International Journal of Computer Theory and Engineering, Vol. 2, No. 5, October, 2010
1793-8201

A Block Cipher Having a Key on One Side of the Plain Text Matrix and its Inverse on the Other Side

Dr. V. U. K. Sastry[1], Prof. D. S. R. Murthy[2], Dr. S. Durga Bhavani[3]

***Abstract*—In this paper, we have modified the Hill cipher by developing an iterative procedure consisting of three steps. In the first step, the plain text matrix is multiplied with the key matrix on one side and with its inverse on the other side. In the second step, the plain text matrix is mixed thoroughly by using a function called Mix ( ). In the last step, the plain text matrix is modified by using XOR operation between the plain text matrix and the key matrix. The cryptanalysis and the avalanche effect discussed in this paper, conspicuously indicate that the cipher is a strong one and it is quite comparable with the other block ciphers.**

***Index Terms*—Block cipher, Key, Modular arithmetic inverse, Encryption, Decryption.**

I. Introduction

In a recent paper [1], we have developed a block cipher by modifying the Hill cipher. In this, we have introduced an iterative scheme, which includes the key K as a multiplier on both the sides of the plain text matrix. Here, we have adopted a procedure, in which we have used a function called Mix ( ) for mixing the plain text at every stage of the iteration, and applied XOR operation between the plain text matrix and the key matrix. In this analysis, we have seen that the strength of the cipher is quite significant and it cannot be broken by any cryptanalytic attack.

In the present paper, our objective is to develop another modification of the Hill cipher, by including both K and K^{-1} (one on the left side and another on the right side of the plain text matrix) in encryption as well as in decryption, instead of having only K in encryption and K^{-1} in decryption. As in [1], here also we have made use of Mix ( ) function and applied the XOR operation between the plain text matrix and the key matrix.

In section 2, we have presented the development of the cipher. We have illustrated the cipher in two different cases, and exhibited the avalanche effect in section 3. We have discussed the cryptanalysis in section 4. Finally, we have drawn conclusions in section 5.

Manuscript received January 9, 2010.
[1]Dr. V. U. K. Sastry is with Dept. of Computer Science & Engg., SNIST, Hyderabad, India, (e-mail: vuksastry@rediffmail.com).
[2]Prof. D. S. R. Murthy is with Dept. of Information Technology, SNIST, Hyderabad, India, (e-mail: dsrmurthy.1406@gmail.com).
[3]Dr. S. Durga Bhavani is with School of Information Technology, SIT, JNTUH, Hyderabad, India, (e-mail: sdurga.bhavani@gmail.com).

II. Development of The Cipher

Consider a plain text P which can be represented in the form of a square matrix given by

P = [P_{ij}], i = 1 to n, j = 1 to n, (2.1)

where each P_{ij} is equal to 0 or 1.

Let us choose a key k. Let it be represented in the form of a matrix given by

K = [K_{ij}], i = 1 to n, j = 1 to n, (2.2)

where each K_{ij} is a binary number.

Let

C = [C_{ij}], i = 1 to n, j = 1 to n (2.3)

be the corresponding cipher text matrix.

The process of encryption and the process of decryption adopted in this analysis are given in Fig. 1.

Here r denotes the number of rounds in the iteration process. In the process of encryption, we have the iteration scheme which includes the relations

$$P = (KPK^{-1}) \bmod 2, \quad (2.4)$$

$$P = \text{Mix}(P), \quad (2.5)$$

and $P = P \oplus K.$ (2.6)

The relation (2.4) is used to achieve diffusion, while the relations (2.5) and (2.6) are used to acquire confusion. The function **Mix (P)** mixes the plain text at every stage of the iteration. For a detailed discussion of this function, we may refer to [1]. In the process of decryption, the function IMix represents the reverse process of Mix.

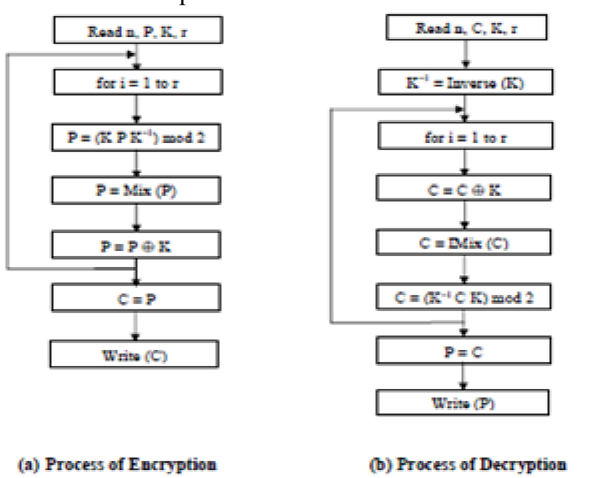

Fig. Scbematic diagram of the cipber

In what follows, we present the algorithms for encryption, decryption, and for the modular arithmetic inverse of a square matrix.

