A Large Block Cipher Using Linear Congruences

Dr. V.U.K Sastry, V.Janaki, *Members, IAENG*

***Abstract*— In this paper we have modified the Hill cipher by using linear congruences. In this analysis we have two secret keys: (1) the key matrix, and (2) the key involving the constants occurring in the linear congruences. These two keys are termed as outer key and inner key respectively. From the cryptanalysis carried out in this paper, we have found that the inner key plays a very significant role in strengthening the cipher..**

***Index Terms*— External key, internal key, linear congruences, modular arithmetic inverse.**

I. Introduction

In a recent paper [1], following Hill [2], we have developed a block cipher by using linear congruences and modular arithmetic inverse [3]. In this, we have introduced a pair of secret keys in which the first key is taken in the form of a matrix, and the second key is chosen as a set of constants occurring in the linear congruences involving the plaintext. The first key is of size nxn, and the second key is of size n. We have illustrated the cipher with n=6.In this analysis, the total length of the keys is 336 binary bits and the length of the plaintext is 84 binary bits.

In the present paper, our objective is to develop a block cipher wherein the block length is significantly large. In this analysis, we have taken the first key as a matrix of size nxn, the second key as a set of numbers of size 2n2, and the plaintext in the form of a matrix of size nxn. Here we have illustrated the cipher with n=4.In this, the total length of the keys is 336 bits, and the length of the plaintext is 112 bits. This analysis is further extended to the case of 224 bits by applying a procedure called interlacing.

In this paper we have dealt with the development of the cipher in section 2, and presented the algorithms for encryption and decryption in section 3.We have illustrated the cipher for n=4 in section 4, and investigated the cryptanalysis in section 5. Then in section 6, we have extended the above analysis to a larger block wherein the block size is doubled. Finally, we have discussed the computations and conclusions in section 7.

II. Development of the Cipher

Consider a plaintext which can be represented in the form of a matrix given by

$$P= [p_{ij}],\ i=1 \text{ to } n,\ j=1 \text{ to } n. \qquad (2.1)$$

Let us choose a key matrix K given by

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

where the matrix K is non singular, and its determinant is relatively prime to 128.Here it is to be noted that the above conditions are to be satisfied for the existence of the modular arithmetic inverse of K with respect to mod 128.

$$\text{Let } C = [c_{ij}],\ i=1 \text{ to } n,\ j=1 \text{ to } n, \qquad (2.3)$$

be the ciphertext matrix.

Let us now introduce n^2 linear congruences given by

$$P_{ij} = (a_{ij}p_{ij} + b_{ij}) \bmod 128,\ i=1 \text{ to } n,\ j=1 \text{ to } n, \qquad (2.4)$$

where a_{ij} and b_{ij} are constants, taken together, constitute the second key. In the process of encryption the ciphertext C can be obtained by using the relation

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

where $P = [P_{ij}]$, i=1 to n, j=1 to n, is the modified plaintext matrix.

Now let us consider the process of decryption. In (2.4), we choose each one of the a_{ij} s as an odd integer lying between 0 and 127, and each one of the b_{ij} s as any integer lying between 0 and 127. It is to be noted that, these conditions are to be satisfied for obtaining p_{ij} in terms of P_{ij} from (2.4).

When a_{ij}, b_{ij} and p_{ij} are known to us, we can readily obtain P_{ij} from (2.4). On the other hand when P_{ij}s are known to us, p_{ij} can be determined, for each i and j, by solving (2.4) .From (2.4) we get

$$P_{ij} - b_{ij} = a_{ij}\, p_{ij} \bmod 128, \qquad (2.6)$$

as all b_{ij}s lie between 0 and 127.As each a_{ij}, is an odd integer lying between 0 and 127, it is relatively prime to 128. Thus we get the multiplicative inverse of a_{ij}, denoted by d_{ij} by solving the equation

$$(a_{ij} .d_{ij}) \bmod 128 = 1, \qquad (2.7)$$

for all i and j.

From (2.6) and (2.7) we get

$$p_{ij} = ((P_{ij} - b_{ij})\ d_{ij}) \bmod 128. \qquad (2.8)$$

Thus we have seen that the relation between p_{ij} and P_{ij} is a reversible one. From the equation (2,5) we get

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

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

In this analysis, we call the key matrix K as the outer key, and the key constituted by a_{ij} and b_{ij} as the inner key, and these two keys will be treated as secret keys.

