Journal of Computer Science 3 (7): 556-560, 2007
ISSN 1549-3636

A Block Cipher Using Linear Congruences

[1]V.U.K. Sastry and [2]V. Janaki
[1]Academic Affairs, Sreenidhi Institute of Science & Technology, Ghatkesar, Hyderabad
[2]Kakatiya Institute of Technology & Science, Warangal, India

Abstract: We have developed a block cipher by using modular arithmetic inverse and linear congruences. The cipher contains a key matrix called the outer key. It also includes another key, which contains a set of constants involved in the linear congruences. This key is called as inner key. The cryptanalysis carried out in this paper indicates that the cipher cannot be broken by any cryptanalytic attack. This cipher is extended to the case of a larger block wherein interlacing and iteration also play a vital role.

Keywords: modular arithmetic inverse, inner key, outer key, linear congruences.

INTRODUCTION

In the literature of cryptography Hill cipher [1] has been a prominent block cipher. Considering only 26 alphabetic characters a to z, Hill developed a block cipher whose encryption can be described by the equation

$$C=KP \bmod 26, \quad (1.1)$$

where K is a key matrix of size *nxn*, P is a plaintext vector, and C is the ciphertext vector both having n components. The decryption of the cipher is carried out by using the relation

$$P=K^{-1} C \bmod 26 \quad (1.2)$$

where K^{-1} is the modular arithmetic inverse [2] of the key matrix K.

From the cryptanalysis of the cipher it is seen that it cannot be broken by bruteforce attack when the size of the matrix is large. However, in the case of the known plaintext attack, it is clearly established that the cipher can be broken by taking appropriately n column vectors of plaintext and ciphertext.

In the present paper our objective is to modify the Hill cipher by introducing an additional key. To this end, we use linear congruences, in the column vector of the plaintext, wherein the congruences contain the numbers corresponding to the plaintext characters. Here, we consider a plaintext, which includes characters that can be represented by ASCII code. Thus, we use mod 128 instead of mod 26 used in the Hill cipher. From the cryptanalysis developed in this paper, we find that the cipher cannot be broken by any cryptanalytic attack.

In section 2 of this paper, we have discussed the development of the cipher. In section 3, we have described the algorithms for encryption, decryption and presented a procedure for the modular arithmetic inverse of a matrix. In section 4, we have illustrated the cipher by considering an example. The cryptanalysis for this cipher has been carried out in section 5.In section 6, we have extended the analysis to a larger block by interlacing and iteration. Then, in section 7, we have examined the avalanche effect. Finally in section 8, we have presented the computations and conclusions.

DEVELOPMENT OF THE CIPHER

Consider a plaintext vector, which can be represented in the form

$$p = (p_1, p_2, p_3, \ldots\ldots\ldots\ldots p_n)^T. \quad (2.1)$$

Let us suppose that we choose a key matrix K given by

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

where the matrix K is non singular, and its determinant is relatively prime to 128.

Corresponding Author: V. Janaki, Kakatiya Institute of Technology and Science, Warangal, India

The aforementioned conditions are to be satisfied for the existence of the modular arithmetic inverse of K with respect to mod 128.

Let $C = (C_1,C_2,C_3\ldots\ldots\ldots\ldots\ldots C_n)^T$ be the ciphertext vector. (2.3)

Let us now introduce n linear congruences given by

$$P_i = (a_i p_i + b_i) \bmod 128,\ i=1 \text{ to } n, \quad (2.4)$$

where a_i and b_i are constants, chosen appropriately, as mentioned below.
In the process of encryption, the ciphertext C can be written as

$$C=KP \bmod 128, \quad (2.5)$$

where $P=(P_1,P_2,P_3\ldots\ldots\ldots\ldots\ldots\ldots P_n)^T$.

Here the components of the plaintext vector p_i (i =1 to n) are obtained from the consecutive n characters of the given plaintext.

