

A Large Block Cipher using an Iterative Method and the Modular Arithmetic Inverse of a key Matrix

S. Udaya Kumar

V. U. K. Sastry

A. Vinaya babu

Abstract

In this paper, we have developed a block cipher for blocks of size 196 bits and 392 bits. In this, we have represented the plaintext in the form of a matrix of size 28×7 , consisting of binary bits. The key matrix is represented in the form of a matrix of size 28×28 , and it comprises binary bits. In the process of decryption, we have used the modular arithmetic inverse (K^{-1}) of the key matrix K . From the cryptanalysis carried out in this paper, we conclude that the cipher cannot be broken by any cryptanalytic attack.

1. INTRODUCTION

In the classical literature of cryptography, Hill cipher [1] occupies a prominent place. In this, the characters A to Z are represented by the numbers 0 to 25, and the ciphertext is written in terms of the numbers. A secret key is taken in the form of a matrix, which contains numbers, wherein each number is less than 26. Here, we get the ciphertext by operating with the key matrix on the plaintext vector and performing mod 26. Following Hill, Feistel [2-3], made an attempt to develop a block cipher, wherein the plaintext and the key matrix are represented in terms of binary bits and mod 2 operation is carried out on the result obtained by multiplying the plaintext vector with the key matrix.

Manuscript was received on July 28, 2006.

S. Udaya Kumar is with SreeNidhi Institute of Science & Technology, Ghatkesar, Hyderabad - 501301, India. (Tel. ++91-9395533303, email: uksusarla@rediffmail.com)

V. U. K. Sastry is with SreeNidhi Institute of Science & Technology, Ghatkesar, Hyderabad -501301, India (Tel. ++91-9395533303, email: vksastry@rediffmail.com).

A. Vinaya babu is with JNT University, Hyderabad, India. (email: dravinayababu@yahoo.com)

However, he found that the cipher can be broken by the known plaintext attack.

In the present paper, our objective is to develop a block cipher wherein the size of the block is large. Here the block is represented in the form of a matrix of size 28×7 , and the key matrix is taken to be of size 28×28 . In this paper, we have adopted an iterative procedure and obtained the ciphertext. In this we have performed cryptanalysis and have shown that the cipher cannot be broken by any cryptanalytic attack. Finally, we have extended the analysis to a block of size 392 bits by applying a procedure called interlacing.

2. DEVELOPMENT OF THE CIPHER

Consider a block of plaintext. Let us represent this block in the form of a matrix P , where $P = [P_{ij}]$, $i = 1$ to n , $j = 1$ to 7. Let $K = [K_{ij}]$, $i = 1$ to n , $j = 1$ to n , be an $n \times n$ matrix in which all the K_{ij} are binary elements.

Let $C = [C_{ij}]$ be the corresponding ciphertext matrix whose size is $n \times 7$.

Here we develop an iterative scheme for encryption as well as for decryption. Before we proceed further, let us denote the plaintext matrix P by P^0 ($P \equiv P^0$). Then the iterative scheme for encryption can be written as

$$P^i = KP^{i-1} \text{ mod } 2, \text{ for } i=1 \text{ to } m, \quad (2.1)$$

where m is the number of iterations. From this, we get P^m , which can be denoted as C .

Thus we have

$$C = P^m. \quad (2.2)$$

In the process of decryption, we get

$$P^{i-1} = K^{-1}P^i \text{ mod } 2, \quad i = m \text{ to } 1, \quad (2.3)$$

where K^{-1} is the modular arithmetic inverse of K , which satisfies the relations

$$KK^{-1} \text{ mod } 2 = K^{-1}K \text{ mod } 2 = I.$$

Now we present algorithms for encryption, decryption and the modular arithmetic inverse of the key matrix K , denoted by K^{-1} .

