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

A Modified Playfair Cipher for a Large Block of Plaintext

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

***Abstract*—In this paper, we have extended the analysis of the modified Playfair cipher, which includes interweaving and iteration, by considering a plaintext of any size. Here, we have carried out cryptanalysis and examined the avalanche effect. From this analysis, we have found 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 a recent investigation [1], we have modified the Playfair cipher [2] by including interweaving and iteration. In this, the substitution table is represented in the form of a matrix of size 8x16. Further, the key consists of 64 distinct numbers, which lie between 0 and 127. The plaintext is taken in the form of a matrix of size 8x2. Thus the size of the key is 448 bits and the size of the plaintext is 112 bits.

For a detailed account of the formation of the substitution matrix, and for the rules in the development of the cipher, one may refer to section II of [1].

In the present paper, we extend the analysis of the above cipher, by taking a plaintext of any size in general. However, we focus our attention on two cases: (1) The plaintext is a matrix of size 8x8, and (2) It is of size 8xm, where m depends upon the length of the plaintext.

Here, we notice that the substitution and the interweaving together with the iteration play a predominant role in strengthening the cipher.

In section II of this paper, we present the development of the cipher. In section III, we put forth the encryption and decryption algorithms. Then in section IV, we illustrate the cipher with a pair of examples. We discuss the cryptanalysis and Avalanche effect in sections V and VI respectively. Finally we deal with the conclusions in section VII.

II. Development of the Cipher

Consider a plaintext P. On using the ASCII code, let it be represented in the form of a matrix of size nxm, by placing the numbers, corresponding to the plaintext characters, in a column wise manner (pad if needed).

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.

Let the plaintext matrix P be represented as

$$P = \begin{bmatrix} P_{11} & P_{12} & \cdots & P_{1m} \\ P_{21} & P_{22} & \cdots & P_{2m} \\ . & . & \cdots & . \\ . & . & \cdots & . \\ . & . & \cdots & . \\ P_{n1} & P_{n2} & \cdots & P_{nm} \end{bmatrix} \quad (1)$$

Let us now describe the process of substitution. To this end, we focus our attention on the first two columns of this matrix. On using the set of substitution rules (mentioned in [1]), the matrix P assumes the form

$$\begin{bmatrix} Q_{11} & Q_{12} & P_{13} & .. & P_{1m} \\ Q_{21} & Q_{22} & P_{23} & \cdots & P_{2m} \\ . & . & . & \cdots & . \\ . & . & . & \cdots & . \\ . & . & . & \cdots & . \\ Q_{n1} & Q_{n2} & P_{n3} & \cdots & P_{nm} \end{bmatrix} .. \quad (2)$$

where Qs are the elements obtained on substitution.

We now take the third and fourth columns of the P, and carryout the substitution process by using the substitution matrix. In a similar manner, we perform the substitution to the pairs of columns (5, 6), (7, 8) and so on till we exhaust all the columns. However, if the plaintext matrix contains odd number of columns, we pad it by including eight more additional characters, so that the number of columns becomes even. Then the matrix assumes its final form at the end of the substitution, denoted by Q.

We now apply the process of interweaving on the matrix obtained above. Firstly, we convert the elements of Q into their binary form. Since each element of Q lies between 0 and 127, it can be represented in terms of seven binary bits. Thus we have