Algorithm for Encryption

1. Read n, P, K, r
2. K^{-1} = Inverse (K)
3. for i = 1 to r

   {

   P = $(K P K^{-1})$ mod 2

   P = Mix (P)

   P = P ⊕ K

   }
4. C = P
5. Write (C)

Algorithm for Decryption

1. Read n, C, K, r
2. K^{-1} = Inverse (K)
3. for i = 1 to r

   {

   C = C ⊕ K

   C = IMix (C)

   C = $(K^{-1} C K)$ mod 2

   }
4. P = C
5. Write (P)

Algorithm for Inverse (K)

// The arithmetic inverse (A^{-1}), and the determinant of the matrix (Δ) are obtained by Gauss reduction method.

1. A = K, N = 2
2. $A^{-1} = [A_{ji}] / \Delta$, i = 1 to n, j = 1 to n //A_{ji} are the cofactors of a_{ij}, where a_{ij} are elements of A, and Δ is the determinant of A
3. for i = 1 to n

   {

   if ((i Δ) mod N = 1)

   d = i;

   break;

   }
4. B = $[d A_{ji}]$ mod N // B is the modular arithmetic inverse of A

III. Illustration Of The Cipher

Let us consider the following plain text.

Just now we have received the news from the border security that all the planes coming from north west corner of the country by today mid–night are containing terrorists. Shoot the planes without any second thought. Finish! (3.1)

Let us focus our attention on the first 32 characters of the above plain text. This is given by

Just now we have received the ne. (3.2)

On using the EBCDIC code, the plain text under consideration can be written in the Hexadecimal notation as follows:

D1 A4 A2 A3 40 95 96 A6 40 A6 85 40 88 81 A5 85

40 99 85 83 85 89 A5 85 84 40 A3 88 85 40 95 85. (3.3)

On placing two numbers in each row, that is, D1 A4 in the first row, A2 A3 in the second row, etc., the plain text matrix P can be written in the binary form as

$$P = \begin{pmatrix}
1&1&0&1&0&0&0&1&1&0&1&0&0&1&0&0\\
1&0&1&0&0&0&1&0&1&0&1&0&0&0&1&1\\
0&1&0&0&0&0&0&0&1&0&0&1&0&1&0&1\\
1&0&0&1&0&1&1&0&1&0&1&0&0&1&1&0\\
0&1&0&0&0&0&0&0&1&0&1&0&0&1&1&0\\
1&0&0&0&0&1&0&1&0&1&0&0&0&0&0&0\\
1&0&0&0&1&0&0&0&1&0&0&0&0&0&0&1\\
1&0&1&0&0&1&0&1&1&0&0&0&0&1&0&1\\
0&1&0&0&0&0&0&0&1&0&0&1&1&0&0&1\\
1&0&0&0&0&1&0&1&1&0&0&0&0&0&1&1\\
1&0&0&0&0&1&0&1&1&0&0&0&1&0&0&1\\
1&0&1&0&0&1&0&1&1&0&0&0&0&1&0&1\\
1&0&0&0&0&1&0&0&0&1&0&0&0&0&0&0\\
1&0&1&0&0&0&1&1&1&0&0&0&1&0&0&0\\
1&0&0&0&0&1&0&1&0&1&0&0&0&0&0&0\\
1&0&0&1&0&1&0&1&1&0&0&0&0&1&0&1
\end{pmatrix} \quad (3.4)$$

Let us choose a key k consisting of 32 decimal numbers. Thus, we have

$$k = \left\{\begin{matrix} 131\ 31\ 18\ 59\ 254\ 126\ 113\ 97\ 127\ 167\ 76\ 116\ 111\ 159\ 245\ 159 \\ 175\ 50\ 236\ 107\ 235\ 74\ 47\ 20\ 190\ 80\ 242\ 139\ 175\ 164\ 187\ 158 \end{matrix}\right\} \quad (3.5)$$