Here in (2.4), we choose each one of the a_is as an odd integer, which lies between 0 and 127, and each one of the b_is as any integer lying between 0 and 127.The reason for this choice of the values of a_i and b_i, will be clear very soon. When a_i, b_i and p_i are known to us we can readily calculate P_i by using (2.4). On the other hand, when the P_i is known to us, p_i can be determined by solving (2.4). As we have assumed that b_i is an integer which lies between 0 and 127, we can write (2.4) in the form

$$P_i - b_i = a_i p_i \bmod 128. \quad (2.6)$$

As a_i is an odd integer, which lies between 0 and 127, it is relatively prime to 128.
Thus we obtain d_i, the multiplicative inverse if a_i, such that

$$a_i d_i \bmod 128=1 \quad (2.7)$$

where d_i is the multiplicative inverse of a_i.
From (2.6) and (2.7), we get

$$p_i = (P_i - b_i) d_i \bmod 128. \quad (2.8)$$

Now let us consider the process of decryption. From the equation (2.5) we get

$$P = K^{-1} C \bmod 128 \quad (2.9)$$

where K^{-1} is the modular arithmetic inverse of K. On using (2.9) and (2.8) we get p_i, the components of the plaintext as we have indicated in the aforementioned discussion.

The problem of the encryption, given by the equation (2.5) can be written in the form

$$\begin{pmatrix} C_1 \\ C_2 \\ C_3 \\ \ldots. \\ \ldots. \\ C_n \end{pmatrix} = \begin{pmatrix} k_{11}\ k_{12}\ \ldots\ldots\ k_{1n} \\ k_{21}\ k_{22}\ \ldots\ldots k_{2n} \\ k_{31}\ k_{32}\ldots\ldots\ k_{3n} \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ k_{n1}\ k_{n2}\ \ldots\ldots k_{nn} \end{pmatrix} \begin{pmatrix} P_1 \\ P_2 \\ P_3 \\ \ldots. \\ \ldots. \\ P_n \end{pmatrix} \bmod 128 \quad (2.10)$$

Here firstly we have to obtain P_i where $P_i = (a_i p_i + b_i) \bmod 128$. For this we require the values of a_i, and b_i (i=1 to n). To this end we introduce a key comprising the numbers $a_1,a_2\ldots\ldots a_n$ and $b_1,b_2\ldots\ldots b_n$ and call this as the inner key. Subsequently we have to apply the key matrix K for obtaining C. Thus we consider this key as the outer key. Here it is to be noted that in the process of decryption firstly the outer key is to be applied and then the inner key is to be used. Thus both the keys are to be supplied by the sender in a secret manner to the receiver.

In what follows we design the algorithms for the encryption, the decryption, and the modular arithmetic inverse of the key matrix.

ALGORITHMS

3.1 Algorithm for encryption

```
{
1. for i=1 to n
   {
2.  read  p_i , a_i , b_i .
3.  P_i  =( p_i  a_i + b_i )  mod 128.
   }
4. read the key matrix K.
5.   C=KP mod 128.
6.   write C.
}
```

3.2 Algorithm for decryption.

{

1. for i=1 to n read a_i , b_i .
2. read K,C.
3. Find K^{-1} .
4. P= K^{-1} C mod 128.
5. for i=1 to n

{

Find d_i such that $a_i d_i$ mod 128=1.

6. p_i =(P_i - b_i) d_i mod 128

}

7. write p_i

}

3.3 Algorithm for modular arithmetic inverse

// A is an nxn matrix. N is a positive integer with which //modular arithmetic inverse is carried out. Here N=128.

