} & R_{48} \\ R_{49} & R_{50} & R_{51} & R_{52} & R_{53} & R_{54} & R_{55} & R_{56} & R_{57} & R_{58} & R_{59} & R_{60} & R_{61} & R_{62} & R_{63} & R_{64} \end{bmatrix} \quad (2)$$

$$\begin{bmatrix} 53 & 62 & 124 & 33 & 49 & 118 & 117 & 43 & 45 & 12 & 63 & 29 & 60 & 35 & 58 & 11 \\ 8 & 41 & 46 & 30 & 108 & 102 & 115 & 51 & 47 & 119 & 38 & 42 & 112 & 99 & 27 & 61 \\ 57 & 120 & 6 & 31 & 116 & 26 & 122 & 125 & 56 & 37 & 113 & 52 & 3 & 54 & 15 & 121 \\ 36 & 40 & 44 & 10 & 19 & 109 & 105 & 4 & 114 & 111 & 83 & 50 & 74 & 0 & 107 & 28 \\ 1 & 2 & 5 & 7 & 9 & 13 & 14 & 16 & 17 & 18 & 20 & 21 & 22 & 23 & 24 & 25 \\ 32 & 34 & 39 & 48 & 55 & 59 & 64 & 65 & 66 & 67 & 68 & 69 & 70 & 71 & 72 & 73 \\ 75 & 76 & 77 & 78 & 79 & 80 & 81 & 82 & 84 & 85 & 86 & 87 & 88 & 89 & 90 & 91 \\ 92 & 93 & 94 & 95 & 96 & 97 & 98 & 100 & 101 & 103 & 104 & 106 & 110 & 123 & 126 & 127 \end{bmatrix} \quad (7)$$