Then k can be written in the form of a matrix given by

$$K = \begin{bmatrix}
1&0&0&0&0&0&1&1&0&0&0&1&1&1&1&1\\
0&0&0&1&0&0&1&0&0&0&1&1&1&0&1&1\\
1&1&1&1&1&1&1&0&0&1&1&1&1&1&1&0\\
0&1&1&1&0&0&0&1&0&1&1&0&0&0&0&1\\
0&1&1&1&1&1&1&1&1&0&1&1&0&1&1&1\\
0&1&0&0&1&1&0&0&0&1&1&1&0&1&0&0\\
0&1&1&0&1&1&1&1&1&0&0&1&1&1&1&1\\
1&1&1&1&0&1&0&1&1&0&0&1&1&1&1&1\\
1&0&1&0&1&1&1&1&0&0&1&1&0&0&1&0\\
1&1&1&0&1&0&1&0&0&1&1&0&1&0&1&1\\
1&1&1&0&1&0&0&1&0&1&0&0&1&0&1&0\\
0&0&1&0&1&1&1&1&0&0&0&1&0&1&0&0\\
1&0&1&1&1&1&1&0&0&1&0&1&0&0&0&0\\
1&1&1&1&0&0&1&0&1&0&0&0&1&0&1&1\\
1&0&1&0&1&1&1&1&1&0&1&0&0&1&0&0\\
1&0&1&1&1&0&1&1&1&0&0&1&1&1&1&0
\end{bmatrix} \quad (3.6)$$

On using the algorithm given in section 2, the modular arithmetic inverse of K can be obtained as

$$K^{-1} = \begin{bmatrix}
0&1&0&1&0&1&1&0&0&1&0&1&1&0&0&1\\
0&1&0&1&1&1&0&1&1&1&1&0&0&1&0&1\\
0&0&0&1&1&1&0&1&1&1&1&1&0&0&1&1\\
1&1&1&1&1&0&0&0&1&1&1&1&0&1&0&0\\
0&0&0&1&1&1&0&0&1&1&1&0&0&1&1&1\\
1&0&1&0&1&1&0&0&1&1&1&0&0&1&1&1\\
1&0&1&1&0&0&0&1&0&1&0&0&1&0&1&0\\
0&0&1&1&0&1&0&1&0&1&0&1&0&1&0&0\\
0&0&1&0&0&1&0&0&0&1&0&0&1&1&1&1\\
0&0&0&1&1&0&0&1&1&1&0&0&1&0&0&0\\
1&1&0&1&1&0&0&1&1&1&0&1&0&0&0&0\\
1&0&1&0&1&0&1&1&1&1&0&1&0&1&0&0\\
0&0&1&0&1&0&1&1&0&0&1&0&0&1&0&0\\
1&0&0&0&0&0&1&0&0&0&1&0&1&0&0&1\\
0&0&0&0&1&1&0&1&0&0&1&1&0&0&0&0\\
0&1&0&1&1&1&0&1&1&0&1&0&1&1&1&0
\end{bmatrix} \quad (3.7)$$

On using (3.6) and (3.7), it can be readily shown that

$$\mathbf{K\,K^{-1} \bmod 2 = K^{-1}K \bmod 2 = I}. \quad (3.8)$$

On applying the encryption algorithm, described in Section 2, we get the cipher text C in the form

$$C=\begin{bmatrix}
1&1&0&0&0&0&1&0&0&1&1&0&0&0&0&0\\
0&0&0&0&1&1&1&0&1&1&1&1&1&1&1&1\\
0&0&0&1&0&1&0&1&1&1&1&1&1&1&1&0\\
1&0&0&1&0&0&1&1&1&0&0&0&1&0&0&0\\
0&1&0&1&1&0&1&1&0&1&0&1&1&1&0&1\\
1&1&1&1&0&1&1&1&1&1&1&1&1&1&1&1\\
0&1&1&0&0&0&0&0&1&0&0&0&0&1&0&1\\
1&0&1&0&0&0&0&0&1&1&0&0&1&1&0&0\\
0&0&1&0&1&1&1&0&1&0&1&1&0&0&0&0\\
1&0&0&1&1&1&1&0&0&0&1&1&0&1&0&0\\
1&0&1&1&1&0&1&1&0&1&1&0&1&1&1&0\\
0&0&0&1&0&1&0&1&0&0&1&0&1&1&0&1\\
1&1&0&0&0&0&0&1&1&0&0&0&1&0&0&0\\
0&1&0&1&0&0&1&1&0&0&1&1&1&0&0&1\\
1&1&1&0&1&1&1&0&1&1&1&0&1&1&0&1\\
0&0&0&1&0&1&0&1&0&1&0&0&1&0&1&1
\end{bmatrix} \tag{3.9}$$

On using (3.6), (3.7), and (3.9), and applying the decryption algorithm described in section 2, we get the Plain text P, which is the same as (3.4).

