Journal of Computer Science 4 (1): 15-20, 2008
ISSN 1549-3636

Modified Hill Cipher for a Large Block of Plaintext with Interlacing and Iteration

V.U.K. Sastry and N. Ravi Shankar
School of Computer Science and Informatics
Sreenidhi Institute of Science and Technology Hyderabad, India

Abstract: In this research, we have developed a large block cipher by modifying the Hill cipher. In this, we have introduced interlacing of the binary bits of the plaintext as the primary concept leading to confusion. This process is strengthened by using iteration. The cryptanalysis and avalanche effect mentioned in this research clearly exhibit the strength of the cipher.

Key words: Modular arithmetic inverse, interlacing, decomposition

INTRODUCTION

In a recent research[1], we have developed a block cipher using a large key matrix. In this, we have used interlacing of the binary bits of the plaintext vectors, occurring in the plaintext matrix, as the primary concept. Here, the multiplication of the plaintext with the key causes diffusion and the interlacing of the plaintext at various stages of iteration causes confusion in an effective manner.

In the present research, our objective is to develop a block cipher, wherein the block is taken in the form of a large matrix. In this, we illustrate the cipher by giving a pair of examples. In the first one, the plaintext block is taken in the form of an 8×8 matrix and in the second one, it is taken as a whole in the form of a matrix which has 8 rows and any number of columns, depending on the size of the entire plaintext.

DEVELOPMENT OF THE CIPHER

Consider a plaintext. Let us use ASCII code and represent it in the form of a matrix of size nxm. Thus we have

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

Let the key matrix K be given by

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

Following Hill[2], the process of encryption is described by using the relation

$$C = KP \bmod 128 \quad (3)$$

The process of decryption is governed by the relation

$$P = K^{-1}C \bmod 128, \quad (4)$$

where k^{-1} is the modular arithmetic inverse of K.

In the present analysis, we include interlacing (decomposition) in the process of encryption (decryption) and use iteration in both encryption and decryption. Here, it is to be noted that decomposition is a reverse process to that of interlacing.

Let us now illustrate the process of interlacing. For simplicity, consider a plaintext matrix of size 8×8 given by

$$P = [p_{ij}], i = 1 \text{ to } 8, j = 1 \text{ to } 8 \quad (5)$$

Writing each number of (2.5) in its binary form, we get $[P_{ij}] =$]
Where, i = 1 to 8, l = 1 to 7, j = 1 to 8.

Typically we can write the first column of the matrix$[p_{ij}]$ as follows:

$$\begin{pmatrix} b^1_{12} & b^1_{13} & b^1_{14} & b^1_{15} & b^1_{16} & b^1_{17} \\ b^1_{22} & b^1_{23} & b^1_{24} & b^1_{25} & b^1_{26} & b^1_{27} \\ b^1_{32} & b^1_{33} & b^1_{34} & b^1_{35} & b^1_{36} & b^1_{37} \\ b^1_{42} & b^1_{43} & b^1_{44} & b^1_{45} & b^1_{46} & b^1_{47} \\ b^1_{52} & b^1_{53} & b^1_{54} & b^1_{55} & b^1_{56} & b^1_{57} \\ b^1_{62} & b^1_{63} & b^1_{64} & b^1_{65} & b^1_{66} & b^1_{67} \\ b^1_{71} & b^1_{73} & b^1_{74} & b^1_{75} & b^1_{76} & b^1_{77} \\ b^1_{82} & b^1_{83} & b^1_{84} & b^1_{85} & b^1_{86} & b^1_{87} \end{pmatrix}$$

Similarly, we can have the second column with superscript 2 on all the elements (instead of 1). In the

Corresponding Author: V.U.K. Sastry, School of Computer Science and Informatics Dean, R&D Sreenidhi Institute of Science and Technology Hyderabad, India

same manner, we can write all the other columns.

