CHAPTER 8

A MODIFIED PLAYFAIR CIPHER INVOLVING INTERWEAVING AND ITERATION
8.1. INTRODUCTION

In all the classical ciphers, Playfair cipher [21] 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 balloon 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, \textbf{AR} is replaced with \textbf{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, \textbf{MU} becomes \textbf{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, \textbf{HS} becomes \textbf{BP} and \textbf{EA} becomes \textbf{IM} or \textbf{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 analysis, 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 8.2, we present the development of the cipher. We design the algorithms for encryption, decryption, interweaving, and inverse interweaving in section 8.3. In section 8.4, we illustrate the cipher with an example. We mention the avalanche effect in section 8.5, and discuss the cryptanalysis in section 8.6. Finally, in section 8.7, we draw conclusions from the computations carried out in this analysis.

8.2. 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

$$P = [P_{ij}], \text{ i=1 to } n, \text{ j=1 to 2}. \quad (8.2.1)$$

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 (8.2.2).

\[
\begin{bmatrix}
K_1 & K_2 & K_3 & K_4 & K_5 & K_6 & K_7 & K_8 & K_9 & K_{10} & K_{11} & K_{12} & K_{13} & K_{14} & K_{15} & K_{16} \\
K_{17} & K_{18} & K_{19} & K_{20} & K_{21} & K_{22} & K_{23} & K_{24} & K_{25} & K_{26} & K_{27} & K_{28} & K_{29} & K_{30} & K_{31} & K_{32} \\
K_{33} & K_{34} & K_{35} & K_{36} & K_{37} & K_{38} & K_{39} & K_{40} & K_{41} & K_{42} & K_{43} & K_{44} & K_{45} & K_{46} & K_{47} & K_{48} \\
K_{49} & K_{50} & K_{51} & K_{52} & K_{53} & K_{54} & K_{55} & K_{56} & K_{57} & K_{58} & K_{59} & K_{60} & K_{61} & K_{62} & K_{63} & K_{64} \\
R_1 & R_2 & R_3 & R_4 & R_5 & R_6 & R_7 & R_8 & R_9 & R_{10} & R_{11} & R_{12} & R_{13} & R_{14} & R_{15} & R_{16} \\
R_{17} & R_{18} & R_{19} & R_{20} & R_{21} & R_{22} & R_{23} & R_{24} & R_{25} & R_{26} & R_{27} & R_{28} & R_{29} & R_{30} & R_{31} & R_{32} \\
R_{33} & R_{34} & R_{35} & R_{36} & R_{37} & R_{38} & R_{39} & R_{40} & R_{41} & R_{42} & R_{43} & R_{44} & R_{45} & R_{46} & R_{47} & R_{48} \\
R_{49} & R_{50} & R_{51} & R_{52} & R_{53} & R_{54} & R_{55} & R_{56} & R_{57} & R_{58} & R_{59} & R_{60} & R_{61} & R_{62} & R_{63} & R_{64}
\end{bmatrix}
\] (8.2.2)
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 $P_{i1}^l, P_{i2}^l$. 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

\[
P^1 = \begin{bmatrix} P_{ij}^1 \end{bmatrix}, \quad i = 1 \text{ to } n, \quad j = 1 \text{ to } 2.
\]  

(8.2.3)

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

\[
b = \begin{bmatrix} b_{11} & b_{12} & \cdots & b_{14} \\ b_{21} & b_{22} & \cdots & b_{24} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n1} & b_{n2} & \cdots & b_{n4} \end{bmatrix}
\]

Let us rotate the first column so that it assumes the form \([b_{21}, b_{31}, \ldots, b_{n1}, b_{11}]^T\), 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

\[
b = \begin{bmatrix} b_{21} & b_{12} & b_{23} & \cdots & b_{213} & b_{114} \\ b_{22} & b_{33} & b_{24} & \cdots & b_{214} & b_{314} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ b_{n2} & b_{13} & b_{n4} & \cdots & b_{n14} & b_{11} \end{bmatrix}
\]

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 carry out the iteration.

In what follows, we present the schematic diagram of the encryption and the decryption and their algorithms.

