CHAPTER 11

A NOVEL BLOCK CIPHER
WITH THE BLENDING OF
THE HILL CIPHER AND THE
PLAYFAIR CIPHER
11.1. INTRODUCTION

The study of the Hill cipher, basing upon the modular arithmetic inverse of a key matrix, has attracted several researchers in view of its potentiality and ease in computation. In the modified Hill cipher, the process of encryption and the process of decryption are governed by the relations

\[ C = KP \mod 128, \]  \hspace{1cm} (11.1.1)

and

\[ P = K^{-1}C \mod 128. \]  \hspace{1cm} (11.1.2)

where \( P \) is the plaintext, \( K \) the key matrix, \( C \) the ciphertext and \( K^{-1} \) is the modular arithmetic inverse of \( K \).

In all the latest investigations concerned to the modified Hill cipher, iteration plays a very prominent role. In addition to this interlacing, permutation and interweaving also contribute to the strength of the cipher in a remarkable manner.

Of late, we have devoted our attention to the study of the modification and generalization of the Playfair cipher and examined a set of problems, which lead to several interesting ciphers. In this analysis, the classical substitution table of the Playfair cipher is modified into a substitution matrix (containing the ASCII codes 0 to 127) of size 8x16, and the set of rules governing the substitution process are formulated appropriately. The modified Playfair cipher is found to be a strong one and an efficient one.
In the present chapter, we consider a blending of the modified Hill cipher and the modified Playfair cipher and developed a new block cipher.

Here, our objective is to see that the strength of the cipher increases on account of the interaction of the characteristic features occurring in both the Hill cipher and the Playfair cipher. In this analysis, we have applied the process of interweaving and the iteration together with the other procedures arising in the Hill cipher and Playfair cipher.

In section 11.2, we present the development of the cipher. We design the algorithms for encryption and decryption in section 11.3. In section 11.4, we illustrate the cipher with an example. We mention the avalanche effect in section 11.5, and discuss the cryptanalysis in section 11.6. Finally, in section 11.7, we draw conclusions from the computations carried out in this analysis.

**11.2. DEVELOPMENT OF THE CIPHER**

Consider a plaintext P, containing 16 characters. On using the ASCII code, P can be represented in the form of a matrix given by

\[ P = [P_{ij}], \text{ } i=1 \text{ to } 8, \text{ } j=1 \text{ to } 2. \]  \hspace{1cm} (11.2.1)

Let us choose a key K, containing 64 distinct numbers, that lie between 0 and 127. Let this be represented in the form of a matrix given by

\[ K = [K_{ij}], \text{ } i=1 \text{ to } 8, \text{ } j=1 \text{ to } 8. \]  \hspace{1cm} (11.2.2)
Then we form the substitution matrix (a primary component of the modified Playfair cipher) by putting the 64 distinct numbers of K (taken in a row wise manner) in the first four rows of the substitution matrix, and placing the rest of the numbers between 0 to 127 in their ascending order in the next four rows of the matrix. Thus, the substitution matrix assumes the form given by (11.2.3). In this, $R_i$, $i=1$ to 64 are the set of numbers, between 0 and 127, excluding the numbers $K_{ij}$, $i=1$ to 8, $j=1$ to 8.

$$
\begin{bmatrix}
K_{11} & K_{12} & K_{13} & K_{14} & K_{15} & K_{16} & K_{17} & K_{18} \\
K_{21} & K_{22} & K_{23} & K_{24} & K_{25} & K_{26} & K_{27} & K_{28} \\
K_{31} & K_{32} & K_{33} & K_{34} & K_{35} & K_{36} & K_{37} & K_{38} \\
K_{41} & K_{42} & K_{43} & K_{44} & K_{45} & K_{46} & K_{47} & K_{48}
\end{bmatrix}
$$

(11.2.3)

Following the modified Playfair cipher, the set of rules governing the substitution process can be written as follows.

