Journal of Computer Science 3 (11): 854-859, 2007
ISSN 1549-3636

Modified Hill Cipher with Interlacing and Iteration

[1]V.U.K. Sastry and [2]N. Ravi Shankar
[1]Department of R and D
[2]Department of CSE, Sreenidhi Institute of Science and Technology,
Hyderabad, India

Abstract: In this research, we have developed a block cipher by taking a large key matrix of size nxn and a plaintext matrix containing n rows and two columns. In this, the plaintext column vectors, operated by the key matrix are thoroughly interlaced at each stage of the iteration. As a typical example, we have taken the key in the form an 8×8 matrix and the plaintext in the form of an 8×2 matrix. Here the key is of the size 384 binary bits and the plaintext is of size 112 binary bits. The cryptanalysis carried out in this research clearly indicates that the cipher cannot be broken by any cryptanalytic attack.

Keywords: Modular arithmetic inverse, interlacing, decomposition

INTRODUCTION

The classical Hill cipher[1] is a typical block cipher which depends mainly on the modular arithmetic inverse of a key matrix. In this, the encryption and the decryption are governed by the relations

$$C = KP \bmod 26 \quad (1)$$

and

$$P = K^{-1} C \bmod 26 \quad (2)$$

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

It is well known that, though this cipher is very strong against brute force attack, it can be broken by the known plaintext attack, as we have direct relations, given by (1) and (2), for the cipher.

In a pioneering research, Sastry and Janaki[2] have obtained the modular arithmetic inverse of a matrix in a systematic manner and have pointed out that the Hill cipher cannot broken by the known plaintext attack, when the elements of the plaintext are transposed in an effective manner.

In the present research, our objective is to modify the Hill cipher by introducing a key matrix, which is significantly large in size (as the strength of a cipher increases with the length of the key) and by considering a plaintext vector which undergoes transposition, repeatedly, on account of interlacing. Here our interest is to modify the Hill cipher such that it cannot be broken by any cryptanalytic attack.

DEVELOPMENT OF THE CIPHER

Consider a plaintext consisting of 2n characters. By using the ASCII code, the corresponding plaintext matrix can be written in the form $P = [P_{ij}]$ where i = 1 to n, j = 1 to 2.

Let $K = [K_{ij}]$, i = 1 to n and j = 1 to n, be the key matrix. Let us suppose that $C = [C_{ij}]$, i = 1 to n and j = 1 to 2, be the corresponding ciphertext. Then, C can be obtained by using the relation

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

After obtaining the modular arithmetic inverse of K, denoted by K^{-1}, from (3), we get

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

The Eq. 3 and 4 describe the process of encryption and the process of decryption.

We now introduce the concept of interlacing. Let us represent the decimal numbers in the two columns of P in terms of their binary bits. As each number lies between zero and 127, we get only seven binary bits corresponding to each number. Thus we have

$$\left.\begin{aligned}[P_{i1}]^T &= [b_{ij}],\\ [P_{i2}]^T &= [d_{ij}],\end{aligned}\right\} i=1 \text{ to } n,\ j=1 \text{ to } 7 \quad (5)$$

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

where, T is the transpose of the vector.

Here, b_{ij} are the binary bits corresponding to the numbers in the first column and d_{ij} are those of the second column. In order to illustrate the process of interlacing, let us consider a simple case where n = 8. Here we have

$$\left.\begin{aligned}[P_{i1}]^T &= [b_{ij}],\\ [P_{i2}]^T &= [d_{ij}],\end{aligned}\right\} i=1 \text{ to } 8,\ j=1 \text{ to } 7 \qquad (6)$$

Now, let us mix b_{ij} and d_{ij}, i = 1 to 8, j = 1 to 7, the binary bits of the first and second columns of the plaintext and write them in terms of a pair of matrices as shown below.

$$\begin{pmatrix} b_{11} & d_{11} & b_{12} & d_{12} & b_{13} & d_{13} & b_{14}\\ d_{14} & b_{15} & d_{15} & b_{16} & d_{16} & b_{17} & d_{17}\\ b_{21} & d_{21} & b_{22} & d_{22} & b_{23} & d_{23} & b_{24}\\ d_{24} & b_{25} & d_{25} & b_{26} & d_{26} & b_{27} & d_{27}\\ b_{31} & d_{31} & b_{32} & d_{32} & b_{33} & d_{33} & b_{34}\\ d_{34} & b_{35} & d_{35} & b_{36} & d_{36} & b_{37} & d_{37}\\ b_{41} & d_{41} & b_{42} & d_{42} & b_{43} & d_{43} & b_{44}\\ d_{44} & b_{45} & d_{45} & b_{46} & d_{46} & b_{47} & d_{47} \end{pmatrix} \qquad (7)$$