Fig. 8.1. Schematic diagram of the cipher

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

8.3.1 ALGORITHM FOR ENCRYPTION
1. read n,N,K,P;
2. Construct Substitution matrix
3. P0 = P;
4. for i=1 to N {
   Pi = Substitute(Pi-1);
   interweave();
}
5. C = Substitute(PN);
6. write C;

8.3.2 ALGORITHM FOR DECRYPTION
1. read n,N,K,C;
2. Construct Substitution matrix
3. PN = reverse substitute(C);
4. for i=N to 1 {
   invinterweave();
   Pi-1 = reverse substitute (Pi);
}
5. P=P0;
6. write P;

8.3.3 ALGORITHM FOR INTERWEAVE
1. construct [bij],i=1ton,j=1to14 from P;
2. for j=1 to 14 in step 2 {
   k=b1j;
   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=b11;
   for j=1 to 13 {
      b_{ij}=b_{(i+1)j};
   }
   b_{i14}=k;
}
4. Construct P from bij;

8.3.4 ALGORITHM FOR INVINTERWEAVE
1. construct [bij], 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)};
   }
}}
3. for \( j = 13 \) to 1 in step 2{
\( k = b_{0j}; \)
for \( i = n \) to 2{
\( b_{ij} = b_{(i-1)j}; \)
\( b_{1j} = k; \)
}
\}

4. Construct \( P^i \) from \( b_{ij} \);

### 8.4. 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. \( (8.4.1) \)

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

I do not Know wh \( (8.4.2) \)

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

\[
P = \begin{bmatrix}
73 & 32 \\
32 & 75 \\
100 & 110 \\
111 & 111 \\
32 & 119 \\
110 & 32 \\
111 & 119 \\
116 & 104 \\
\end{bmatrix}
\] \( (8.4.3) \)

The substitution matrix, described in section 8.2, is given in (8.4.4).

\[
\begin{array}{cccccccccccccccccccc}
53 & 62 & 124 & 33 & 49 & 118 & 117 & 43 & 45 & 12 & 63 & 29 & 60 & 35 & 58 & 11 \\
57 & 120 & 6 & 31 & 116 & 26 & 122 & 125 & 56 & 37 & 113 & 52 & 3 & 54 & 15 & 121 \\
36 & 40 & 44 & 10 & 19 & 109 & 105 & 4 & 114 & 111 & 83 & 50 & 74 & 0 & 107 & 28 \\
1 & 2 & 5 & 7 & 9 & 13 & 14 & 16 & 17 & 18 & 20 & 21 & 22 & 23 & 24 & 25 \\
32 & 34 & 39 & 48 & 55 & 59 & 64 & 65 & 66 & 67 & 68 & 69 & 70 & 71 & 72 & 73 \\
75 & 76 & 77 & 78 & 79 & 80 & 81 & 82 & 84 & 85 & 86 & 87 & 88 & 89 & 90 & 91 \\
92 & 93 & 94 & 95 & 96 & 97 & 98 & 100 & 101 & 103 & 104 & 106 & 110 & 123 & 126 & 127 \\
\end{array}
\] \( (8.4.4) \)
On applying the substitution process (see section 8.2) on the elements of $P$, we get the modified $P$, denoted by $P_1$, as

$$
P_1 = \begin{bmatrix}
32 & 34 \\
75 & 92 \\
101 & 123 \\
83 & 83 \\
67 & 8 \\
92 & 70 \\
18 & 37 \\
113 & 96 \\
\end{bmatrix}
$$

(8.4.5)

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

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

(8.4.6)

On applying the process of interweaving described in section 8.2, we get the modified $b$. Thus we have

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

(8.4.7)

We now convert these binary numbers into their corresponding decimal numbers, and construct the modified $P_1$, as
After carrying out all the sixteen iterations, we get the ciphertext in the form

\[
P_1 = \begin{bmatrix} 21 & 108 \\ 97 & 89 \\ 15 & 119 \\ 83 & 2 \\ 19 & 25 \\ 86 & 7 \\ 97 & 64 \\ 113 & 32 \end{bmatrix}
\]

(8.4.8)

Now, let us consider the process of decryption. On taking the \( C \) given in (8.4.9), and applying the reverse substitution process, we get

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

(8.4.9)

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

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

(8.4.10)

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

(8.4.11)
Following the same procedure, after carrying out all the sixteen iterations, we get the plaintext $P$ in the form

$$P = \begin{bmatrix}
73 & 32 \\
32 & 75 \\
100 & 110 \\
111 & 111 \\
32 & 119 \\
110 & 32 \\
111 & 119 \\
116 & 104 \\
\end{bmatrix} \quad (8.4.12)$$

This is the same as the plaintext given in (8.4.3).