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

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, $R_{39}$, $R_{39}$ will be replaced by $R_{40}$, $R_{40}$.

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, R31, R32 is replaced by R32, R17.

3. If A1 and A2 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, R45, R61 is replaced by R61, K25.

4. If A1 and A2 are distinct and fall in different rows and columns of the substitution matrix, then A1 is replaced by the number that exists in the same row as A1 and in the column of A2, and A2 is replaced by the number that exists in the same row as A2 and in the column of A1. For example, K36, R41 is replaced by K41, R38.

The procedure for the encryption and the decryption are shown in the schematic diagram given in Fig. 11.1.

In this, the steps P^i=KP^(i-1)mod128 and C=KP^Nmod128 are in accordance with the modified Hill cipher. The function substitute() deals with the substitution process governed by the set of rules 1 to 4, mentioned above.

The process of interweaving is represented by the function interweave(). This can be described as follows.

Consider any matrix given by A= [A_ij], i=1 to 8, j=1 to 2, where each element of A lies between 0 and 127. This enables us to represent each
element in terms of seven binary bits. Then, the matrix A can be written in the form

\[
b = \begin{bmatrix}
  b_{11} & b_{12} & \ldots & b_{14} \\
  b_{21} & b_{22} & \ldots & b_{24} \\
  \vdots & \vdots & \ddots & \vdots \\
  b_{81} & b_{82} & \ldots & b_{84}
\end{bmatrix}
\]  

(11.2.4)

Let us now focus our attention on the first column of the matrix b. We carry out a circular rotation on this column so that it takes the form \([b_{21}, b_{31}, \ldots, b_{81}, b_{11}]^T\), where T denotes the transpose of the vector. Here, each element of the column under consideration is moved up by one position and the first element occupies the last position. Similarly, all the odd numbered columns of b are rotated. We now perform a circular left shift, by one position, on all the even numbered rows of the matrix b. After this transformation, the matrix will be in the form

\[
b = \begin{bmatrix}
  b_{21} & b_{22} & b_{23} & \ldots & b_{24} & b_{14} \\
  b_{22} & b_{23} & b_{24} & \ldots & b_{25} & b_{15} \\
  \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
  b_{28} & b_{29} & b_{30} & \ldots & b_{34} & b_{11}
\end{bmatrix}
\]  

(11.2.5)

We now convert the binary bits in the matrix b, taken in a row wise manner, into their decimal equivalent and construct the modified matrix \([A_{ij}], i=1 \text{ to } 8, j=1 \text{ to } 2\). This completes the process of interweaving.

Each round in this cipher comprises the operations multiplication with the key matrix, substitution and interweaving. All these operations are carried out in an iterative manner. We denote the reverse process of
interweaving as inverse interweaving and that of substitution as reverse substitution. These are employed in the process of the decryption.

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

11.3.1 ALGORITHM FOR ENCRYPTION
1. read n,N,K,P;
2. \(P^0 = P\);
3. construct substitution matrix;
4. for \(i = 1\) to \(N\) {
   \(P^i = K^{P\text{-}1}\mod 128;\)
   substitute();
   interweave();
}
5. \(C = K^P \mod 128;\)
6. write \(C\);

11.3.2 ALGORITHM FOR DECRYPTION
1. read n,N,K,C;
2. find modinverse(K);
3. construct substitution matrix;
4. \(P^N = K^{-1}C \mod 128;\)
5. for \(i = N\) to \(1\) {
   invinterweave();
   reverse substitute();
   \(P^{i-1} = K^{-1}P^{i} \mod 128;\)
}
6. \(P = P^0;\)
7. write \(P;\)

11.3.3 ALGORITHM FOR MODINVERSE
1. read n,K;
2. find \(K_{ij}, \Delta;\) /* \(K_{ij}\) are the cofactors of the elements of \(K\) and \(\Delta\) is the determinant of \(K\) */
3. find \(d\) such that \((d\Delta) \mod 128 = 1;\) /* \(d\) is the multiplicative inverse of \(\Delta\) */
4. \(K^{-1} = (K_{ij}d) \mod 128;\)