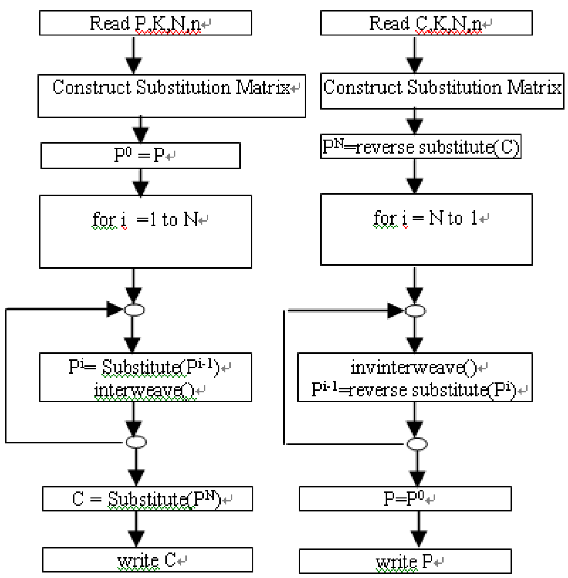
$$b = \begin{bmatrix} b_{11} & b_{12} & \cdots & b_{17m} \\ b_{21} & b_{22} & \cdots & b_{27m} \\ . & . & \cdots & . \\ . & . & \cdots & . \\ . & . & \cdots & . \\ b_{n1} & b_{n2} & \cdots & b_{n7m} \end{bmatrix}$$

We now take the first column of b, and give a circular rotation, so that it assumes the form $[b_{21}, b_{31}, b_{41}, \ldots b_{n1}, b_{11}]^T$, where T denotes the transpose of the vector.

Here, each element of the column is moved up by one row with the element in the first row circularly following the last. We apply similar procedure on all the odd numbered columns. We then apply a circular left shift by one position on all the even numbered rows.

Converting the matrix b into its decimal form, we get the modified Q.

On applying the aforementioned processes, i.e., substitution and interweaving for N rounds, we get the ciphertext C. This completes the process of encryption. The process of decryption is opposite to that of encryption. The reverse process of interweaving is called as inverse interweaving and that of substitution as reverse substitution. These are employed in the process of decryption. The schematic diagram describing the cipher is given 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

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=1to7m from P;
2. for j=1 to 7m 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 7m-1 {
   b_{ij}=$b_{i(j+1)}$;
   }
   b_{in}=k;
   }
4. Construct P from b_{ij};

D Algorithm for invinterweave

1. construct [b_{ij}],i=1to8,j=1to7m from P;
2. for i= n to 2 in step 2 {
   k=b_{i7m};
   for j= 7m to 2{
   b_{ij}=$b_{i(j-1)}$;
   }
   b_{i1}=k;
   }
3. for j = 7m-1 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 from b_{ij};

III. Illustration of the Cipher

Consider the plaintext given below.

No one shall forget the past. The destruction of Hiroshima and Nagasaki, as the destiny speaks, shall be remembered for ever. Whenever we think of the development of the nuclear energy, we must fully feel that it should be utilized for the welfare of the mankind. Transmit this message as safely as you can. (3)

Let us focus our attention on the first sixty four characters of the plaintext given by

No one shall forget the past. The destruction of Hiroshima and$\not{b}$ (4)

This plaintext, in its ASCII representation, when arranged in the form of an 8x8 matrix, assumes the form

$$P = \begin{bmatrix} 78 & 104 & 103 & 112 & 104 & 117 & 102 & 105 \\ 111 & 97 & 101 & 97 & 101 & 99 & 32 & 109 \\ 32 & 108 & 116 & 115 & 32 & 116 & 72 & 97 \\ 111 & 108 & 32 & 116 & 100 & 105 & 105 & 32 \\ 110 & 32 & 116 & 46 & 101 & 111 & 114 & 97 \\ 101 & 102 & 104 & 32 & 115 & 110 & 111 & 110 \\ 32 & 111 & 101 & 32 & 116 & 32 & 115 & 100 \\ 115 & 114 & 32 & 84 & 114 & 111 & 104 & 32 \end{bmatrix}$$

(5)

On adopting the procedure described in section II of [1], we get the substitution matrix given by (6).