Now, let us place the eight columns of $[P_{ij}]$ one after the other. Thus we get a matrix of size 8×56, containing the elements of $[b_{il}^{j}]$. Here, the process of interlacing can be described as follows. Let us focus our attention on the fifty six elements of the first row of the matrix formed above. This set of elements is divided into two equal halves. The first bit of the second half is placed after the first bit of the first half, the second bit of the second half is placed after the second bit of the first half and so on. After mixing in this manner, we place these elements in the form of a matrix which is given below.

$$\begin{pmatrix}
b_{11}^{5} & b_{12}^{1} & b_{12}^{5} & b_{13}^{1} & b_{13}^{5} & b_{14}^{1} \\
b_{15}^{1} & b_{15}^{5} & b_{16}^{1} & b_{16}^{5} & b_{17}^{1} & b_{17}^{5} \\
b_{11}^{6} & b_{12}^{2} & b_{12}^{6} & b_{13}^{2} & b_{13}^{6} & b_{14}^{2} \\
b_{15}^{2} & b_{15}^{6} & b_{16}^{2} & b_{16}^{6} & b_{17}^{2} & b_{17}^{6} \\
b_{11}^{7} & b_{12}^{3} & b_{12}^{7} & b_{13}^{3} & b_{13}^{7} & b_{14}^{3} \\
b_{15}^{3} & b_{15}^{7} & b_{16}^{3} & b_{16}^{7} & b_{17}^{3} & b_{17}^{7} \\
b_{11}^{8} & b_{12}^{4} & b_{12}^{8} & b_{13}^{4} & b_{13}^{8} & b_{14}^{4} \\
b_{15}^{4} & b_{15}^{8} & b_{16}^{4} & b_{16}^{8} & b_{17}^{4} & b_{17}^{8}
\end{pmatrix}$$

Similarly we get seven more matrices by using the rows two to eight of the matrix of the size 8×56 mentioned above.

Thus we get all the eight matrices having binary bits in each row. Basing upon these binary bits, we find the corresponding decimal numbers and hence obtain an 8×8 matrix, which is including the elements of all the columns. This can be considered as the new plaintext matrix (obtained after interlacing).

In a similar manner, it is possible to interlace the plaintext matrix, even when we are having more number of columns.

The procedures interlacing and decomposition are used in encryption and decryption respectively. The development of the cipher is shown in the schematic diagram given in Fig. 1

The algorithms required for encryption and decryption are designed as follows:

Algorithm for encryption

{

1. Read n,N,K,P;
2. $P^0 = P$;
3. for i = 1 to N
   {
   $P^i = KP^{i-1} \bmod 128$;
   Interlace(P^i);
   }
4. $C = KP^N \bmod 128$;
5. Write C;

}

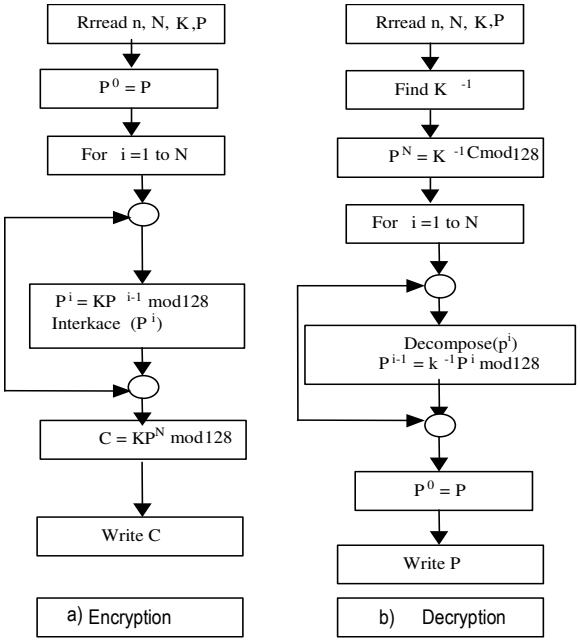

Fig. 1: Schematic diagram of the cipher. In this, N denotes the number of iterations, in this analysis, we have taken N = 16

Algorithm for decryption

{

1. Read n,N,K,C;
2. find modinverse(K);
3. $P^N = k^{-1}C \bmod 128$;
4. for i = N to 1
   {
   decompose(P^i);
   $P^{i-1} = k^{-1}P^i \bmod 128$;
   }
5. $P = P^0$;
6. Write P;