Let us now discuss the avalanche effect. Here, we modify the 11th character 'e' in (3.2) to 'd'. Then the plain text changes only in one binary bit as the EBCDIC codes of e and d are 85 and 84 respectively.

On using the modified plain text and the encryption algorithm, we get the cipher text C in the form

$$C=\begin{bmatrix}
0&1&0&1&1&1&0&0&0&1&1&0&1&0&0&0\\
0&1&1&1&0&1&0&1&0&1&0&0&0&1&0&1\\
0&0&1&1&1&1&0&1&0&0&1&1&1&0&1&0\\
0&0&1&0&0&0&0&0&1&0&1&0&0&0&1&0\\
1&0&1&1&0&0&0&1&1&0&1&1&0&1&0&0\\
1&1&0&0&1&0&0&0&0&1&0&0&0&0&1&1\\
1&1&0&1&1&0&0&1&0&0&1&1&0&0&0&0\\
0&0&1&1&1&1&0&1&0&0&1&0&1&0&0&1\\
1&0&1&0&1&1&1&0&0&0&0&0&0&1&0&0\\
1&0&0&1&0&0&0&1&0&1&0&1&0&1&1&0\\
0&1&1&0&0&1&1&0&0&0&1&1&1&1&1&0\\
0&0&1&0&1&1&0&0&0&0&0&0&1&1&0&0\\
1&0&0&1&1&1&1&1&1&1&0&1&0&0&1&1\\
0&0&0&0&0&0&1&0&1&1&1&0&1&1&0&1\\
0&0&1&0&1&0&0&0&1&1&0&1&0&0&0&0\\
1&1&1&1&1&0&0&1&1&0&0&0&1&1&0&1
\end{bmatrix} \tag{3.10}$$

On comparing (3.9) and (3.10), we find that the two cipher texts differ in 132 bits out of 256 bits, which is quite significant.

Now let us change the key in (3.5) by 1 binary bit. This can be achieved by replacing the 3rd element 18 of the key k by 19. Then on using the original plain text (3.4), the modified key and the encryption algorithm, we get C in the form

$$C=\begin{bmatrix}
1&1&0&0&0&0&1&0&0&1&1&0&0&0&0&0\\
0&0&0&0&1&1&1&0&1&1&1&1&1&1&1&1\\
0&0&0&1&0&1&0&1&1&1&1&1&1&1&1&0\\
1&0&0&1&0&0&1&1&1&0&0&0&1&0&0&0\\
0&1&0&1&1&0&1&1&0&1&0&1&1&1&0&1\\
1&1&1&1&0&1&1&1&1&1&1&1&1&1&1&1\\
0&1&1&0&0&0&0&0&1&0&0&0&0&1&0&1\\
1&0&1&0&0&0&0&0&1&1&0&0&1&1&0&0\\
0&0&1&0&1&1&1&0&1&0&1&1&0&0&0&0\\
1&0&0&1&1&1&1&0&0&0&1&1&0&1&0&0\\
1&0&1&1&1&0&1&1&0&1&1&0&1&1&1&0\\
0&0&0&1&0&1&0&1&0&0&1&0&1&1&0&1\\
1&1&0&0&0&0&0&1&1&0&0&0&1&0&0&0\\
0&1&0&1&0&0&1&1&0&0&1&1&1&0&0&1\\
1&1&1&0&1&1&1&0&1&1&1&0&1&1&0&1\\
0&0&0&1&0&1&0&1&0&1&0&0&1&0&1&1
\end{bmatrix} \tag{3.11}$$

On comparing (3.11) with (3.9), we find that the cipher texts differ in 114 bits.

From the above analysis, we find that the Avalanche effect is quite pronounced and hence the cipher is a strong one.