11.3.4 ALGORITHM FOR INTERWEAVE
1. convert \(P^i\) into binary bits;
2. construct \([b_{ij}], i = 1\) to \(n, j = 1\) to 14;
3. for \(j = 1\) to 14 in step 2 {
   \(k = b_{ij};\)
   for \(i = 1\) to \(n-1\)
   {
      \(b_{ij} = b_{i+1}j;\)
   }
   \(b_{nj} = k;\)
}
4. for \(i = 2\) to \(n\) in step 2 {
   \(k = b_{11};\)
   for \(j = 1\) to 13 {

5. Construct $P_i$ from $b_{ij}$.

### 11.3.5 Algorithm for InvInterweave

1. convert $P_i$ into binary bits;
2. construct $[b_{ij}]$, $i=1$ to $n$, $j=1$ to 14;
3. for $i = n$ to 2 in step 2 {
   
   $k=b_{i14};$
   
   for $j = 14$ to 2 {
      
      $b_{ij}=b_{i(j-1)};$
      
      $b_{i1}=k;$
   }

   $b_{i1}=k;$
}

4. for $j = 13$ to 1 in step 2 {
   
   $k=b_{nj};$
   
   for $i = n$ to 2 {
      
      $b_{ij}=b_{i-1}j;$
      
      $b_{1j}=k;$
   }

   $b_{1j}=k;$
}

5. Construct $P_i$ from $b_{ij}$.

### 11.4. Illustration of the Cipher

Consider the plaintext given below.

The bomb blast which took place in the recent past in the cave must not be cared by any one of us. We must boldly fight out all the soldiers in the forest by surrounding them from all corners. This is my order. Do implement it and see that our country wins the enemies in this attempt. \[(11.4.1)\]

Let us focus our attention on the first sixteen characters of the above plaintext given by

The bomb blast w \[(11.4.2)\]

Using the ASCII code, these characters can be represented in the form of a matrix shown below:
Let the key matrix $K$ be represented as

$$K = \begin{bmatrix}
53 & 62 & 124 & 33 & 49 & 118 & 107 & 43 & 45 & 112 & 63 & 29 & 60 & 35 & 58 & 11 \\
88 & 41 & 46 & 30 & 48 & 32 & 15 & 51 & 47 & 99 & 38 & 42 & 12 & 59 & 27 & 61 \\
57 & 20 & 6 & 31 & 106 & 126 & 22 & 125 & 56 & 37 & 113 & 52 & 3 & 54 & 105 & 21 \\
36 & 40 & 44 & 100 & 119 & 39 & 55 & 94 & 14 & 81 & 23 & 50 & 34 & 70 & 7 & 28 \\
0 & 1 & 2 & 4 & 5 & 8 & 9 & 10 & 13 & 16 & 17 & 18 & 19 & 24 & 25 & 26 \\
64 & 65 & 66 & 67 & 68 & 69 & 71 & 72 & 73 & 74 & 75 & 76 & 77 & 78 & 79 & 80 \\
82 & 83 & 84 & 85 & 86 & 87 & 89 & 90 & 91 & 92 & 93 & 95 & 96 & 97 & 98 & 101 \\
\end{bmatrix} \quad (11.4.5)$$

The substitution matrix (see section 11.2) is given in (11.4.5).

