CHAPTER 10

A GENERALIZED PLAYFAIR CIPHER INVOLVING INTERTWINING, INTERWEAVING AND ITERATION
10.1. INTRODUCTION

The Playfair cipher, which enjoyed its prominence during the Second World War, encrypts data by taking two characters (digrams) at a time. In this, the characters of both the plaintext and the ciphertext are the 26 letters of the English language. Though this cipher cannot dissipate the statistical characteristics of the plaintext effectively, owing to the lack of computing power in those days, it was considered to be a strong one. The advent of computers in the later half of the last century, which has brought in a revolution in the computing capabilities, has made this cipher vulnerable to statistical cryptanalysis.

Let us now analyze the basic principles of the classical Playfair cipher.

In this, 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 in their ascending order, 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:
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 bal lo x 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.

In this chapter, our objective is to generalize the Playfair cipher, by taking the character set of the plaintext and the ciphertext as the 128 ASCII characters instead of the 26 characters of the English language. In addition to this, we also have introduced the concepts of interweaving, intertwining and iteration, which strengthen the cipher significantly. We
have also increased the size of the plaintext block, from two characters to any number of characters (nxm), which is encrypted as a block as a whole. Here, we have illustrated the cipher with a pair of examples, wherein the sizes of the plaintext blocks are (1) 8x8, and (2) 8xm, in which, m depends upon the size of the plaintext.

In section 2 of this chapter, we have presented the development of the cipher. In section 3, we have put forth the encryption and decryption algorithms. Then in section 4, we have illustrated the cipher with a pair of examples. We have discussed Avalanche effect and the cryptanalysis in sections 5 and 6 respectively. Finally we have dealt with the conclusions in section 7.

10.2. DEVELOPMENT OF THE CIPHER

Let us take a plaintext P. On using the ASCII codes, this plaintext can be represented in the form of a matrix (in a column wise manner)

\[ P = [P_{ij}], \quad i = 1 \text{ to } n, \quad j = 1 \text{ to } m. \]  

(10.2.1)

We now choose a key K, containing 64 distinct numbers that lie between 0 and 127, in a random order. We place these numbers in the first four rows of a matrix, of size 8x16, in a row wise manner. We then place the rest of the numbers between 0 and 127 (excluding the numbers in K) in the subsequent four rows of the above matrix in their ascending order. We denote this matrix as the substitution matrix. If we denote the numbers in the key as \( K_i, \ i=1 \text{ to } 64 \), and the rest of the numbers as \( R_i, \ i=1 \text{ to } 64 \), then, the substitution matrix assumes the form
Let us consider a pair of characters, denoted by $P_1, P_2$. Let them be represented in terms of their ASCII codes, say $A_1, A_2$. Then, the set of rules 1 to 4, mentioned in section 10.1, can be modified appropriately 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 \( K_{41}, R_{36} \).

Let us now consider the plaintext matrix \( P \) given in (1). We take the characters in the first and second columns of the first row of this plaintext matrix, i.e., \( P_{11}, P_{12} \). We apply the substitution process, described above, on these characters, and map them into another pair of characters denoted by \( P_{11}^i \) and \( P_{12}^i \). We now take the characters in the second and third columns of the first row, i.e., \( P_{12}^i \) and \( P_{13}^i \) and apply the same procedure. Similarly we adopt the substitution process on pairs of characters in the columns \( (3,4) \), \( (4,5) \) and so on. The same process is employed on all the other rows of the plaintext matrix. Here, it is to be noted that the characters in the columns 2 to \( m-1 \) are subjected to substitution in an intertwined manner, while the elements in the first and the last columns have undergone mere substitution. After carrying out the substitution in the aforementioned manner, we get the modified plaintext matrix, denoted by \( [P_{ij}^i] \), \( i=1 \) to \( n \), \( j=1 \) to \( m \).
Let us now describe the process of interweaving. Firstly, we convert the plaintext matrix $[P_{ij}]$ into its binary form. Here, as each element of the plaintext matrix lies between 0 and 127, it can be represented in terms of seven binary bits. Thus we get $n \times 7m$ elements, which can be written in the form of a matrix $b$ given by