$$\begin{pmatrix} b_{51} & d_{51} & b_{52} & d_{52} & b_{53} & d_{53} & b_{54}\\ d_{54} & b_{55} & d_{55} & b_{56} & d_{56} & b_{57} & d_{57}\\ b_{61} & d_{61} & b_{62} & d_{62} & b_{63} & d_{63} & b_{64}\\ d_{64} & b_{65} & d_{65} & b_{66} & d_{66} & b_{67} & d_{67}\\ b_{71} & d_{71} & b_{72} & d_{72} & b_{73} & d_{73} & b_{74}\\ d_{34} & b_{35} & d_{75} & b_{76} & d_{76} & b_{77} & d_{77}\\ b_{81} & d_{81} & b_{82} & d_{82} & b_{83} & d_{83} & b_{84}\\ d_{84} & b_{85} & d_{85} & b_{86} & d_{86} & b_{87} & d_{87} \end{pmatrix} \qquad (8)$$

In these matrices, each b_{ij} lies adjacent to its corresponding d_{ij}.

Now we obtain the decimal numbers corresponding to the binary bits of each row, in the above two matrices and reconstruct the modified plaintext matrix $[P_{ij}]$, i = 1 to 8 and j = 1 to 2. Similarly we can obtain $[P_{ij}]$, for i = 1 to n, j = 1 to 2, in general.In the process of decryption, we carryout the reverse process of the above interlacing, which is hereafter called as decomposition.

The cipher involving interlacing and iteration is shown in the schematic diagram given in Fig.1

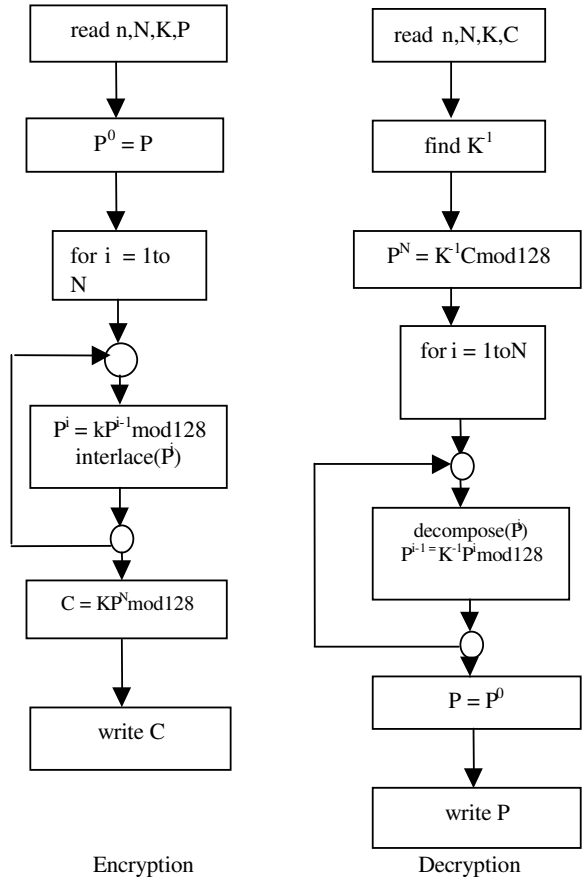

Fig. 1: Schematic diagram of the cipher. In this, N denotes the number of iterations and analysis, we have taken N = 16

DESIGN OF ALGORITHMS

Algorithm for Encryption

{

1. Read n,N,K,P;
2. $P^0 = P$;
3. for i = 1 to N

{

4. $P^i = KP^{i-1} \bmod 128$;
5. Interlace(P^i);

}

$C = KP^N \bmod 128$;

Write C;

}

Algorithm for decryption

{

1. Read n,N,K,C;

```
    2.  find modinverse(K);
    3.  P = k C mod 128;
    4.  for i = N to 1
{   decompose(P );
    5.  P = k P mod 128;
}
    1.  P = P ;
    2.  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) mod 128;
}
```

Algorithm for interlace

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

ILLUSTRATION OF THE CIPHER

Consider the following plaintext: The World Bank has given an assistance of 100 billion dollars for the community development in our country. Let us have progress in all directions.

Let us focus our attention on the first sixteen characters of the above plaintext. This is given by
The World Bank h.

By using the ASCII code, the matrix corresponding to the above plaintext can be constructed, in a row wise manner, as

$$\begin{pmatrix} 84 & 100 \\ 104 & 32 \\ 101 & 66 \\ 32 & 97 \\ 87 & 110 \\ 111 & 107 \\ 114 & 32 \\ 108 & 104 \end{pmatrix} \quad (9)$$

Here, as we have sixteen numbers, the size of the plaintext block is 112 binary bits.

Let us consider a key matrix given by

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

Here, each element in the key matrix is less than 64. In view of this fact, as each number can be represented in terms of 6 binary bits, the size of the key matrix is 6x64 i.e., 384 binary bits.