On multiplying the plaintext with the $K$, and taking mod 128, we get the modified plaintext, denoted by $P^1$, as

$$P^1 = \begin{bmatrix}
17 & 5 \\
76 & 62 \\
23 & 29 \\
104 & 19 \\
0 & 32 \\
76 & 62 \\
74 & 119 \\
100 & 74
\end{bmatrix} \quad (11.4.6)$$
After carrying out the substitution process, we get the transformed plaintext $P^1$ as

$$
\begin{bmatrix}
18 & 8 \\
65 & 29 \\
50 & 63 \\
121 & 2 \\
8 & 88 \\
65 & 29 \\
68 & 81 \\
81 & 67 \\
\end{bmatrix}
$$

(11.4.7)

In the process of interweaving, we first convert the plaintext matrix, obtained above, into its binary form given by

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

(11.4.8)

On applying the interweaving process, the above matrix is transformed into

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

(11.4.9)

On converting the $b$ obtained above into decimal form, we get the modified $P^1$ as
After carrying out all the sixteen iterations, we get the ciphertext in its final form as

\[
\begin{bmatrix}
87 & 97 \\
81 & 33 \\
87 & 27 \\
116 & 44 \\
44 & 25 \\
0 & 82 \\
23 & 2 \\
52 & 118
\end{bmatrix}
\]

The modular arithmetic inverse of \(K\), denoted by \(K^{-1}\), is obtained as

\[
K^{-1} = 
\begin{bmatrix}
7 & 124 & 49 & 41 & 71 & 50 & 127 & 124 \\
33 & 64 & 65 & 80 & 69 & 65 & 24 & 81 \\
119 & 113 & 56 & 60 & 80 & 38 & 21 & 76 \\
56 & 51 & 48 & 83 & 118 & 46 & 40 & 105 \\
25 & 53 & 41 & 118 & 60 & 71 & 57 & 116 \\
49 & 122 & 64 & 118 & 115 & 112 & 47 & 28 \\
80 & 47 & 69 & 80 & 53 & 105 & 61 & 26 \\
47 & 125 & 87 & 98 & 116 & 104 & 125 & 41
\end{bmatrix}
\]

In the process of decryption, we multiply the \(C\) obtained above, with the \(K^{-1}\) and take mod 128. Thus we get the \(P^N\) in the form

\[
\begin{bmatrix}
37 & 115 \\
70 & 113 \\
125 & 14 \\
75 & 23 \\
42 & 109 \\
38 & 52 \\
33 & 43 \\
126 & 117
\end{bmatrix}
\]

On carrying out the inverse interweaving process, we get the modified \(P^N\) as
On applying the reverse substitution process, the transformed $P^N$ takes the form

$$p^N = \begin{bmatrix} 127 & 125 \\ 70 & 113 \\ 22 & 83 \\ 107 & 71 \\ 95 & 55 \\ 4 & 52 \\ 114 & 20 \\ 84 & 117 \end{bmatrix}$$

After carrying out all the sixteen iterations, we obtain the plaintext in its final form as

$$P = \begin{bmatrix} 84 & 32 \\ 104 & 98 \\ 101 & 108 \\ 32 & 97 \\ 98 & 115 \\ 111 & 116 \\ 109 & 32 \\ 98 & 119 \end{bmatrix}$$

This is the same as the plaintext given in (11.4.3).

In what follows, we examine the avalanche effect, a desirable property of all block ciphers.

**11.5. AVALANCHE EFFECT**

Let us study this effect in two cases, by considering (1) one bit change in the plaintext, and (2) one bit change in the key.
If we change the third character of (11.4.2) from $e$ to $d$ (i.e., from the ASCII code 101 to 100), the plaintext will undergo a change of one bit.

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

\begin{align*}
10101111010001101111101000101100000000000010111011010011 \\
00001010000100110110110110000110011010010000000101110110
\end{align*}

and

\begin{align*}
0011010111011110110001100111111101011010101011100101 \\
0101011111001010001100001000100000011110100010110010.
\end{align*}

(11.5.1) \hspace{1cm} (11.5.2)

It can be readily seen that (11.5.1) and (11.5.2) differ by 61 bits (out of 112 bits), which is quite significant.

We now change the key element $K_{45}$ from 12 to 76. With this change, the key under consideration changes by one bit. On using the modified key and the original plaintext, given in (11.4.2), and applying the encryption algorithm we get the corresponding ciphertext as

\begin{align*}
1101100111110111101011001111011011010010111001000101110010011 \\
011000101000000011110101011100000100101010101110110001.
\end{align*}

(11.5.3)

The ciphertexts given in (11.5.1) and (11.5.3) differ by 61 bits (out of 112 bits), which is also conspicuous.