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

We now apply a circular rotation, in the upward direction, to the first column, so that it assumes the form $[b_{21}, b_{31}, \ldots, b_{n1}, b_{11}]^T$, where $T$ is the transpose of the row vector. Immediately after this, we apply a left circular rotation, by one position, to the first row of the matrix. Then the first row assumes the form $[b_{12}, b_{13}, \ldots, b_{17m}, b_{21}]$. Now the second column is given a circular rotation (similar to that of the first column) and then the second row is rotated circularly by one position. In a similar manner, we rotate all the columns and rows of the matrix. However, if the number of columns is more than the number of rows, we repeatedly apply rotation to the rows with the first row circularly following the last row.

After carrying out all the rotations, we convert the binary bits into their decimal equivalent and form the modified $P$. This completes the process of interweaving. The processes that are opposite to substitution and interweaving are called as reverse substitution and inverse
interweaving respectively. These are employed in the process of decryption.

The schematic diagram describing the procedures of encryption and decryption are given in Fig. 10.1.

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

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

10.3.2 ALGORITHM FOR DECRYPTION
1. read n,N,K,C;
2. Construct Substitution matrix
3. \( P^N = \text{reverse substitute}(C) \);
4. for \( i=N \) to \( 1 \) {
   \( \text{invinterweave}(); \)
   \( P^{i-1} = \text{reverse substitute}(P^i); \)
}
5. \( P=P^0 \);
6. write \( P \);

10.3.3 ALGORITHM FOR INTERWEAVE
1. construct \([b_{ij}], i=1\text{ to } n, j=1\text{ to } 7m\) from \( P \);
2. for \( j=1 \) to \( 7m \) {
   \( k=b_{1j} \);
   for \( i=1 \) to \( n-1 \) {
      \( b_{ij}=b_{(i+1)j} \);
   }
   \( b_{nj}=k \);
   \( k=b_{(j \mod n)1} \);
   for \( i=1 \) to \( 7m-1 \) {
      \( b_{(j \mod n)i}=b_{(j \mod n)(i+1)} \);
   }
   \( b_{(j \mod n)n}=k \);
}
3. Construct \( P \) from \( b_{ij} \);

10.3.4 ALGORITHM FOR INVINTERWEAVE
1. construct \([b_{ij}], i=1\text{ to } 8, j=1\text{ to } 7m\) from \( P \);
2. for \( i=7m \) to \( 1 \) {
   \( k=b_{(i \mod n)7m} \);
   for \( j=7m \) to \( 2 \) {
      \( b_{(i \mod n)j}=b_{(i \mod n)(j-1)} \);
   }
}
\[
\begin{align*}
b_{(i \mod n)1} &= k; \\
k &= b_{ni}; \\
\text{for } j = n \text{ to } 2 \{ \\
\quad b_{ji} &= b_{(j-1)i}; \\
\} \\
\quad b_{11} &= k; \\
\} \\
\end{align*}
\]

3. Construct \( P \) from \( b_{ij} \);

10.4. ILLUSTRATION OF THE CIPHER

Consider the plaintext given below.

Every gun that is made, every warship launched, every rocket fired signifies, in the final sense, a theft from those who are hungry and are not fed, those who are cold and not clothed. This world in arms is not spending money alone. It is spending the sweat of its laborers, the genius of its scientists, the hopes of its children. This is not a way of life at all in any true sense. Under the cloud of threatened war, it is humanity hanging from a cross of iron. \hspace{1cm} (10.4.1)

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

Every gun that is made, every warship launched, every rocket fir \hspace{1cm} (10.4.2)