3. ALGORITHMS

3.1 Algorithm for Encryption

```
{
1. Read n, m, K and P0
2. for i = 1 to m
   {
   Pi = KPi-1 mod 2
   }
3. C = Pm
}
```

3.2 Algorithm for Decryption

```
{
1. Read n, m, K and C
2. Find K-1 // K-1 is the
   modular arithmetic inverse of K with mod 2.
3. Pm = C
4. for i = m to 1
   {
   Pi-1 = K-1 Pi mod 2
   }
5. P = P0
}
```

3.3 Algorithm for K^{-1}

```
{
1. Let A = K. Find the determinant of A. Let it
be denoted by Δ.
```

2. Find the inverse of A. The inverse is given by

$$A^{-1} = \frac{1}{\Delta} [A_{ij}], \quad i = 1 \text{ to } n, j = 1 \text{ to } n, \text{ where}$$

A_{ij} are the cofactors of a_{ij} , which are elements of A, and Δ is the determinant of A.

3. for i = 1 to n,

```
{
   if ((iΔ) mod N = 1) d = i;
   break;
}
```

4. B = [dA_{ij}] mod N. // B is the modular arithmetic inverse of A.

```
}
```

Here it is to be noted that the modular arithmetic inverse [4] of a matrix A exists only when A is non-singular, and Δ is relatively prime to N. In the present analysis, we take $N = 2$, and obtain the modular arithmetic inverse of K such that $KK^{-1} \text{ mod } 2 = K^{-1}K \text{ mod } 2 = I$.

4. ILLUSTRATION OF THE CIPHER

Let us consider a key given by

$$K_0 = [65, 71, 95, 121, 50, 31, 99, 81, 122, 119, 23, 41, 37, 11, 114, 67, 87, 105, 117, 115, 127, 31, 118, 116, 124, 113, 98, 35]. \quad (4.1)$$

This consists of 28 numbers. We place the first two numbers in the first row, the next two numbers in the second row, and so on, and form a matrix of size 14 x 2. Then we represent each number in its binary form, and obtain a matrix of size 14 x 14 with binary elements. Thus we have

Consider the plaintext: Transfer one million dollars into my Swiss bank account. (4.5)

Let us focus our attention on the first 28 characters - Transfer one million dollars, which include twenty-five characters and three blank spaces. On using the ASCII Code, the plaintext under consideration can be written as a 28 x 7 matrix given by

Let us now form a 28 x 28 key matrix K in the form

$$K = \begin{bmatrix} Z & R & Y \\ Q & P & X \\ \vdots & \vdots & \vdots \end{bmatrix}, \quad (4.3)$$

where $Z = Q^T$, and R is obtained by interchanging the first and the last rows of Q, the second and the last but one rows of Q, and so on. The matrix Y is obtained by making the last column of Q as the first row of Y, the last but one column of Q as the second row of Y, and so on.

Thus we have

$$P = \begin{bmatrix} T & r & \dots \\ \vdots & \vdots & \vdots \end{bmatrix}. \quad (4.6)$$

In this matrix, the first row corresponds to the first character 'T' of the plaintext, the second row corresponds to the next character 'r', and so on.

On using the encryption algorithm mentioned in section 3.1, and performing sixteen iterations (taking $m = 16$), we obtain the corresponding ciphertext in the form

$$K = \begin{bmatrix} \dots \\ \dots \\ \dots \end{bmatrix}. \quad (4.4)$$

$$\begin{bmatrix} 0000010001001000110010111001101001011111101 \\ 0101010111101011100110010111010101001001010 \\ 0011100101001110101011011101111010000011110 \\ 0010111110000110011011111010010001001000001 \\ 010111100100100110001110. \end{bmatrix} \quad (4.7)$$

On applying the procedure for the modular arithmetic inverse mentioned in section 3, we obtain

$$2^{196} \approx 2^{200} = (2^{10})^{20} \approx 10^{60}.$$

Hence, the cipher cannot be broken by brute force attack. Now let us consider the known plaintext attack. Here we have as many plaintext and ciphertext pairs as we require.

From the equation (2.1), we have

$$P^1 = KP^0 \text{ mod } 2. \quad (5.1)$$

$$\begin{aligned} P^2 &= KP^1 \text{ mod } 2 \\ &= K^2 P^0 \text{ mod } 2 \end{aligned} \quad (5.2)$$

$$P^3 = K^3 P^0 \text{ mod } 2. \quad (5.3)$$

Similarly, we get

$$P^m = K^m P^0 \text{ mod } 2, \quad (5.4)$$

where m is the number of iterations.