By decomposing the entire plain text given by (3.1) into blocks, wherein each block is of size 32 characters, the corresponding cipher text can be written in hexadecimal notation in the form

C2	60	0E	FF	15	FE	93	88	5B	5D	F7	FF	60	85	A0	CC
2E	B0	9E	34	BB	6E	15	2D	C1	88	53	39	EE	ED	15	4B
A4	2A	12	36	93	3F	56	53	3B	7E	00	9C	60	3B	0E	D8
26	82	73	60	E7	FB	49	2C	E1	52	CC	20	28	2D	EA	65
79	67	F5	4D	36	EB	EC	44	C1	49	8F	BF	0F	31	74	64
EA	A5	65	09	8B	9E	D4	24	C6	6C	E5	EE	BC	CC	50	99
E1	41	7D	0E	14	D5	31	7A	A6	95	98	14	E1	C9	CC	71
08	3F	0B	29	16	62	7F	B7	DA	F4	CF	28	C4	58	CF	FE
6C	9D	DF	F7	F2	F1	33	75	4B	DF	33	06	8D	D7	FA	BA
3B	94	F6	01	8F	9E	2C	2A	EC	79	A4	2F	56	DD	99	7E
A3	63	D9	B8	AA	0C	8D	07	CC	38	0C	4F	EC	27	B9	8C
03	FF	FA	CB	69	90	A0	DD	62	55	39	F5	BF	AD	66	ED
76	3B	EF	A2	7E	5E	29	78	7B	FC	DE	DA	82	64	BE	C3
49	D9	4B	CB	9F	71	FC	5E	86	8B	04	2B	31	48	E8	3C

(3.12)

The problem under consideration can also be studied, in the case when K and K^{-1} are interchanged, i.e., when (2.4) is replaced by

$$\mathbf{P = (K^{-1}\,P\,K) \bmod 2}. \tag{3.13}$$

This amounts to interchanging K and K^{-1} in (2.4). Corresponding changes can be made in the algorithms. In this case, the C is given by

$$C=\begin{bmatrix}
1&1&1&0&0&0&1&1&1&1&0&0&0&0&1&0\\
1&0&0&1&0&1&1&0&0&0&0&0&0&0&1&0\\
0&1&1&0&1&0&0&0&0&0&1&0&0&0&0&1\\
0&0&0&1&0&0&1&0&0&1&1&1&0&0&0&1\\
0&1&1&1&0&0&1&1&1&0&1&1&0&1&0&1\\
0&0&1&0&0&0&1&1&0&1&1&0&1&0&0&0\\
0&1&0&1&0&1&0&0&0&1&0&1&0&1&1&0\\
1&0&1&1&0&1&1&0&1&0&1&0&1&0&1&1\\
0&0&0&1&0&1&1&0&1&1&0&1&0&0&0&0\\
0&1&1&0&0&1&0&0&1&0&1&0&1&1&0&1\\
1&1&0&1&1&0&0&0&0&0&1&0&1&0&1&1\\
0&1&0&1&1&0&0&0&0&0&0&0&1&1&0&0\\
1&1&0&0&1&0&1&1&0&0&1&1&0&0&1&1\\
1&1&0&0&0&0&1&0&1&0&1&0&1&0&1&0\\
0&0&0&1&1&1&1&1&0&0&1&1&0&1&1&0\\
0&0&0&0&1&0&0&0&1&1&1&1&1&0&0&0
\end{bmatrix} \tag{3.14}$$

Though we have got a different cipher text, on account of modifications, we have obtained the same plain text P by performing decryption.

When the plain text P is changed by one bit (i.e., the 11th character 'e' is changed to 'd'), then the corresponding cipher text assumes the form

$$C=\begin{bmatrix}
0&1&1&0&0&1&0&0&1&0&0&1&0&1&0&0\\
1&1&1&0&0&1&1&0&0&1&1&0&0&0&1&0\\
1&0&1&0&1&1&0&0&0&1&0&1&0&1&0&0\\
1&0&1&0&0&1&1&1&1&1&0&0&1&1&1&1\\
0&1&0&0&0&1&0&1&1&1&1&0&0&0&1&0\\
1&0&1&1&0&0&0&1&0&1&1&1&0&1&1&1\\
0&0&1&1&0&0&0&1&1&0&0&0&1&0&0&1\\
1&0&1&0&0&0&1&1&1&0&0&0&1&0&0&1\\
1&0&1&0&0&1&1&0&0&1&0&1&1&1&0&0\\
1&0&0&0&0&0&1&0&0&1&0&0&1&1&1&0\\
0&1&0&1&0&1&1&0&1&0&1&0&1&1&1&1\\
1&1&0&1&1&0&0&1&0&1&1&0&0&0&0&0\\
1&0&1&1&0&1&0&0&0&0&0&0&0&0&0&1\\
1&0&0&0&1&0&0&1&1&1&0&1&0&0&0&1\\
1&1&0&0&1&0&1&0&1&1&0&1&0&1&0&1\\
0&1&0&1&1&1&0&1&0&0&0&0&1&0&1&1
\end{bmatrix} \tag{3.15}$$