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

\[
P = \begin{bmatrix}
69 & 110 & 115 & 101 & 114 & 117 & 101 & 99 \\
118 & 32 & 32 & 118 & 115 & 110 & 118 & 107 \\
114 & 104 & 97 & 114 & 105 & 104 & 114 & 116 \\
121 & 97 & 100 & 121 & 112 & 101 & 121 & 32 \\
32 & 116 & 101 & 32 & 32 & 100 & 32 & 102 \\
103 & 32 & 44 & 119 & 108 & 44 & 114 & 105 \\
117 & 105 & 32 & 97 & 97 & 32 & 111 & 114 \\
\end{bmatrix}
\hspace{1cm} (10.4.3)
A key consisting of 64 numbers is selected in the form

\[
\begin{array}{cccccccccccccccccccccc}
53 & 62 & 124 & 33 & 49 & 118 & 117 & 43 & 45 & 12 & 63 & 29 & 60 & 35 & 58 & 11 \\
57 & 120 & 6 & 31 & 116 & 26 & 122 & 125 & 56 & 37 & 113 & 52 & 3 & 54 & 15 & 121 \\
36 & 40 & 44 & 10 & 19 & 109 & 105 & 4 & 114 & 111 & 83 & 50 & 74 & 0 & 107 & 28 \\
\end{array}
\]

\(K=\)

On adopting the procedure described in section 10.2, we get the substitution matrix in the form.

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

(10.4.4)

On applying the substitution process, we get the modified P, denoted by \(P^1\), as

\[
P^1 = \begin{bmatrix}
70 & 98 & 47 & 101 & 105 & 45 & 123 & 42 \\
53 & 64 & 59 & 117 & 112 & 97 & 58 & 40 \\
96 & 26 & 17 & 63 & 123 & 56 & 47 & 45 \\
83 & 103 & 101 & 4 & 83 & 101 & 19 & 125 \\
26 & 92 & 127 & 3 & 56 & 11 & 57 & 66 \\
55 & 56 & 92 & 82 & 53 & 80 & 8 \\
92 & 39 & 18 & 116 & 46 & 83 & 83 & 4 \\
115 & 1 & 59 & 100 & 92 & 67 & 4 & 111 \\
\end{bmatrix}
\]

(10.4.5)

After carrying out the interweaving process, we have
After carrying out all the sixteen rounds of the iteration procedure, we get the ciphertext in its final form as

\[
P^1 = \begin{bmatrix}
64 & 59 & 117 & 112 & 97 & 56 & 40 & 48 \\
24 & 17 & 127 & 123 & 52 & 47 & 45 & 115 \\
103 & 101 & 4 & 91 & 99 & 19 & 125 & 8 \\
93 & 63 & 3 & 52 & 9 & 57 & 98 & 63 \\
56 & 85 & 76 & 80 & 53 & 80 & 8 & 85 \\
39 & 34 & 120 & 47 & 83 & 115 & 4 & 117 \\
1 & 59 & 102 & 92 & 3 & 4 & 103 & 78 \\
68 & 95 & 73 & 82 & 123 & 110 & 86 & 43 \\
\end{bmatrix}
\]

(10.4.6)

In the process of decryption, we take the \( C \), obtained above, and apply the reverse substitution process (see section 10.2). Thus we get the \( P^N \) as

\[
P^N = \begin{bmatrix}
51 & 55 & 46 & 15 & 38 & 20 & 119 & 45 \\
117 & 120 & 67 & 98 & 51 & 31 & 98 & 84 \\
4 & 117 & 1 & 48 & 27 & 125 & 29 & 84 \\
75 & 79 & 104 & 74 & 10 & 5 & 30 & 72 \\
125 & 86 & 34 & 98 & 7 & 89 & 113 & 89 \\
123 & 76 & 104 & 109 & 80 & 45 & 9 & 10 \\
42 & 27 & 38 & 97 & 62 & 119 & 10 & 9 \\
108 & 105 & 3 & 27 & 12 & 103 & 125 & 23 \\
\end{bmatrix}
\]

(10.4.7)