From (2.2) and (5.4) we obtain

$$C = P^m = K^m P^0 \text{ mod } 2. \quad (5.5)$$

Here P^0 is a matrix of size 28×7 . Thus taking three more plaintexts of the same size, we obtain the corresponding ciphertexts. We now arrange all the four-plaintext matrices, one adjacent to the other, so that they form a matrix of size 28×28 . Similarly, we place the four corresponding ciphertext matrices in the form of a matrix of the same size. Then we get an equation of the form

$$Y = K^m X \text{ mod } 2, \quad (5.6)$$

where X and Y are matrices containing plaintexts and ciphertexts respectively. Then on assuming that the conditions for obtaining the modular arithmetic inverse of X are satisfied, from (5.6), we get

$$X^{-1}Y \text{ mod } 2 = K^m \text{ mod } 2. \quad (5.7)$$

This is a non-linear equation of degree m. Hence, the cipher cannot be broken in the case of the known plaintext attack also.

6. MODIFICATION OF THE CIPHER FOR A LARGER BLOCK (392 BITS)

So far we have considered a plaintext block of size 196 bits. Now we extend the cipher to a block of

$$K^{-1} = \dots (4.8)$$

The value of the determinant of K, denoted by Δ is equal to 45991, which is relatively prime to 2. From (4.4) and (4.8), we can readily find that

$$KK^{-1} \text{ mod } 2 = K^{-1}K \text{ mod } 2 = I.$$

On using the K^{-1} given in (4.8) and the ciphertext given in (4.7), and applying the decryption algorithm mentioned in section 3.2, the receiver can readily obtain the plaintext.

5. CRYPTANALYSIS

In the development of this cipher, we have taken a key K_0 containing 28 numbers. On using this key, we have generated a matrix Q, which is of size 14×14 . Then we have formed the key matrix K, wherein K contains Q and the other three matrices namely, R, Y and Z, which are all, formed basing upon Q. Thus Q plays a vital role in the development of the cipher. As Q is of size 14×14 , and it contains 0s and 1s, the size of the key space for the key under consideration is

size 392 bits. This can be achieved by mixing two plaintext blocks of size 196 bits each. The modifications in the process of the encryption and the process of the decryption are shown in Fig. 1 and Fig. 2 respectively.