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

On applying the substitution process, we get the modified plaintext, denoted by P^1, as

$$P1=\begin{bmatrix} 86 & 95 & 110 & 119 & 98 & 63 & 115 & 109 \\ 105 & 103 & 103 & 98 & 123 & 47 & 59 & 36 \\ 55 & 8 & 122 & 108 & 55 & 57 & 59 & 126 \\ 19 & 119 & 55 & 57 & 98 & 4 & 36 & 64 \\ 92 & 70 & 6 & 108 & 103 & 114 & 109 & 101 \\ 97 & 47 & 92 & 68 & 112 & 98 & 74 & 103 \\ 67 & 36 & 92 & 66 & 57 & 55 & 51 & 98 \\ 47 & 105 & 66 & 75 & 111 & 83 & 92 & 68 \end{bmatrix}$$

(7)

On using the process of interweaving, we get the transformed plaintext as

$$P1=\begin{bmatrix} 121 & 31 & 77 & 69 & 84 & 95 & 118 & 89 \\ 99 & 34 & 111 & 102 & 115 & 59 & 59 & 116 \\ 47 & 59 & 100 & 114 & 110 & 88 & 99 & 84 \\ 25 & 102 & 23 & 108 & 98 & 80 & 44 & 69 \\ 104 & 14 & 25 & 89 & 75 & 69 & 31 & 75 \\ 67 & 46 & 92 & 64 & 120 & 55 & 98 & 98 \\ 87 & 67 & 45 & 6 & 119 & 102 & 51 & 77 \\ 7 & 125 & 106 & 95 & 103 & 23 & 118 & 69 \end{bmatrix}$$

(8)

After carrying out all the 16 iterations, we get the ciphertext C in the form

$$C=\begin{bmatrix} 42 & 56 & 40 & 14 & 126 & 122 & 36 & 65 \\ 86 & 114 & 87 & 116 & 123 & 44 & 42 & 60 \\ 31 & 114 & 55 & 9 & 105 & 5 & 89 & 16 \\ 28 & 119 & 40 & 47 & 123 & 36 & 52 & 46 \\ 1 & 110 & 120 & 55 & 2 & 90 & 68 & 81 \\ 71 & 59 & 79 & 44 & 67 & 69 & 99 & 89 \\ 81 & 108 & 88 & 99 & 116 & 20 & 82 & 115 \\ 64 & 31 & 11 & 17 & 18 & 22 & 35 & 94 \end{bmatrix} \quad (9)$$

In the process of decryption, we take the cipher text C, obtained above, and apply the reverse substitution procedure. Thus we get

$$PN=\begin{bmatrix} 47 & 52 & 105 & 2 & 98 & 15 & 4 & 32 \\ 84 & 83 & 79 & 52 & 94 & 0 & 112 & 29 \\ 56 & 10 & 9 & 19 & 44 & 14 & 82 & 23 \\ 111 & 61 & 114 & 41 & 92 & 0 & 6 & 42 \\ 22 & 92 & 116 & 34 & 24 & 76 & 64 & 86 \\ 70 & 55 & 77 & 19 & 66 & 68 & 35 & 71 \\ 79 & 115 & 89 & 112 & 113 & 9 & 81 & 51 \\ 48 & 122 & 45 & 25 & 17 & 21 & 124 & 123 \end{bmatrix} \quad (10)$$

On employing the inverse interweaving process, we get the modified P^N as

$$PN=\begin{bmatrix} 53 & 90 & 60 & 17 & 17 & 23 & 104 & 81 \\ 86 & 82 & 101 & 97 & 116 & 5 & 82 & 24 \\ 84 & 81 & 14 & 28 & 94 & 2 & 33 & 31 \\ 77 & 45 & 80 & 105 & 86 & 5 & 44 & 43 \\ 43 & 63 & 50 & 1 & 12 & 34 & 2 & 42 \\ 78 & 38 & 111 & 19 & 72 & 4 & 33 & 3 \\ 71 & 61 & 76 & 57 & 18 & 68 & 98 & 77 \\ 50 & 123 & 45 & 88 & 57 & 68 & 124 & 123 \end{bmatrix} \quad (11)$$