In what follows, we analyze avalanche effect, which is a desired property of every cipher.

### 8.5. AVALANCHE EFFECT

On changing the eleventh character of the plaintext given by (8.4.2), from $n$ to $o$, whose ASCII codes are 110 and 111, the plaintext under goes a change of one bit.

The ciphertexts corresponding to the original plaintext and the modified plaintext are

$$11100101110110110111100011100010101001100110101101100010000101$$

and

$$1101100010011101111001011100000010011100010111001100011010$$

It can be readily noticed that (8.5.1) and (8.5.2) differ by 55 bits (out of 112 bits), which is 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 (8.4.2), we get the corresponding ciphertext as

\[1110111101111101100101111011111010110000011110011111100110010010110100000010110.\]  

(8.5.3)

It can be seen that the ciphertexts given in (8.5.1) and (8.5.3) differ by 55 bits (out of 112 bits), which is also a good departure.

From the above analysis, we conclude that the plaintext is undergoing a good amount of change before it turns out the ciphertext.

**8.6. CRYPTANALYSIS**

In the science of cryptology, the different types of cryptanalytic attacks are

1. Ciphertext only attack (Brute force attack)
2. Known plaintext attack
3. Chosen plaintext attack and
4. Chosen ciphertext attack.

However, as we have pointed out earlier, we restrict our attention to the first two attacks.

In this block cipher, the key is containing 64 distinct numbers, wherein, each number is lying between 0 and 127. Thus, the size of the key space is \(2^{64}\). Here, we have selected sixty four numbers out of one hundred and twenty eight distinct numbers. If the time required for execution of the algorithm with one key is \(10^{-7}\) seconds, then the time
required for the execution of the cipher with all possible keys in the key space is

\[
\frac{128 \cdot P_{64} \cdot X \cdot 10^{-7}}{365 \cdot 24 \cdot 60} = \frac{128 \cdot 3 \cdot 12 \cdot X \cdot 10^{-15}}{64!} \approx 9.48 \times 10^{111} \text{ years.}
\]

Thus, as the time required is very large, it is impossible to break this cipher by the brute force attack.

Now, let us consider the known plaintext attack. In this case, we have plaintext and ciphertext pairs as many as we require. The basic relations that are governing the cipher are

\[
P = P_0,
\]

\[
P^i = \text{Substitute}(P^{i-1}), \ i = 1 \text{ to } 16,
\]

\[
P^i = \text{interweave}(P^i).
\]

For the sake of convenience in representation, let us denote the function substitute by S and the function interweave by \( \Psi \).

At the end of the sixteenth round of the iteration process, the relation connecting the ciphertext C and the plaintext P is given by

\[
C = S( \Psi( \ldots( S( \Psi( S(P) ) ) ) ) \ldots )
\]

As P is thoroughly influenced by the substitution process and interweaving, it cannot be transferred to the left side, as it could be done in the case of the classical Hill cipher, so that a function of K or K can be determined, for the purpose of breaking the cipher. Thus, this cipher cannot be broken by the known plaintext attack.
8.7. COMPUTATIONS AND CONCLUSIONS

In this chapter, we have devoted our attention to a modification of the Playfair cipher (which depends upon key based substitution) 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.

On using the ASCII code, the plaintext given in (8.4.1) can be represented in the form of a set of matrices wherein each matrix is of size 8x2. By applying the procedure mentioned in section 8.4, the ciphertext corresponding to the entire plaintext given in (8.4.1), in its hexadecimal notation, can be written in the form

\[
E5DBFF70E2A66F65B8A9792B6105FC8FB3097ACCA938982C3B6437A57299E6A042AB38AA02E70162EB2F5F27038A0F9AE25CBE667984B998D37C4BDDBC1F18795B9F159FD4AF99D38A62DAB5660A5CA65FEA72F7D49C044CCE5F989620392A1B033D5C055EE9591CD3C4DAE9B8A2AAC8394FE29A84C62C2BE2BE5170841B310653E04C496F456C132B76AAA2. \quad (8.7.1)
\]

However, it may be noted that we have padded eleven blank characters in forming the last block.
The time required for the encryption of the entire plaintext given in (8.4.1) is $10.3 \times 10^{-3}$ seconds and the time for the decryption is $10.3 \times 10^{-3}$ seconds.

This analysis can be extended to the case of a plaintext block of any size. This problem is examined in the following chapter.