{

1. Find the determinant of A. Let it be denoted by Δ , where $\Delta \neq 0$.
2. Find the inverse of A. The inverse is given by $[A_{ji}]/\Delta$.
3. for i = 1 to N

{

if ((iΔ) mod N = 1) d = i;

//Δ is relatively prime to N.

break;

}

4. B=(d[A_{ji}]) mod N

// B is the modular arithmetic inverse of A

}

ILLUSTRATION OF THE CIPHER

Let us consider the plaintext –*Burn the forest as soon as the thieves enter into it*. Let the key matrix K be taken in the form

$$K = \begin{pmatrix} 99 & 4 & 12 & 9 & 5 & 12 \\ 13 & 125 & 18 & 26 & 6 & 14 \\ 30 & 10 & 124 & 24 & 26 & 87 \\ 28 & 29 & 30 & 98 & 50 & 44 \\ 63 & 45 & 78 & 89 & 120 & 56 \\ 127 & 45 & 59 & 110 & 53 & 111 \end{pmatrix}$$

Here n=6. (4.1)

Now let us focus our attention on the first six characters of the plaintext under consideration. The first six characters are *Burn*.

Considering the corresponding ASCII codes, the plaintext vector p can be obtained as

$$p = (66\ \ 117\ \ 114\ \ 110\ \ 32\ \ 116)^T. \quad (4.2)$$

Let us choose the inner key in the form

$$(a_1\ a_2\ a_3\ a_4\ a_5\ a_6\ \ b_1\ b_2\ b_3\ b_4\ b_5\ b_6) = (45\ \ 23\ \ 11\ \ 21\ \ 33\ \ 55\ \ 42\ \ 78\ \ 12\ \ 110\ \ 45\ \ 24) \quad (4.3)$$

On using (4.2) and (4.3), and the encryption algorithm 3.1, we get

$$(P_1\ P_2\ P_3\ P_4\ P_5\ P_6) = (68\ \ 81\ \ 114\ \ 116\ \ 77\ \ 4) \quad (4.4)$$

$$\text{and } C = (45\ \ 83\ \ 104\ \ 27\ \ 1\ \ 68)^T. \quad (4.5)$$

Then on using the algorithm 3.3, the modular arithmetic inverse of the matrix K, denoted by K^{-1},is obtained as

$$K^{-1} = \begin{pmatrix} 108 & 97 & 38 & 75 & 76 & 12 \\ 88 & 68 & 98 & 57 & 114 & 66 \\ 21 & 85 & 9 & 83 & 21 & 61 \\ 6 & 95 & 54 & 68 & 13 & 28 \\ 23 & 74 & 112 & 111 & 95 & 76 \\ 26 & 110 & 91 & 46 & 118 & 96 \end{pmatrix} \quad (4.6)$$

It can be readily verified that K^{-1} K mod 128 = K K^{-1} mod 128 = I.

Then on using the algorithm 3.2, we get

$$P = (68\ \ 81\ \ 114\ \ 116\ \ 77\ \ 4)^T \quad (4.7)$$

$$(p_1\ p_2\ p_3\ p_4\ p_5\ p_6) = (66\ \ 117\ \ 114\ \ 110\ \ 32\ \ 116). \quad (4.8)$$

The values of $p_1 \ldots p_6$ given by (4.2) and (4.8) are the same. Thus we get back the plaintext.

CRYPTANALYSIS

In the process of encryption we have

$$C = KP \bmod 128, \quad (5.1)$$

where $P_i = (a_i p_i + b_i) \bmod 128$, i=1 to n. (5.2)

Here when the ciphertext C is known to us, the plaintext p can be found if the matrix K, and the a_i and

the b_i are known to us, i.e if the outer key and the inner key are known to us. The key matrix is of size n×n. The a_i's are n in number and the b_i's are also n in number. The number of combinations of the secret key, including the outer key K and the inner key comprising a_i and b_i, can be determined as follows. The outer key K contains n^2 numbers wherein each one can be represented in terms of 7 binary bits. Thus the key space corresponding to this key is given by