On using the algorithm for encryption we get

$$p^1=\begin{pmatrix}87 & 81\\ 40 & 112\\ 28 & 82\\ 87 & 95\\ 32 & 53\\ 2 & 82\\ 56 & 41\\ 79 & 84\end{pmatrix} \quad (11)$$

Now, we illustrate the process of interlacing (see section 2). From (6), we get

$$[b_{ij}]=\begin{pmatrix}1&0&1&0&1&1&1\\ 0&1&0&1&0&0&0\\ 0&0&1&1&1&0&0\\ 1&0&1&0&1&1&1\\ 0&1&0&0&0&0&0\\ 0&0&0&0&0&1&0\\ 0&1&1&1&0&0&0\\ 1&0&0&1&1&1&1\end{pmatrix} \quad (12)$$

$$[d_{ij}]=\begin{pmatrix}1&0&1&0&0&0&1\\ 1&1&1&0&0&0&0\\ 1&0&1&0&0&1&0\\ 1&0&1&1&1&1&1\\ 0&1&1&0&1&0&1\\ 1&0&1&0&0&1&0\\ 0&1&0&1&0&0&1\\ 1&0&1&0&1&0&0\end{pmatrix} \quad (13)$$

Now, we carryout interlacing, as explained in section 2 and obtain the new $[b_{ij}]$ and $[d_{ij}]$ as follows:

$$[b_{ij}]=\begin{pmatrix}1&1&0&0&1&1&0\\ 0&1&0&1&0&1&1\\ 0&1&1&1&0&1&1\\ 0&0&0&0&0&0&0\\ 0&1&0&0&1&1&1\\ 0&1&0&0&1&0&0\\ 1&1&0&0&1&1&0\\ 1&1&1&1&1&1&1\end{pmatrix} \quad (14)$$

$$[d_{ij}]=\begin{pmatrix}0&0&1&1&0&1&0\\ 0&0&1&0&0&0&1\\ 0&1&0&0&0&1&0\\ 0&0&0&1&1&0&0\\ 0&0&1&1&1&0&1\\ 1&0&0&0&0&0&1\\ 1&1&0&0&0&1&1\\ 0&1&1&1&0&1&0\end{pmatrix} \quad (15)$$

Thus, we have the transformed plaintext, after the first iteration, in the form

$$P^1=\begin{pmatrix}102 & 26\\ 43 & 17\\ 59 & 34\\ 0 & 12\\ 39 & 29\\ 36 & 65\\ 102 & 99\\ 127 & 58\end{pmatrix} \quad (16)$$

After carrying out all the sixteen rounds (N = 16), involved in the process of encryption, we get

$$C=\begin{pmatrix}113 & 59\\ 115 & 121\\ 106 & 44\\ 5 & 70\\ 89 & 32\\ 53 & 108\\ 96 & 48\\ 92 & 87\end{pmatrix} \quad (17)$$

The modular arithmetic inverse of K, given by (4.4), is obtained as

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

Here we readily notice that,

$KK^{-1} \bmod 128 = K^{-1}K \bmod 128 = I$. On using (17) and (18) and applying the process of decryption, given in algorithm decryption, we get

$$P^N = \begin{pmatrix} 27 & 77 \\ 85 & 70 \\ 86 & 98 \\ 64 & 18 \\ 81 & 96 \\ 4 & 9 \\ 83 & 91 \\ 54 & 85 \end{pmatrix} \quad (19)$$

On converting the numbers in the above matrix into their equivalent binary bits, we get $[b_{ij}]$ and $[d_{ij}]$ from the first and second columns as follows:

$$[b_{ij}] = \begin{pmatrix} 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 \end{pmatrix} \quad (20)$$

$$[d_{ij}] = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} \quad (21)$$

On adopting the process of decomposition, given in algorithm 3.5, in the first iteration, we get

$$[b_{ij}] = \begin{pmatrix} 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 \end{pmatrix} \quad (22)$$

and

$$[d_{ij}] = \begin{pmatrix} 0 & 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix} \quad (23)$$

Hence we have the new P^N as

$$P^N = \begin{pmatrix} 25 & 77 \\ 85 & 70 \\ 86 & 98 \\ 64 & 18 \\ 81 & 96 \\ 4 & 9 \\ 83 & 91 \\ 54 & 85 \end{pmatrix} \quad (24)$$

After carrying out all the sixteen rounds, involved in the process of decryption, in a similar manner, we get

$$P = \begin{pmatrix} 84 & 100 \\ 104 & 32 \\ 101 & 66 \\ 32 & 97 \\ 87 & 110 \\ 111 & 107 \\ 114 & 32 \\ 108 & 104 \end{pmatrix} \quad (25)$$

This is the same as (9)

The above steps clearly indicate the encryption and the decryption processes underlying in the cipher.