On applying the inverse interweaving on the \( P^N \), obtained above, we have
After carrying out all the sixteen iterations, we get back the plaintext in the form

\[
P = \begin{bmatrix}
69 & 110 & 115 & 101 & 114 & 117 & 101 & 99 \\
118 & 32 & 32 & 118 & 115 & 110 & 118 & 107 \\
114 & 104 & 97 & 114 & 105 & 104 & 114 & 116 \\
121 & 97 & 100 & 121 & 112 & 101 & 121 & 32 \\
32 & 116 & 101 & 32 & 32 & 100 & 32 & 102 \\
103 & 32 & 44 & 119 & 108 & 44 & 114 & 105 \\
117 & 105 & 32 & 97 & 97 & 32 & 111 & 114 \\
\end{bmatrix}
\]

(10.4.10)

This is the same as the plaintext given in (10.4.2).

The ciphertext corresponding to the entire plaintext given by (10.4.1), in its hexadecimal form, is obtained as

\[
66DD70F4C53B4DEBE21E2667F15409D40B037F4ED4973F44A1414F48FB591620F678D9F73346DA0B448A546D3617DCC509D9A419B199FE976D30914BD7D9A691F18B5711A00542FFD14A8C2F6F1653697935808BA318F883A1D895AB081B153E258F29ADCD9B9CF95746DC8E3878AE6BFECCE98EC7AADCB92E765EFE052AB05CDBFD67A77402711A5DC286A.
\]

(10.4.11)

We now illustrate another example, wherein the entire plaintext given by (10.4.1) is taken as a single block. This plaintext is arranged in the form of a matrix of size 8x58. For convenience, it is represented as

\[
P = [AB], \text{ where } A \text{ and } B \text{ are shown in (10.4.13) and (10.4.14) respectively.}
\]
On applying the encryption process on the plaintext given by (10.4.12) & (10.4.13), we get the corresponding ciphertext, in hexadecimal notation, as

CE17B2B7B4F7DA52441C7B8E06F555A1B3BA254415D73ECD5DE2F1312D6B92882347054F90B5EC48ACDB813659A8F26C913D90770DA0784964FEFC9F6C308802181DFC14EDF6B4A51A20CA7FA70B5F50AA343868909E013B33C526F222E6F8D7B2F14A96D87EF2D9C0AD50D0DA7640907C9F5C15B213C890EED1BA21280005F322E69E58645E43F665109F4A. (10.4.14)

It can be readily verified that the above ciphertext can be brought back to its original form, by applying the decryption process.

In what follows, we discuss the avalanche effect, a desirable property of block ciphers, which shows how the confusion and diffusion are taking place in an effective manner.

10.5. AVALANCHE EFFECT

Let us examine this effect firstly, by changing the plaintext by one bit, and then by changing the key by one bit.
Here, it may be mentioned that the ciphertext, corresponding to the plaintext given by (10.4.2), in its binary form, is obtained as

\[011001101110110101000011101001100010101110111010101111\]
\[1010110110001000111011100011001110111011011100001010101000000\]
\[10011010100000010110000001111011110100111011101100101010101\]
\[1101111111010010100001010000001001100111101101000100111111011\]
\[01011000101000101000011101100111011011110110000100100110110\]
\[110110100011010110100001011000100001011001001100111011101100\]
\[110110101100010111010110111000010110111011001100110010111010\]
\[0000011001100110011001111101001011100100001111011000101111111011\]

(10.5.1)

On changing the 29th character of the plaintext given by (10.4.2), from y to x, i.e., from ASCII code 121 to 120, the plaintext changes by one bit. The ciphertext corresponding to the modified plaintext is obtained as

\[111000101011100100010011000101101111000110010110000110001110\]
\[0010110001110100100011100110000111011110011001100001010111101\]
\[0001111001010011100001010000111100110100011100001100011111111\]
\[1100010100110101101000010100011001111001101111101011001111010\]
\[110011011111010011110011001110110111001111011110110011111100\]
\[1000111111110100011101111111011111110111111111110111010010111\]

(10.5.2)

The ciphertexts given by (10.5.1) and (10.5.2) differ by 242 bits (out of 448 bits), which is significant.