2^{7n^2}. Now let us consider the key space of the inner key. As the a_is are purely odd numbers, lying between 0 and 127, they can be represented by 7 binary bits wherein the least significant bit all the while remain as 1. As the number of a_i s is n, the possible number of combinations of the a_is is 2^{6n}. As b_i is any number that lies between 0 and 127, the possible number of combinations of b_i s is 2^{7n}. Thus the total search space for the secret key including the outer key K, and the inner key $a_1, a_2 \ldots\ldots a_n$, $b_1, b_2 \ldots\ldots b_n$ can be obtained as

$$2^{7n^2} \times 2^{6n} \times 2^{7n} = 2^{7n^2 + 13n}.$$

For every possible key of the key space, the attacker has to find the plaintext till he gets a meaningful one. This process is to be carried out at least with half of the possible keys. If a plaintext corresponding to a secret key, can be obtained, by the decryption process in 10^{-7} sec., then the time T required for computing with half of the possible keys, is given by

$$T = \lambda \cdot 2^{7n^2 + 13n} \text{ centuries},$$

where $\lambda = 10^{-7} / 60 \times 60 \times 24 \times 365 \times 100 = 1.585 \times 10^{-18}$

Let us now consider the known plaintext attack. In this case we know as many pairs of plaintext and ciphertext as we require. For each plaintext vector p we are to find P s for all possible combinations of the values of a_i and b_i i.e, for each possible inner key. Thus the number of P s corresponding to each p is $(2^6)^n \times (2^7)^n = 2^{13n}$ as a_i is an odd integer lying between 0 and 127, and b_i is any integer lying between 0 and 127. If we take n plaintext vectors and form a matrix with these vectors, then the number of matrices containing the corresponding Ps is $2^{13\,n^2}$.

In view of the example given in section 4,we have n=6.In this case the number of matrices containing P s are 2^{13x36}.

Now, let us suppose that finding the modular arithmetic inverse of each matrix takes

10^{-7} sec., then finding all possible modular arithmetic inverses will take

$$2^{13x36} \times 10^{-7} \approx 10^{133} \text{ sec} \approx 3.17 \times 10^{122} \text{ centuries}.$$

Thus we conclude that the strength of the cipher increases enormously, and it cannot be broken by the known plaintext attack.

A LARGER BLOCK CIPHER USING INTERLACING AND ITERATION

In section 2, we have developed the cipher for a block of n characters. Let us now extend the analysis for a block of 2n characters by introducing the concepts interlacing and iteration. In this section, the procedures used for encryption and decryption are presented in Figures 1 and 2.

In the procedure of encryption, the block consisting of 2n characters is divided into two blocks left half and right half each containing n characters. On these two halves the same procedure, discussed in section 2, is applied. Then we obtain n characters as output on both the sides. The n characters on each side are converted into 7n binary bits.