From the above discussion, we find that the interweaving, the substitution and the multiplication with the key matrix involving the modular arithmetic, are causing confusion and diffusion in a significant manner.
11.6. CRYPTANALYSIS

Whenever a cipher is developed, in cryptography, the crucial problem associated with it is – whether the cipher can be broken within a reasonable amount of time or not. Examining this issue is the primary concern in cryptanalysis.

The cryptanalytic attacks available in the study of cryptology for breaking a cipher are

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

However, any cipher which can withstand the first two attacks can be considered as up to the mark, as it is very well pointed by William Stallings [21].

In this cipher, the key is containing 64 distinct numbers lying between 0 and 127. Hence the size of the key space is \(128^{64}\). 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 execution of the cipher with all the keys in the key space is

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

As this number is extremely large, we notice that this cipher cannot be broken by the brute force attack.
Let us now focus our attention on the known plaintext attack. In this case, we have any number of plaintext and ciphertext pairs that we require for the purpose of our analysis. The basic relations governing this cipher are

\[ P_0 = P, \]  
\[ P_i = K(P_{i-1}) \mod 128, \text{ } i = 1 \text{ to } 16 \]  
\[ P_i = S(P_i), \text{ and} \]  
\[ P_i = \Psi(P_i). \]  

Here, \( S \) denotes the function substitute, and \( \Psi \) denotes the function interweave. This notation is used for simplicity in presentation.

On using the encryption algorithm, containing the afore mentioned relations, the relation connecting the ciphertext and the plaintext (at the end of the iteration process) can be obtained in the form

\[ C = (K(\Psi(S(\ldots(K(\Psi(S(KP \mod 128)) \mod 128)) \ldots)) \mod 128). \]

The plaintext \( P \), which is totally under the operation of the substitution and the interweaving, it cannot be transferred to the left side by taking the modular arithmetic inverse of the \( P \), as it could be done in the case of the classical Hill cipher. Thus, this cipher cannot be broken by the known plaintext attack.

In the light of the above facts, we find that it is difficult to be break this cipher by the conventional cryptanalytic attacks, and hence, it is a strong one.
11.7. COMPUTATIONS AND CONCLUSIONS

In this chapter, we have developed a block cipher by including the basic features of the Hill cipher and the Playfair cipher. In this, the multiplication of the plaintext block with the key matrix, involving modular arithmetic, and the use of the substitution matrix (formed by using the key) together with interweaving and iteration play a dominant role in the development of the cipher.

The algorithms designed for the encryption and the decryption in this analysis are implemented in C language.

The ciphertext corresponding to the entire plaintext given in (11.4.1), in hexadecimal notation, is obtained as follows:

\[
\text{AF46BF45800BB4C284DAC3348176E672B5D5E32742BFB3E0D524AA}
\]
\[
880968661965CFFDE6F74F59569C72681070EB0E88CEAF142A38438
\]
\[
066DC82B37408F0D26F3D8494D1DF30C87DDF42C99A5800F7738F8
\]
\[
E26BF8084D161390AA58B00EC86889FBE6D036CAD9235BCDD6BB7
\]
\[
46E26406BC66ECEF01015F9608BA0D9D765A3D703E7CDE8D56C8CE
\]
\[
4A9D62E098. \quad (11.7.1)
\]

The time required for encrypting the complete plaintext, given in (11.4.1), is \(11.5 \times 10^{-3}\) seconds, and the time for decryption is \(16.5 \times 10^{-3}\) seconds. This shows that this cipher is an efficient one.

From the cryptanalysis presented in this chapter, we find that the strength of the cipher is considerable.

From the above analysis, we conclude that this cipher is a strong one and an efficient one, and it is difficult to break this cipher by conventional attacks.