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

$$P=\begin{bmatrix} 78 & 104 & 103 & 112 & 104 & 117 & 102 & 105 \\ 111 & 97 & 101 & 97 & 101 & 99 & 32 & 109 \\ 32 & 108 & 116 & 115 & 32 & 116 & 72 & 97 \\ 111 & 108 & 32 & 116 & 100 & 105 & 105 & 32 \\ 110 & 32 & 116 & 46 & 101 & 111 & 114 & 97 \\ 101 & 102 & 104 & 32 & 115 & 110 & 111 & 110 \\ 32 & 111 & 101 & 32 & 116 & 32 & 115 & 100 \\ 115 & 114 & 32 & 84 & 114 & 111 & 104 & 32 \end{bmatrix} \quad (12)$$

The ciphertext corresponding to the entire plaintext (taken as blocks of 64 characters), given in (3), in hexadecimal notation, is

14A0D71B4E82199113E8D2AFB01C541E081B70390B42
20CB1AD6E0A12FDF882AADF1A1498C997D0EB4767F
E1CF206DAE946ED6CF49F00CDC5211BF1AD19088986
2349123053D1E98A29DE314D7ACA4FB2C177637CB41
926D02A45512A534C9C4C1159F9F33A00FE187FA6D4
E77A22573C13948B7EF9CB3B4952CD1831587B165F95
0DE536EC81492C712A15E.

(13)

We now take another example, wherein the entire plaintext, given in (3), is taken as a single block, consisting of 312 characters. Let us now pad the plaintext by including eight more characters, say, *s,t,u,v,w,x,y,z*. Then the plaintext, consisting of 320 characters, is arranged in the form of a matrix of size 8x40. For convenience, this is represented as P=[AB], where A and B are given in (14) and (15) respectively.

The ciphertext corresponding to the above mentioned plaintext (taken as a single block of 320 characters), in its hexadecimal notation, is obtained as

E7C24E39557A51FD112BB453F2CCA78E0EE3F6E80
278D85DE7F668613DEBCA24925B91CEF6D9413026CA

1D10D221B0CD0F8B5FE77D456124F7E9C0172333A9D FD49CDBF8056A1B748EA2418FC0AEFFEB900ACD215 B7725801F6A3C5AAEE3277FC89400C16BAAF7313B42 A698A7B0809D5F95FCCDC89FA82BCE9E94DFBCC26 B6CC1CC713DD61353FDF6AE4483. It can be verified

$$\begin{bmatrix} 78 & 104 & 103 & 112 & 104 & 117 & 102 & 105 & 78 & 44 & 32 & 32 & 32 & 101 & 101 & 32 & 32 & 114 & 110 & 101 \\ 111 & 97 & 101 & 97 & 101 & 99 & 32 & 109 & 97 & 32 & 100 & 115 & 115 & 32 & 114 & 101 & 87 & 32 & 107 & 32 \\ 32 & 108 & 116 & 115 & 32 & 116 & 72 & 97 & 103 & 97 & 101 & 112 & 104 & 114 & 101 & 118 & 104 & 119 & 32 & 100 \\ 111 & 108 & 32 & 116 & 100 & 105 & 105 & 32 & 97 & 115 & 115 & 101 & 97 & 101 & 100 & 101 & 101 & 101 & 111 & 101 \\ 110 & 32 & 116 & 46 & 101 & 111 & 114 & 97 & 115 & 32 & 116 & 97 & 108 & 109 & 32 & 114 & 110 & 32 & 102 & 118 \\ 101 & 102 & 104 & 32 & 115 & 110 & 111 & 110 & 97 & 116 & 105 & 107 & 108 & 101 & 102 & 46 & 101 & 116 & 32 & 101 \\ 32 & 111 & 101 & 32 & 116 & 32 & 115 & 100 & 107 & 104 & 110 & 115 & 32 & 109 & 111 & 32 & 118 & 104 & 116 & 108 \\ 115 & 114 & 32 & 84 & 114 & 111 & 104 & 32 & 105 & 101 & 121 & 44 & 98 & 98 & 114 & 32 & 101 & 105 & 104 & 111 \end{bmatrix} \quad (14)$$