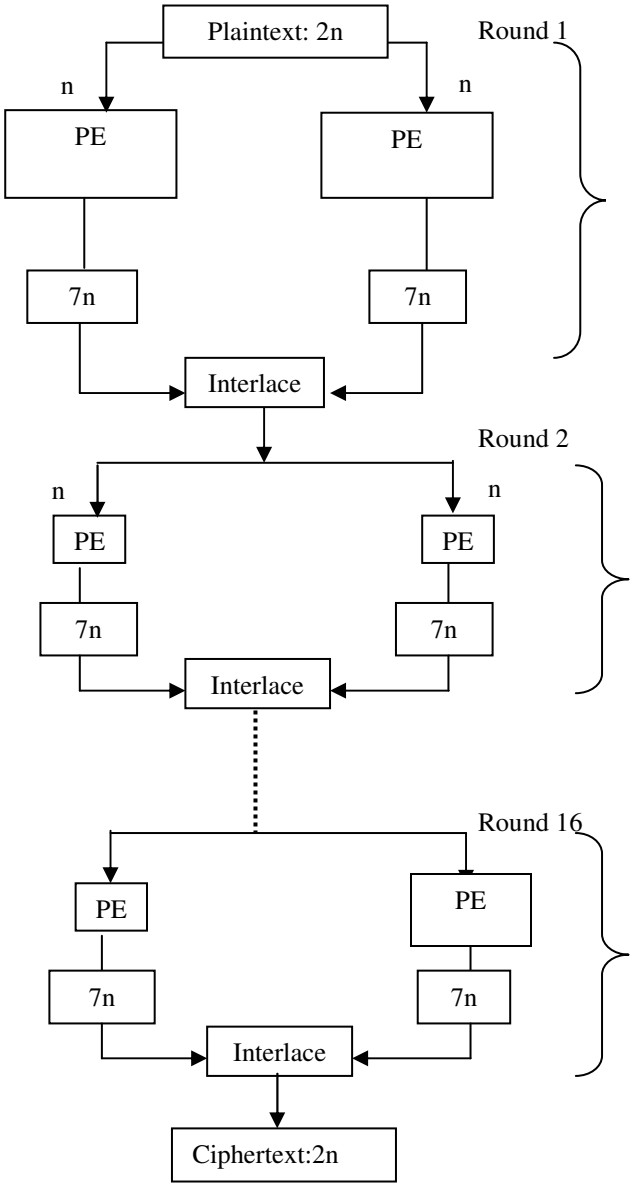

Fig.1: Procedure for Encryption in the case of larger block cipher containing 2n

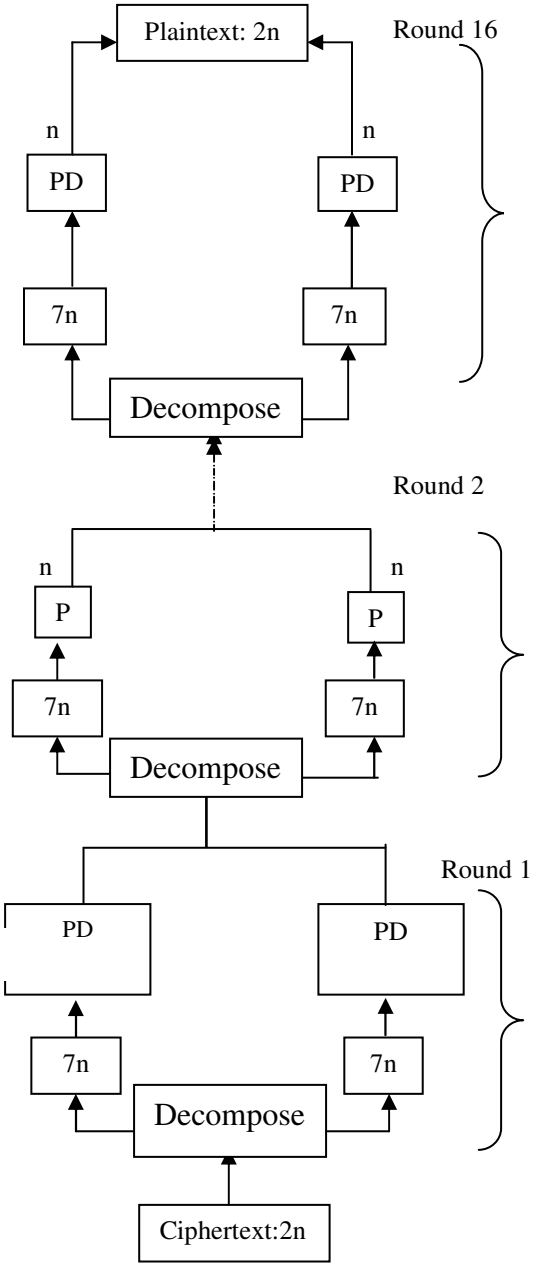

Fig.2: Procedure for Decryption in the case of larger block cipher containing 2n characters

The process of interlacing can be described as follows. The first bit of left side 7n bits is placed as the first bit of an array. The first bit of the right side 7n bits is placed as a second bit in the array. Then the second bit of the left 7n bits is placed in the third place of the array. This process is continued till we exhaust all the 7n bits on both the sides.