We now change the key element K_{55} (i.e., 4th row and 7th column element of (10.4.4)) from 105 to 104. With this change, the key under consideration changes by one bit. If we using the modified key and the original plaintext given by (10.4.3), and applying the encryption algorithm, we get the corresponding ciphertext in the form
The ciphertexts (10.5.1) and (10.5.3) differ by 230 bits (out of 448 bits). This is also quite considerable.

From the above discussion, we conclude that this cipher exhibits strong avalanche effect.

10.6. CRYPTANALYSIS

The basic cryptanalytic attacks which are generally mentioned in the literature of cryptology are

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

However, a cipher is considered to be potential if it withstands the first two attacks [21].

Let us now examine the brute force attack. In this analysis, we have taken, randomly, sixty four distinct numbers, between 0 and 127, in the key. Thus, the size of the key space is $128^64$ (as sixty four distinct numbers are taken out of 128 distinct numbers). If we assume that the time required for the execution of the cipher with one value of the key in
the key space is $10^{-7}$ seconds, then the time required for the computation with all the possible keys is

$$\frac{128}{365 \times 24 \times 60 \times 60} P_{64} \times 10^{-7} = \frac{128 \times 3.12 \times 10^{-15}}{64!} \approx 9.48 \times 10^{111} \text{ years.}$$

As this time is enormously large, we cannot break the cipher with the brute force attack.

Let us now consider the known plaintext attack. In this case, we know as many plaintext and ciphertext pairs as we require to carry out the attack.

The basic equations governing this cipher are

1. $P = P_0$ \hspace{1cm} (10.6.1)
2. $P_i = \text{Substitute}(P_{i-1}), \; i = 1 \text{ to } 16$ \hspace{1cm} (10.6.2)
3. $P_i = \text{interweave}(P_i)$. \hspace{1cm} (10.6.3)

We may recall that the function Substitute and the function interweave that we are having in (10.6.2 and 10.6.3) both include intertwining (see section 10.2). Now, in order to have convenience in representation, we denote the function Substitute by $T$ and the function interweave by $\Omega$. Thus the relations (10.6.2) and (10.6.3) can be written in the form

4. $P_i = T(P_{i-1})$, \hspace{1cm} (10.6.4)
5. $P_i = \Omega(P_i)$. \hspace{1cm} (10.6.5)
On using the above relations, the ciphertext $C$, at the end of the iteration process, can be written in the form

$$C = T(\Omega(\cdots(T(\Omega(T(P))))\cdots))$$  \hspace{1cm} (10.6.6)

The plaintext $P$ occurring in this equation is typically under the control of the functions $T$ and $\Omega$. Hence, it cannot be taken out and transferred to the left side (in the form of inverse of $P$), so that, the key or a function of the key can be determined for breaking the cipher. Thus, we cannot break the cipher by the known plaintext attack.

In the light of the above discussion, we conclude that this cipher is a strong one and it is difficult to break this cipher by the conventional cryptanalytic attacks.

10.7. CONCLUSIONS

In this chapter, we have generalized the Playfair cipher by extending it from 26 characters of the English alphabet to the 128 ASCII character set. In this, we have modified the substitution process of the classical Playfair cipher by including a procedure which includes both interweaving and intertwining.

The algorithms designed in this analysis are implemented in C language.

The time required for encrypting the entire plaintext, taken as a single block, is $43.25 \times 10^{-3}$ seconds, and that for decrypting is $43.25 \times 10^{-3}$ seconds.
The cryptanalysis discussed in this chapter clearly reveal the strength of the cipher. Finally, we conclude that this cipher is a strong one and it is difficult to break this cipher by any conventional cryptanalytic attack.