}

Algorithm for modinverse

{

1. read K,n;
2. find K_{ji}, Δ; // K_{ij} are the cofactors of the elements of K and Δ is the determinant of K.
3. find d such that (dΔ) mod 128 = 1; // d is the multiplicative inverse of Δ.
4. $K^{-1} = (K_{ji} * d) \bmod 128$;

}

Algorithm for interlace

```
{
    1.  l = 1;
    2.  convert P into binary bits;
    3.  for i = 1 to n
        {
            for j = 1 to 28
            {
                    temp(l) = b_ij;
                    temp(l+1) = d_ij;
                    l = l+2;
            }
        }
    5.      l = 1;
    6.      for i = 1 to n {
                    for j = 1 to 28 {
                            b_ij = temp(l);
                            d_ij = temp(l+n*7);
                            l = l+1 ;
                    }
            }
}
```

Algorithm for decomposition

```
{
   1.  l = 1;
   2.  convert P into binary bits;
   3.  for i = 1 to n
       {
            for j = 1 to 28
            {
                    temp(l) = b_ij;
                    temp(l+n*7) = d_ij;
                    l = l + 1 ;
            }
       }
   4.      l = 1;
   5.      for i = 1 to n {
                    for j = 1 to 28 {
                          b_ij = temp(l);
                          d_ij = temp(l+1);
                          l = l + 2 ;
                    }
            }
   6.      convert binary bits to decimal numbers;
}
```

RESULTS AND DISCUSSION

Consider the plaintext given below.

The policy of the other country is not clear. Let us watch for a few months and take a decision in respect of the external affairs and warfare. (6) Let us focus our attention on the first sixty four characters given by:

The policy of the other country is not clear. Let us watch for a (7)

On writing the ASCII codes for characters in a columnwise manner, the above plaintext can be written in the form of a matrix given by

$$\begin{pmatrix} 84 & 99 & 101 & 99 & 105 & 108 & 116 & 99 \\ 104 & 121 & 32 & 111 & 115 & 101 & 32 & 104 \\ 101 & 32 & 111 & 117 & 32 & 97 & 117 & 32 \\ 32 & 111 & 116 & 110 & 110 & 115 & 115 & 102 \\ 112 & 102 & 104 & 116 & 111 & 46 & 32 & 111 \\ 111 & 32 & 101 & 114 & 116 & 32 & 119 & 114 \\ 108 & 116 & 114 & 121 & 32 & 76 & 97 & 32 \\ 105 & 104 & 32 & 32 & 99 & 101 & 116 & 97 \end{pmatrix} \quad (6)$$

Here we take

$$K = \begin{pmatrix} 53 & 62 & 24 & 33 & 49 & 18 & 17 & 43 \\ 45 & 12 & 63 & 29 & 60 & 35 & 58 & 11 \\ 8 & 41 & 46 & 30 & 48 & 32 & 5 & 51 \\ 47 & 9 & 38 & 42 & 2 & 59 & 27 & 61 \\ 57 & 20 & 6 & 31 & 16 & 26 & 22 & 25 \\ 56 & 37 & 13 & 52 & 3 & 54 & 15 & 21 \\ 36 & 40 & 44 & 10 & 19 & 39 & 55 & 4 \\ 14 & 1 & 23 & 50 & 34 & 0 & 7 & 28 \end{pmatrix} \quad (7)$$

On using the algorithm 1, we get

$$P^1 = \begin{pmatrix} 57 & 14 & 121 & 40 & 109 & 45 & 122 & 3 \\ 7 & 14 & 25 & 108 & 16 & 56 & 113 & 58 \\ 21 & 87 & 12 & 6 & 0 & 18 & 33 & 119 \\ 48 & 20 & 106 & 15 & 47 & 76 & 52 & 114 \\ 97 & 112 & 81 & 33 & 18 & 9 & 63 & 2 \\ 52 & 23 & 63 & 27 & 83 & 85 & 122 & 54 \\ 61 & 40 & 105 & 37 & 93 & 74 & 18 & 39 \\ 35 & 9 & 53 & 15 & 127 & 4 & 8 & 88 \end{pmatrix} \quad (8)$$