CRYPTANALYSIS

In the case of the classical Hill cipher, it is well known that the cipher can be broken by applying the known plaintext attack. In the present cipher, we have introduced interlacing and iteration. On account of these two concepts, the binary bits arising due to the interaction between the key and the plaintext, are undergoing a thorough diffusion and confusion. Thus the cipher is expected to be a very strong one.

In what follows, let us discuss the ciphertext only attack, the known plaintext attack and the chosen plaintext/ciphertext attacks.

In the case of the ciphertext only attack, the ciphertext is known to us. In this, the key matrix is of size nxn. As each element of the matrix can be represented in terms of binary bits, the size of the key space is, in general, 2^{7n^2}. However, in the present analysis, each element of the key matrix is taken to be

less than 64. Thus it can be represented in six binary bits. Therefore the key space is of size 2^{6n^2}. From these facts, when n is greater than or equal to four, we readily conclude that the cipher cannot be broken by 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. Though we know as many Ps and the corresponding Cs as we want, we do not have a direct relation between them as the P is under going transposition at every stage of the iteration. Thus we cannot construct an equation of the form X = KY mod 128.
(as we could do in the case of the Hill cipher[1]) and determine K by obtaining the modular arithmetic inverse of Y. Hence, the cipher cannot be broken by the known plaintext attack.

Further, we notice that any special choice of the plaintext vector or the ciphertext vector will not help the attacker as the plaintext interacting with the key, is interlaced at every stage of the encryption process.

From the above discussion, we find that the strength of the cipher is enhanced enormously by the interlacing and the iteration introduced into the cipher.

Avalanche effect: The plaintext given by (4.2) can be written in terms of binary bits as

```
10101001101000110010101000001010111111
01111111001011011001100100010000001000      (26)
01011000011101110110101101000001101000
```

On changing the first character of the plaintext from T to U, we get

```
10101011101000110010101000001010111111
01111111001011011001100100010000001000      (27)
01011000011101110110101101000001101000
```

The plaintexts given by (26) and (27) differ exactly by one bit.

The ciphertexts corresponding to (26) and (27) are

```
11100011110011110101000001011011001011
01011100000101110001110111111100101011      (28)
00100011001000001101100011000010101111

10000100000111011010001101101100001000
10011010010011000110011010110101011100      (29)
11001000000110110100101001001010101 1
```

From (28) and (29), we notice that, they differ by sixty five bits, which is a large departure.

Now, let us consider the key given by (10). If we change the key element K_{33} from 46 to 47, the key under consideration changes by one bit. The ciphertext obtained for the plaintext given by applying the original key is given in (28).

In the case of the modified key, the corresponding ciphertext obtained for the same plaintext is

```
10100100111111110011011010000101011111
00011101000011101100000100001001000001      (30)
10111100000010100001011001010001011001
```

We notice that (28) and (30) differ by 55 bits. This is also considerable.
From the above discussion, we find that the avalanche effect is quite significant.

RESULTS AND DISCUSSIONS

In this research, we have developed a block cipher by modifying the Hill cipher. Here, we have illustrated the cipher by taking an example, in which the key is in the form of an 8x8 matrix and the plaintext is in the form of an 82 matrix. After performing the usual operations of the Hill cipher, the resulting numbers, converted into their binary form, are interlaced. This process is repeated at each stage of the iteration. Effectively, this has led to a significant amount of confusion and diffusion and thus the strength of the cipher is enhanced.

In this analysis, the programs required for encryption and decryption are written in C language.

By using the cipher developed in this analysis, we have obtained the ciphertext corresponding to the entire plaintext. The ciphertext obtained in this analysis, in hexadecimal notation, is given by
E3CF505B2D705C77E564641B1857F1561F84361E22
57694AA25F98AD2E2BE45478E50403BE05C3E3522
F9CD6FCB30BD46DDE47A035026D28AB82B5C9B
7778E628441D8D51DB07B71BF8CAD6315BC194A
803400F3EDFB6C636613F6412CF7500C883B14DA3
FE14340C004A5AB7DB76BC1E8A987B212571F522
CB1422D74CA61AADD034B05279B1EBCF8D503A
9.

CONCLUSIONS

From the cryptanalysis and the avalanche effect discussed in this research, we find that the strength of the cipher is quite significant.

From the above analysis, we conclude that the interlacing and the iteration play a vital role in strengthening the cipher.

This analysis can be extended to the case wherein, the plaintext can be of any size.

REFERENCES

1. William Stallings, Cryptography and Network Security: Principles and Practices, Third edition, Chapter 2, pp: 37.
2. Sastry, V.U.K. and V. Janaki, 2005. On the Modular Arithmetic Inverse in the Cryptology of Hill Cipher, Proceedings of North American Technology and Business Conference, Montreal, Canada.