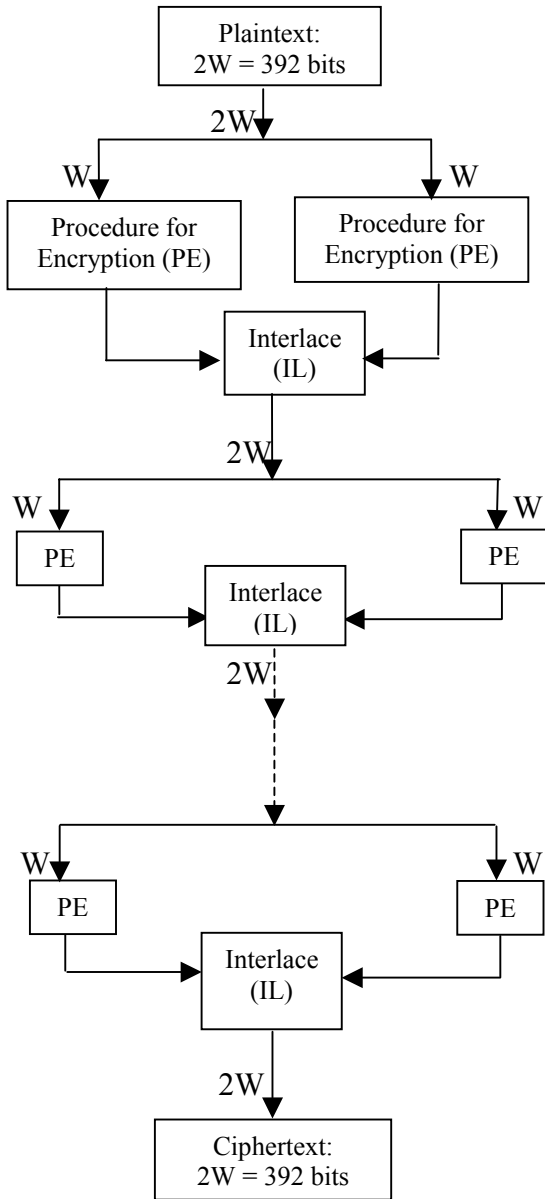


Fig. 1. Process of Encryption for 392 bits Plaintext

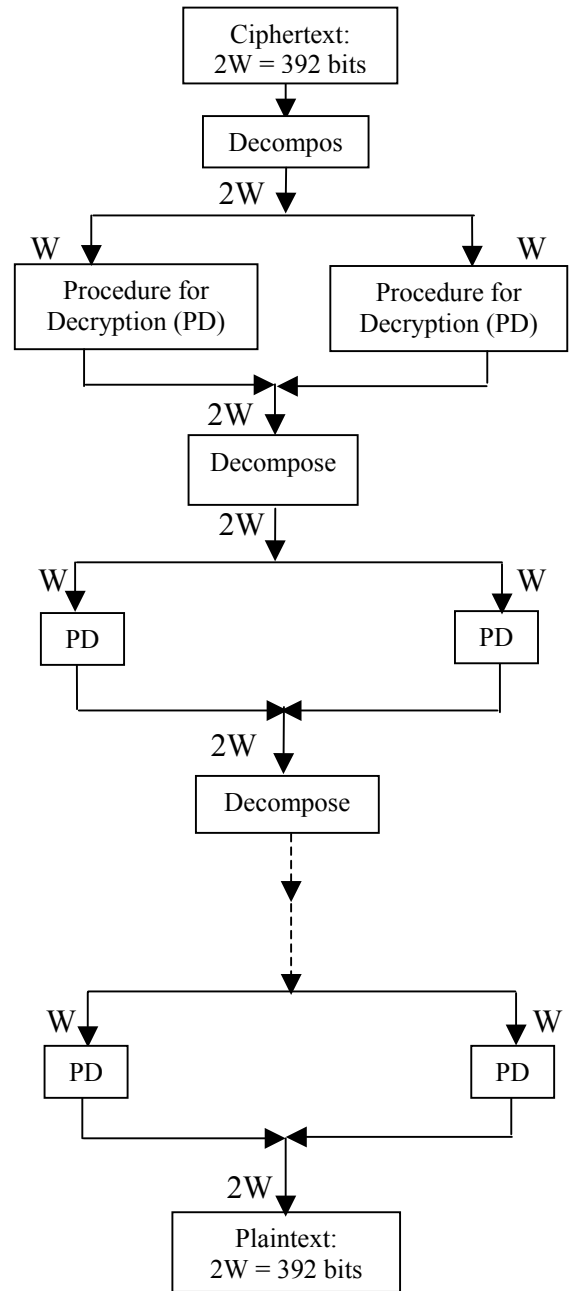


Fig. 2. Process of Decryption for 392 bits Ciphertext

In Fig. 1, the plaintext of length $2W = 392$ bits is divided into two halves of W each. Then the procedure for encryption (PE) described in section 4, is adopted on each W . Then the resulting W s are interlaced as per the following procedure. The two W s are arranged such that each W forms a matrix of

size 28 x 7. Let us now represent the matrices as A and B, respectively.

$$\text{Let } A = [a_{ij}], B = [b_{ij}], i = 1 \text{ to } 28, j = 1 \text{ to } 7.$$

Now we mix the elements of the matrices A and B, placing the elements of the first column of A as they are, and the elements of the last column of B in the reverse order.

In a similar manner, we mix the elements of the second column of A, and the elements of the last but one column of B. We continue this process till all the columns of A, and B are exhausted. In the process of mixing, we place the last element of the last column of B next to the first element of the first column of A, the last but one element of the last column of B as the next element to the second element of the first column of A, and so on. Thus the elements appear in the form

$$a_{11}, b_{287}, a_{21}, b_{277}, a_{31}, b_{267}, a_{41}, b_{257}, \dots$$

Here a_{11} is the first element in the first row and the first column of the matrix A, and b_{287} is the element in the twenty-eighth row and the seventh column of the matrix B. The same notation is followed for other elements also.