On performing the interlacing mentioned in section 2, the new P^1 can be obtained in the form

$$P^1 = \begin{pmatrix} 61 & 83 & 9 & 121 & 82 & 6 & 84 & 65 \\ 127 & 70 & 17 & 5 & 78 & 87 & 16 & 6 \\ 2 & 42 & 11 & 104 & 54 & 37 & 38 & 59 \\ 42 & 3 & 91 & 100 & 63 & 110 & 15 & 30 \\ 4 & 35 & 70 & 46 & 55 & 115 & 49 & 68 \\ 9 & 33 & 42 & 61 & 83 & 6 & 24 & 55 \\ 28 & 85 & 36 & 112 & 58 & 95 & 1 & 18 \\ 91 & 24 & 43 & 46 & 20 & 98 & 65 & 106 \end{pmatrix} \quad (9)$$

After carrying out all the sixteen rounds (N = 16), we get

$$\begin{pmatrix} 115 & 35 & 112 & 78 & 96 & 21 & 25 & 88 \\ 113 & 94 & 1 & 80 & 95 & 65 & 119 & 54 \\ 53 & 22 & 49 & 67 & 108 & 99 & 35 & 90 \\ 101 & 120 & 68 & 4 & 76 & 125 & 23 & 29 \\ 31 & 60 & 122 & 90 & 86 & 41 & 95 & 16 \\ 60 & 13 & 56 & 63 & 89 & 116 & 114 & 53 \\ 0 & 77 & 30 & 68 & 106 & 53 & 30 & 70 \\ 21 & 18 & 3 & 117 & 25 & 71 & 58 & 36 \end{pmatrix} \quad (10)$$

The modular arithmetic inverse of K, denoted by K^{-1}, can be obtained as

$$K^{-1} = \begin{pmatrix} 27 & 40 & 53 & 3 & 117 & 48 & 25 & 2 \\ 41 & 60 & 17 & 92 & 5 & 21 & 106 & 81 \\ 57 & 39 & 115 & 118 & 18 & 0 & 37 & 116 \\ 94 & 97 & 52 & 27 & 94 & 102 & 104 & 19 \\ 63 & 123 & 117 & 0 & 98 & 9 & 97 & 32 \\ 61 & 50 & 54 & 60 & 101 & 12 & 69 & 56 \\ 64 & 41 & 57 & 22 & 73 & 75 & 49 & 122 \\ 71 & 61 & 17 & 32 & 42 & 88 & 81 & 113 \end{pmatrix} \quad (11)$$

Here we are to note that we are able to obtain the K^{-1} as the matrix of K is nonsingular and the determinant of K is relatively prime to 128. Further, it can be readily established that

$KK^{-1} \bmod 128 = K^{-1}K \bmod 128 = I$.

On taking the C given in (10) and using the algorithm (2), we get

$$P^N = \begin{pmatrix} 6 & 92 & 31 & 37 & 66 & 13 & 108 & 15 \\ 100 & 10 & 54 & 59 & 104 & 82 & 119 & 47 \\ 22 & 102 & 105 & 110 & 3 & 69 & 116 & 6 \\ 79 & 108 & 38 & 113 & 40 & 53 & 26 & 55 \\ 107 & 47 & 90 & 80 & 120 & 96 & 81 & 63 \\ 118 & 112 & 40 & 42 & 42 & 79 & 18 & 86 \\ 65 & 64 & 72 & 120 & 24 & 26 & 115 & 83 \\ 114 & 48 & 35 & 58 & 54 & 57 & 91 & 66 \end{pmatrix} \quad (12)$$

On performing decomposition, as we have mentioned in section 2, we get the new P^N in the form

$$P^N = \begin{pmatrix} 18 & 60 & 83 & 55 & 30 & 51 & 64 & 85 \\ 53 & 79 & 94 & 20 & 26 & 106 & 58 & 93 \\ 79 & 96 & 116 & 7 & 115 & 60 & 92 & 96 \\ 72 & 70 & 100 & 15 & 8 & 44 & 84 & 84 \\ 66 & 83 & 65 & 127 & 19 & 99 & 108 & 83 \\ 8 & 113 & 4 & 37 & 27 & 66 & 103 & 55 \\ 100 & 111 & 3 & 33 & 104 & 7 & 123 & 30 \\ 35 & 105 & 54 & 105 & 36 & 93 & 85 & 56 \end{pmatrix} \quad (13)$$