The procedure described above constitutes one round. This process is repeated for 16 rounds and then ultimately we get the ciphertext.

The process of decryption is completely a reverse process of encryption. The decompose, used in decryption, is a function in which the 14n bits of the 2n characters are separated into 7n bits on the left side and 7n bits on the right side.

By using the process of encryption we are able to encrypt 2n characters and obtain the corresponding ciphertext. Further, by performing decryption we are able to obtain the plaintext of length 2n characters from the ciphertext.

In order to illustrate the above procedure, let us consider the plaintext

Burn the for (6.1)

which is consisting of 12 characters. Following the encryption procedure given in Fig.1, the ciphertext corresponding to the plaintext (6.1), is obtained in terms of binary bits as follows

100011110010101000110111011100001001010111010
100000011010001111101100101101000011101 (6.2)

On applying the procedure given in Fig.2, the ciphertext (6.2) can be converted into the plaintext given by (6.1).

AVALANCHE EFFECT

Let us consider the plaintext given by (6.1). On changing the first character B in the plaintext to C, the plaintext assumes the form

Curn the for. (6.3)

In binary bit representation (6.1) and (6.3) differ only one in binary bit as B and C differ in one bit. Now on applying the encryption procedure given in Fig.1, on the modified plaintext (6.3), we get the ciphertext in the form

110100010011111111100100010001111001010101011
101111000110010111010011000101101100001 (6.4)

Here we notice that (6.2) and (6.4) differ in 30 bits. This indicates that the avalanche effect is not at all less significant.

Consider the effect on account of a change in the inner key, which plays a prominent role on the cipher. Let us now we take the inner key as

45 21 11 21 33 55 42 78 12 110 45 24 (6.5)

instead of (4.3). On using this key and the encryption procedure given in Fig.1, we get the ciphertext in the form

011010011101010101000111111000000101000000001
001101110010010000001010011101011010000 (6.6)

On comparing (6.2) and (6.6) we find that they differ in 31 bits. This again shows that the avalanche effect is significant.

COMPUTATIONS AND CONCLUSIONS

In this paper we have developed a block cipher by using linear congruences and modular arithmetic inverse. Firstly the plaintext vector is modified by using the linear congruences. These congruences contain a set of constants, which form a key called the inner key. The modified plaintext is operated by a key matrix called as outer key The inner and outer keys are used in the process of encryption and in the process of decryption, and they form the secret key. This cipher is extended to the case of larger block (block size is doubled) by introducing interlacing and iteration.

Here all the programs for encryption and decryption are written in C language. On performing computations we have obtained the ciphertext for a given plaintext and vice-versa. The ciphertext obtained in the case of the plaintext *Burn the forest as soon as the thieves enter into it.* is given by

100011110010101000110111011100001001010111010
100000011010001111101100101101000011101111101
010111101011000010110000000011010111010110001
001011101000110101001101100000100101110000001
001111011011111010011000010011101110000010001
001101001010000001100110101100000001100110110
000100100111011111100011001110110011001100111
000111111100001100100001101101100010110011110
000010100010000011110101111001101101100110101
010000111001010

From the cryptanalysis it is cleanly seen that the cipher cannot be broken by any cryptanalytic attack. The interlacing and the iteration strengthen the cipher remarkably.

From the analysis presented in this paper we find that the outer key and the inner key both play a vital role in strengthening the cipher. The strength is further enhanced in the case of the larger block.

REFERENCES

1. Cryptography and Network Security, William Stallings, 3rd Edition, Pearson Education
2. On the Modular Arithmetic Inverse in the Cryptology of Hill cipher, 2005. V.U.K.Sastry, V.Janaki, Proceedings of North American Technology and Business Conference, Canada