The same mixing procedure is applied for all the other pairs of columns.

In Fig. 2, Decompose is a function, which performs operations in the opposite manner to interlacing. Ultimately, this leads to two matrices, wherein each one is of size 28 x 7. Here PD is the procedure for decryption. It is the same that is adopted earlier in the case of 196 bits (see section 4).

Let us now consider the plaintext given in (4.5). On using the encryption procedure shown in Fig. 1, we obtain the following ciphertext:

```
010000010111010011001101101011110110001000
110101011110000001010111101110010010011001
1000101111011011011001000001110001010100001
```

```
1111010110001000110110011011000100101100000
0111110001010010011110110101010100110000100
1101111001101100110011010110110111011000001
110111100111110001110100111101110110001001
1110010111000111100000110110011001110001001
1010010000101100011001110000001010001001010
01001. (6.1)
```

On applying the decryption procedure shown in Fig.2, the receiver obtains the plaintext.

7. AVALANCHE EFFECT

Let us again focus our attention on the plaintext given in (4.5). We change the binary representation of the plaintext in one bit. This is achieved by replacing the character T, that is the first character in the plaintext by S. We now apply the encryption procedure described in section 6, and obtain the corresponding ciphertext given by

```
0100110101101001011001000000100001001110100
1000011101101101110011111010011000111011101
1010111111101110111101000010011111011000011
1101001101011001001010110010110011100101001
1101000011110010101101100010100010011000010
0100110011001010001100011000110100000101010
10110100110010001001111010001000111101111110
1000010010111101001010010010010110011000111
0001011100000100111001011100100101011100111
10010. (7.1)
```

On comparing (6.1) and (7.1), we notice that these two ciphertexts differ in two hundred (200) bits. This indicates the algorithm exhibits strong avalanche effect.

Let us now change the key K_0 , given in (4.1), by one bit. This is achieved by replacing the number 50 by 48 in (4.1). On using the resulting key and performing the process of the encryption (described

in section 6) on the plaintext given in (4.5), we get the ciphertext

```
0111100011000011111110100101000111001100101
1100010010010000001000111000100100111011101
110100010111011000101110110000001111010011
1010001101011101100100110001101110100111010
0001101101010101000001100000111010011001111
100010111110110010100101001011111000001010
1100011000001010100110001001110001111011001
1101100001100011000000111000010101001101111
0101010110101001110001000111101010011110000
11011. (7.2)
```

From (7.2) and (6.1), we find that the two ciphertexts differ in two hundred (200) bits. This once again shows that the algorithm has a pronounced avalanche effect.

8. COMPUTATIONAL EXPERIMENTS AND CONCLUSIONS

In this paper, we have developed a block cipher for a block of size 196 bits. Further, it is extended to a block of size 392 bits by adopting a procedure called interlacing.

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

The iterative procedure together with interlacing adopted in this analysis enabled us to mix the plaintext and the key very thoroughly. This has resulted in a cipher, which cannot be broken by any cryptanalytic attack.

We, therefore, conclude that the cipher is a very strong one, and it can be used effectively for achieving security in transfer of information.

REFERENCES

- [1] William Stallings, "Cryptography and Network Security: Principles and Practices", Third edition, Chapter 2, pp.37.
- [2] Feistel, H. "Cryptography and Computer Privacy", Scientific American, vol. 228, No. 5, pp.15-23, 1973.
- [3] Feistel, H., Notz, W., and Smith, J. "Some Cryptographic Techniques for Machine-to-Machine Data Communications", Proceedings of the IEEE, vol. 63, No. 11, pp. 1545-1554, Nov. 1975.
- [4] V.U.K.Sastry, and V.Janaki, "On the Modular Arithmetic Inverse in the Cryptology of Hill Cipher", Proceedings of North American Technology and Business Conference, September 2005, Montreal, Canada.