This process can be continued in the case of all the sixteen rounds (N = 16). Thus we get

$$P = \begin{pmatrix} 84 & 99 & 101 & 99 & 105 & 108 & 116 & 99 \\ 104 & 121 & 32 & 111 & 115 & 101 & 32 & 104 \\ 101 & 32 & 111 & 117 & 32 & 97 & 117 & 32 \\ 32 & 111 & 116 & 110 & 110 & 114 & 115 & 102 \\ 112 & 102 & 104 & 116 & 111 & 46 & 32 & 111 \\ 111 & 32 & 101 & 114 & 116 & 32 & 119 & 114 \\ 108 & 116 & 114 & 121 & 32 & 76 & 97 & 32 \\ 105 & 104 & 32 & 32 & 99 & 101 & 116 & 97 \end{pmatrix} \quad (14)$$

This is the same as the plaintext given in (8).

Let us now consider another example wherein we have taken the complete plaintext, given by (6). This plaintext is containing 143 characters. To represent this in the form of a matrix consisting of n rows and m columns, where n = 8 and m is having an appropriate value, we add one more character ($ is added here) to the plaintext. With this padding, the plaintext can be represented in terms of ASCII codes as follows:

$$P = \begin{pmatrix} 84 & 99 & 101 & 99 & 105 & 108 & 116 & 99 & 32 & 116 & 116 & 101 & 105 & 99 & 101 & 97 & 114 & 97 \\ 104 & 121 & 32 & 111 & 115 & 101 & 32 & 104 & 102 & 104 & 97 & 99 & 110 & 116 & 32 & 108 & 115 & 114 \\ 101 & 32 & 111 & 117 & 32 & 97 & 117 & 32 & 101 & 115 & 107 & 105 & 32 & 32 & 101 & 32 & 32 & 102 \\ 32 & 111 & 116 & 110 & 110 & 114 & 115 & 102 & 119 & 32 & 101 & 115 & 114 & 111 & 120 & 97 & 97 & 97 \\ 112 & 102 & 104 & 115 & 111 & 46 & 32 & 111 & 32 & 97 & 32 & 105 & 101 & 102 & 116 & 102 & 110 & 114 \\ 111 & 32 & 101 & 114 & 116 & 32 & 119 & 114 & 109 & 110 & 97 & 111 & 115 & 32 & 101 & 102 & 100 & 101 \\ 108 & 116 & 114 & 121 & 32 & 76 & 97 & 32 & 111 & 100 & 32 & 110 & 112 & 116 & 114 & 97 & 32 & 46 \\ 105 & 104 & 32 & 32 & 99 & 101 & 116 & 97 & 110 & 32 & 100 & 32 & 101 & 104 & 110 & 105 & 119 & 36 \end{pmatrix} \quad (15)$$

Here, we perform the interlacing as we have mentioned earlier 2. Then, on adopting the process of encryption, we get the ciphertext, in hexadecimal notation, as shown below.

```
80F0B933CC7C103760098E3C5EF00DE82DDD0A2ED1B25585B90D1A69408A060354946C6BE1B272F6D26
B465F562781E777F64BE2992826209AC926BC532DF9D39A4A6A894D1E499E70D69EE1A3420D482AE9BC   (16)
4DE28B5E319C4FF13505748923A398151FC2EB302719763000F93599292EC8F49F7E46579BD344CDDBAC3
```

On using the process of decryption, we readily find that this ciphertext can be brought into the form of the original plaintext.

In what follows, we examine the strength of the cipher by considering cryptanalysis and avalanche effect.

Cryptanalysis: In this analysis, the key matrix is of size nxn and each element in this matrix is lying between zero and sixty three. Thus, the size of the key space is 2^{6n^2}. In view of this fact, this cipher cannot be broken by the ciphertext only attack when n is greater than or equal to four.