$$\begin{bmatrix} 112 & 32 & 108 & 114 & 109 & 108 & 116 & 115 & 101 & 101 & 104 & 114 & 101 & 100 & 110 & 105 & 103 & 102 & 121 & 115 \\ 109 & 116 & 101 & 103 & 117 & 121 & 104 & 104 & 32 & 100 & 101 & 101 & 32 & 46 & 115 & 115 & 101 & 101 & 111 & 116 \\ 101 & 104 & 97 & 121 & 115 & 32 & 97 & 111 & 117 & 32 & 32 & 32 & 109 & 32 & 109 & 32 & 32 & 108 & 117 & 117 \\ 110 & 101 & 114 & 44 & 116 & 102 & 116 & 117 & 116 & 102 & 119 & 111 & 97 & 32 & 105 & 109 & 97 & 121 & 32 & 118 \\ 116 & 32 & 32 & 32 & 32 & 101 & 32 & 108 & 105 & 111 & 101 & 102 & 110 & 32 & 116 & 101 & 115 & 32 & 99 & 119 \\ 32 & 110 & 101 & 119 & 102 & 101 & 105 & 100 & 108 & 114 & 108 & 32 & 107 & 84 & 32 & 115 & 32 & 97 & 97 & 120 \\ 111 & 117 & 110 & 101 & 117 & 108 & 116 & 32 & 105 & 32 & 102 & 116 & 105 & 114 & 116 & 115 & 115 & 115 & 110 & 121 \\ 102 & 99 & 101 & 32 & 108 & 32 & 32 & 98 & 122 & 116 & 97 & 104 & 110 & 97 & 104 & 97 & 97 & 32 & 46 & 122 \end{bmatrix} \quad (15)$$

that the ciphertext obtained above can be brought back to its original form by applying the decryption process.

IV. CRYPTANALYSIS

It is well known to us that the general types of cryptanalytic attacks are (1) Ciphertext only (Brute force) attack, (2) Known plaintext attack and (3) Chosen plaintext/ciphertext attack. When the ciphertext is known to us, we take various plaintexts one after another and try to see if any one of the plaintexts taken by us yields the ciphertext under consideration. In this problem, when the size of the plaintext matrix is 8x8 i.e. 448 binary bits, the different possible plaintexts which we have to make use of, are 2^{448} ($\approx 10^{134.4}$). As this is a very large number, the cipher cannot be broken by the brute force attack. When the size of the plaintext matrix is immensely large (i.e., in the case of the plaintext matrix of size 8x40), this brute force attack is totally ruled out.

In this problem, the key consists of 64 distinct numbers, where each number lies between 0 and 127. Thus the size of the key space is ${}^{128}P_{64}$. Hence it is impossible to find the plaintext corresponding to the given ciphertext by exhausting the computation with all possible keys.

Now let us consider the known plaintext attack. In this case, we know as many plaintext and ciphertext pairs as we require. As we know the plaintext at the beginning of the first iteration, and the ciphertext at the end of the last iteration, linking them directly in any manner and determining the key in any way is totally impossible, as there are a number of transformations in between.

A choice of the plaintext or a choice of the ciphertext for the determination of the key cannot be done as the plaintext undergoes a number of transformations at various stages of the iterative process.

Thus this approach also is not of any use.

In the light of the above facts, we conclude that this cipher is a strong one and it cannot be broken by any cryptanalytic attack.

V. AVALANCHE EFFECT

On using the ASCII code, the plaintext, given in (4), can be represented in its binary form as

10011101101000110011111110000110100011101011100110110100111011111110000111001011100001110010111000110100000110110101000001101100111010011100110100000111010010010001100001*1101111*1101100010000011101001100100110100111010010100000110111001000001110100010111011001011101111111001011000011100101110011011010000100000111001111011101101111111011100100000110111111001010100000111010001000001110011110010011100111111001001000001010100111001011011111101000001000000.