Thus in this case, the change in the cipher text is 133 bits out of 256 bits.

On changing 1 bit in the key (i.e., replacing 18 by 19), we have

$$C=\begin{bmatrix}
0&0&1&1&1&0&0&1&1&1&1&1&1&0&0&1\\
1&1&0&1&1&1&0&1&1&1&1&1&1&1&0&1\\
1&0&0&0&0&0&0&0&0&0&1&1&0&1&1&0\\
1&0&1&1&1&0&1&0&0&0&1&0&0&0&0&1\\
0&1&1&1&0&0&1&0&0&0&0&1&1&1&0&0\\
0&1&0&1&0&0&0&1&0&0&0&0&0&0&0&0\\
1&0&1&0&0&0&0&1&0&1&1&0&0&1&1&1\\
1&0&1&1&0&0&1&1&1&1&1&0&1&0&1&1\\
0&1&0&0&1&0&1&0&1&1&1&0&0&0&1&0\\
0&0&1&0&0&0&1&0&1&0&0&0&1&1&1&0\\
0&0&1&0&1&1&0&0&1&0&0&0&0&0&1&1\\
1&1&0&1&0&0&0&1&1&0&1&0&1&0&1&1\\
0&1&1&0&0&1&0&0&0&0&1&0&0&0&0&0\\
1&1&0&1&1&0&1&1&0&0&1&1&0&1&0&1\\
0&0&0&0&0&0&0&1&1&0&0&1&0&0&0&0\\
0&1&0&1&1&1&0&1&1&0&0&0&0&0&0&1
\end{bmatrix} \tag{3.16}$$

From (3.14) and (3.16), we notice the change in C is 123 bits out of 256 bits. From the above analysis, we find that the Avalanche effect is quite significant and hence this cipher is also is a very strong one.

In this case, the cipher text corresponding to the entire plain text (3.1), in hexadecimal form, is given by

E3	C2	96	02	68	21	12	71	73	B5	23	68	54	56	B6	AB	
16	D0	64	AD	D8	2B	58	0C	CB	33	C2	AA	1F	36	08	F8	
44	10	72	F8	CF	D6	9B	B1	3A	95	BC	A0	4A	85	B8	81	
19	98	64	BB	83	70	67	5B	07	D5	15	9C	63	8C	9C	CC	
84	F4	E8	12	2B	DB	50	87	63	A4	A0	34	68	DD	B9	CC	
0A	FE	D0	80	EC	61	86	49	6C	FC	C8	B5	DD	8E	AD	B5	
82	5B	CA	E6	CB	E7	91	2F	FF	5C	D5	B1	7B	25	62	5B	
47	B1	98	B6	29	E5	52	C7	1D	44	D9	CF	D0	DC	05	40	
8D	D4	FB	F9	A6	66	D7	4E	25	68	7E	52	8A	9A	6D	D7	
D0	46	7C	FF	A6	23	AA	5D	37	C8	22	A1	B7	53	06	6A	
79	5E	7D	86	1C	33	5E	C6	15	05	23	54	C2	8C	A9	F3	
A1	4A	1B	F9	25	96	B5	DE	C1	64	CD	27	65	6F	EA	1A	
97	18	7B	BC	EA	88	3E	79	BE	C4	10	06	D0	5D	4E	66	
77	ED	17	DD	2A	BE	53	64	9E	95	CD	87	4A	CB	36	39	(3.17)

IV. Cryptanalysis

The different types of cryptanalytical attacks available in the literature are:

(1) Cipher text only attack,
(2) Known plain text attack,
(3) Chosen plain text attack,
(4) Chosen cipher text attack.