In the case of the known plaintext attack, we know as many pairs of P and C as we require. P is a matrix of size nxm where $m \geq n$ and the C is also of the same size. Here as we have introduced interlacing and iteration, we do not have any direct simple relationship between P and C, as we have in the case of the Hill cipher. Thus, this ciphertext cannot be broken by the known plaintext attack.

Here, it is to be noticed that, any special choice of P or C will also not help any attacker in breaking the cipher.

Avalanche effect: Consider the plaintext given by (7). On applying the algorithm 1, the corresponding ciphertext can be obtained as:

```
11100110100011111000010011101110001101111000000011010000011010100101100110001100001111001
01111100010001000000100001111101111001111010101101001111000001101011100001111100000001001
10100111101000100001010100100100000011111010111000000010101001100110110001011111100000111   (17)
10111011011011011001100011010001110110101001100111110100101110011101101011001010011011111 0
01000010110011111010011100100110101110101001101010011110100011000110011000111011101001001 00
```

On replacing the first character ‘T’ of the plaintext under consideration by ‘U’, it assumes the form Uhe policy of the other country is not clear. Let us watch for a. (18)

Here it is to be noted that the T and U represented in terms of binary bits (from their ASCII codes) differ in one bit. On applying the encryption algorithm, the ciphertext corresponding to (18) can be written as:

```
11111010100111001111010001010111001101010001011100111101001000011000101110001011110010101 01
00100010000110100000111110001100010100001100001111001110001100111011011011001001010111010 01
10000010101010110111011010110000010010011100010110001011011010010101010101001010101001011 01   (18)
10001010111011001010100000101001000011111100000001001110111000011011000001101001001110110 11
00010011110001010000100011111110000011101001110110110101010011011111101100010100000101
```

Here we readily notice that (17) and (18) consisting of 448 bits, differ by 242 bits. This is quite significant.

Let us now change the key matrix element K_{33} from 46 to 47. These two also differ in one bit. Now we use the modified key and the original plaintext and apply the encryption algorithm. Thus, we get the ciphertext in the form

```
01101100101111010101000101001110100001011100111100001101110100101011001101000011
00100000000010000101011000000010000110000010101100101111100010101000101111000001
01010000001011011010101101010011011010011000110010101100011111100000111101010101
00000101000011100101010110101000000111001001111000000010010101010101011001100000   (19)
01110000011001110101001110100011010011111011011100100101101001100011000100010000
11110110010100100000000110101100100101101100100 1
```

On comparing (17) and (19), having 448 bits, we find that the ciphertexts differ by 235 bits. This departure is also considerable.

From the above analysis, we conclude that the avalanche effect is highly pronounced.

CONCLUSIONS

In this research, we have developed a block cipher by modifying the Hill cipher. In this, the key is represented in the form of a matrix of size nxn and the plaintext is represented in the form of a matrix of size nxm, where m≥n. Thus we are able to accommodate a large number of characters of the plaintext into the plaintext matrix.

In this analysis, we have adopted an iterative process. In each round of the iteration, we have performed multiplication of the plaintext matrix with the key matrix and modulo operation with 128. In every round, the modified plaintext is represented in terms of binary bits and these binary bits are interlaced so that we get a plaintext matrix of the same size. This sort of interlacing of the binary bits of the plaintext is expected to cause a lot of confusion in the structure of the plaintext.

In this research, we have taken the size of the key matrix as 384 bits. The size of the plaintext block is 448 bits in the first example and 1008 bits in the second example.

The cryptanalysis and avalanche effect discussed in this research, clearly indicate that the cipher is a strong one and it cannot be broken by any cryptanalytic attack.

In the light of the above analysis, we find that the cipher under consideration can be applied to a plaintext of any size (with padding, if needed) and the strength of the cipher is quite significant as interlacing is causing a lot of transposition in the elements of the plaintext.

REFERENCES

1. Sastry, V.U.K. and N. Ravi Shankar, Modified Hill Cipher with Interlacing and Iteration, communicated for publication.
2. William Stallings. Cryptography and Network Security: Principles and Practices, Third edition, Chapter 2, pp: 37.