(16)

If we change the 4th character from **o** to **n** (i.e., from ASCII code 111 to 110), the plaintext will be in the form

10011101101000110011111110000110100011101011100110110100111011111110000111001011100001110010111000110100000110110101000001101100111010011100110100000111010010010001100001*1101110*1101100010000011101001100100110100111010010100000110111001000001110100010111011001011101111111001011000011100101110011011010000100000111001111011101101111111011100100000110111111001010100000111010001000001110011110010011100111111001001000001010100111001011011111101000001000000.

(17)

It can be seen that the plaintexts, given in (16) and (17), differ by one bit.

The ciphertexts corresponding to the above plaintexts are

000101001010000011010111000110110100111010000010000110011001000100010011111010001101001010101111101100000000111000101010000001111000000100000011011011110000000111001000010110100001000100000011001011000110101101010110111000001010000100101111111011111100010000001010101010110111110001101000010100100 1

1000110010011001011111010000111010110100011101100111111111110000111001111001000000110110110101110100101000110111011010110110011110100100111110000 0000110011011100

(18)

and

1001110011111111001110000000110000000001011001100 0010000101010011001101010000110110101010111110001 0010101000111111110011111000101111110000010001000 0011110101010011010101110111010100010011001011111 1010101110011010000111100100011101011000001100101 0000010001010101110100101100111001010000110100101 1100011101101010001100110110010011001000010111001 0100000000110001100110110101000011111011100000 0001111111010010111000101110001000011001001011100 010111010110000.

(19)

It can be readily verified that the ciphertexts, given in (18) and (19), differ by 235 bits. This is quite considerable.

We now change the key element K_{22} (i.e., second row and sixth column of (6)) from 102 to 103. With this change, the key changes by one bit. On applying the modified key on the original plaintext, given in (5), we get the corresponding ciphertext as

1111001111001110111111100111000010100011000111010 1001011010000000101111000111010110001001100110101 0000000110011111010010111110010100110111100011000 0110100101100100010111010000000111111011011100001 1010001000101001011111110010110000000101001000011 0110100011010100100110000000100010101111001110100 0100111100010001011011001101001110101111010000001 0000001011111111101000001110000100000000111111111 1110011101100110101001001111000011011100001010111 00000000001100.

(20)

The ciphertexts given in (18) and (20) differ by 241 bits which is conspicuous.

From the above analysis, we notice that this cipher produces strong avalanche effect.

VI. CONCLUSIONS

In this paper, we have extended the analysis of modified Playfair cipher by taking a very large plaintext into consideration. Here, pairs of characters are taken from the adjacent columns (characters are taken from 1^{st} and 2^{nd} columns, 3^{rd} and 4^{th} columns, etc.) of the plaintext matrix for the purpose of substitution. The process of interweaving and the process of substitution modify the plaintext at each stage of the iteration. This causes confusion and diffusion in a systematic manner and enhances the strength of the cipher.

The algorithms developed in this analysis for encryption and decryptions, along with the other requisites, are implemented in C language.

The time required for the encryption of the entire plaintext in (3), (taken as a single block) is $20.5*10^{-3}$ seconds and that of the decryption is $20.5*10^{-3}$ seconds.

From the cryptanalysis, and the avalanche effect carried out in this analysis, we conclude that the cipher is a potential one, and it cannot be broken by any cryptanalytic attack.

REFERENCES

[1] 1. VUK Sastry, N.Ravi Shankar, "A Modified Playfair Cipher Involving Interweaving and Iteration", (accepted for publication) *International Journal of Computer Theory and Engineering, to be published.*

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

[3] Biographical notes:

[4] 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.

[5] 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.

[6] 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.