When the cipher text is known to us, we can determine the plain text, if the key is known. As the key contains 32 decimal numbers, the key space is of size

$$2^{256} \simeq (10^3)^{25.6} = 10^{76.8}.$$

As the computation of the cipher text corresponding to all possible keys would take a very large amount of time, the cipher cannot be broken by the brute force approach.

We know that, the Hill cipher can be broken by the known plain text attack, as we can form a direct relation between C and P. But in the present modification, which involves K and K^{-1}, one on the left side of P and the other on the right side of P, and the process of iteration together with the Mix function and the XOR operation, we cannot get a direct relation between C and P. Hence, this cipher developed in this analysis cannot be broken by the known plain text attack.

The chosen plain / cipher text attack is totally ruled out as the steps involved in the cipher are typical in nature.

V. Conclusions

In this paper, we have modified the Hill cipher, governed by the single relation

$$\mathbf{C = (K\,P) \bmod 26}, \tag{5.1}$$

in two different cases.

In case one, the iterative scheme includes the relations

$$\mathbf{P = (K\,P\,K^{-1}) \bmod 2}, \tag{5.2}$$

$$\mathbf{P = Mix\,(P)}, \tag{5.3}$$

and $\mathbf{P = P \oplus K}$,

(5.4)

and in case two, it includes the relations

$$\mathbf{P = (K^{-1}\,P\,K) \bmod 2}, \tag{5.5}$$

$$\mathbf{P = Mix\,(P)}, \tag{5.6}$$

and $\mathbf{P = P \oplus K}$. (5.7)

In this analysis, the length of the plain text block is 256 bits and the length of the cipher text block is also 256 bits. As the cryptanalysis clearly indicates, this cipher is a strong one and it cannot be broken by any cryptanalytic attack. This analysis can be extended to a block of any size by using the concept of interlacing [2].

References

[1] V. U. K. Sastry, D. S. R. Murthy, S. Durga Bhavani, "A Block Cipher Involving a Key Applied on Both the Sides of the Plain Text", International Journal of Computer and Network Security (IJCNS), Vol. 1, No. 1, pp. 27 -30, Oct. 2009.

[2] V. U. K. Sastry, V. Janaki, "A Modified Hill Cipher with Multiple Keys", International Journal of Computational Science, Vol. 2, No. 6, 815 – 826, Dec. 2008.

Dr. V. U. K. Sastry is presently working as Professor in the Dept. of Computer Science and Engineering (CSE), Director (SCSI), Dean (R & D), SreeNidhi Institute of Science and Technology (SNIST), Hyderabad, India. He was Formerly Professor in IIT, Kharagpur, India and worked in IIT, Kharagpur during 1963 – 1998. He guided 12 PhDs, and published more than 40 research papers in various international journals. His research interests are Network Security & Cryptography, Image Processing, Data Mining and Genetic Algorithms.

Dr. S. Durga Bhavani is presently working as Professor in School of Information Technology (SIT), JNTUH, Hyderabad, India. She has more than 18 years of teaching experience. Her research area includes Evidential Reasoning, Cryptography and Image Processing. She has no. of research publications to her credit.

Prof. D. S. R. Murthy obtained B. E. (Electronics) from Bangalore University in 1982, M. Tech. (CSE) from Osmania University in 1985 and presently pursuing Ph.D. from JNTUH, Hyderabad since 2007. He is presently working as Professor in the Dept. of Information Technology (IT), SNIST since Oct. 2004. He earlier worked as Lecturer in CSE, NIT (formerly REC), Warangal, India during Sep. 1985 – Feb. 1993, as Assistant Professor in CSE, JNTUCE, Anantapur, India during Feb. 1993 – May 1998, as Academic Coordinator, ISM, Icfaian Foundation, Hyderabad, India during May 1998 – May 2001 and as Associate Professor in CSE, SNIST during May 2001 - Sept. 2004. He worked as Head of the Dept. of CSE, JNTUCE, Anantapur during Jan. 1996 – Jan 1998, Dept. of IT, SNIST during Apr. 2005 – May 2006, and Oct. 2007 – Feb. 2009. He is a Fellow of IE(I), Fellow of IETE, Senior Life Member of CSI, Life Member of ISTE, Life Member of SSI, DOEACC Expert member, and Chartered Engineer (IE(I) & IETE). He published a text book on C Programming & Data Structures. His research interests are Image Processing and Image Cryptography and published research papers in International Journal of Computer and Network Security (IJCNS) and International Journal of Computer Theory and Engineering (IJCTE).