III. ALGORITHMS

3.1 Algorithm for Encryption

```
  {
 1 .read n, K;
 2. read $a_{ij}$, $b_{ij}$, $p_{ij}$ for i=1 to n, j=1 to n;
 3. for i =1 to n
      for j=1 to n
      {
    $P_{ij}=(a_{ij}\, p_{ij} + b_{ij})$ mod 128;
      }
 4. C=KP mod 128;
 5. write C;
  }
```

3.2 Algorithm for Decryption

```
  {
 1. read  n, K, C;
 2. read  $a_{ij}$, $b_{ij}$, for i=1 to n, j=1 to n;
 3. find $K^{-1}$;
    4. P=$K^{-1}$C mod 128;
 5. for i=1 to n
      for j=1 to n
      {
        find $d_{ij}$ such that  $a_{ij}\, d_{ij}$ mod 128=1;
        $p_{ij}=(p_{ij}-b_{ij})d_{ij}$ mod 128;
      }
 6. write $p_{ij}$;
  }
```

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 $\Delta$, 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 ( $(i\Delta)$ mod N = 1 )  d = i;
      //$\Delta$ is relatively prime to N.
      break;
    }
 B=( d[$A_{ji}$] ) mod N
      // B is the modular arithmetic inverse of A
 }
```

IV. ILLUSTRATION OF THE CIPHER

Consider the plaintext:

we have granted one billon dollars as flood relief fund. Sorry to note that your land is devastated and the crop is rooted out! (4.1)

Let us focus our attention on the first 16 characters of the plaintext which is given by:

we ␢ *have* ␢ *granted* ␢ (4.2)

By using ASCII codes, the above plaintext can be written in the form of a matrix given by

$$p=\begin{pmatrix} 119 & 101 & 32 & 104 \\ 97 & 118 & 101 & 32 \\ 103 & 114 & 97 & \\ 110 & & & \end{pmatrix} \qquad (4.3)$$

We take the outer key K in the form

$$K=\begin{pmatrix} 18 & 4 & 7 & 3 \\ 4 & 6 & 5 & 42 \\ 40 & 31 & 9 & 22 \\ 35 & 17 & 23 & 71 \end{pmatrix} \qquad (4.4)$$

Let us represent the inner key in the form of a pair of matrices $[a_{ij}]$ and $[b_{ij}]$, i=1 to 4, j=1 to 4.

These matrices are taken as

$$[a_{ij}]=\begin{pmatrix} 1 & 21 & 3 & 23 \\ 5 & 25 & 7 & 27 \\ 9 & 29 & 11 & 31 \\ 13 & 33 & 15 & 35 \end{pmatrix} [b_{ij}] = \begin{pmatrix} 21 & 102 & 37 & 49 \\ 85 & 126 & 87 & 100 \\ 31 & 112 & 43 & 84 \\ 91 & 26 & 67 & 21 \end{pmatrix} \qquad (4.5)$$

On using the algorithm 3.1 we get

$$P=\begin{pmatrix} 12 & 47 & 5 & 9 \\ 58 & 4 & 26 & 68 \\ 62 & 90 & 86 & 38 \\ 63 & 31 & 31 & 117 \end{pmatrix} \qquad (4.6)$$

and

$$C=\begin{pmatrix} 47 & 49 & 121 & 27 \\ 24 & 44 & 116 & 44 \\ 126 & 40 & 30 & 8 \\ 9 & 96 & 60 & 28 \end{pmatrix} \qquad (4.7)$$

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

$$K^{-1}=\begin{pmatrix} 75 & 85 & 127 & 37 \\ 120 & 115 & 69 & 84 \\ 110 & 101 & 22 & 64 \\ 115 & 125 & 76 & 114 \end{pmatrix} \qquad (4.8)$$

From (4.4) and (4.8) we readily find that

$$KK^{-1} \bmod 128=K^{-1}K \bmod 128=I. \qquad (4.9)$$

Then on using the algorithm 3.2 we get

$$P=\begin{pmatrix} 12 & 47 & 5 & 9 \\ 58 & 4 & 26 & 68 \\ 62 & 90 & 86 & 38 \\ 63 & 31 & 31 & 117 \end{pmatrix} \qquad (4.10)$$

and hence

$$p=\begin{pmatrix} 119 & 101 & 32 & 104 \\ 97 & 118 & 101 & 32 \\ 103 & 114 & 97 & 110 \\ 116 & 101 & 100 & 32 \end{pmatrix} \qquad (4.11)$$

Thus we have obtained the original plaintext given by (4.3).

V. Cryptanalysis

In the case of the Hill cipher, it is well known that it can be broken by known plaintext attack. This is on account of the fact that we can form an equation of the form

$$Y=KX \bmod 26,$$

where Y contains the ciphertext column vectors, X contains the plaintext column vectors, and the modular arithmetic inverse of X is calculable.

Now let us perform the cryptanalysis of the present problem by considering all possible conventional cryptanalytic attacks namely, ciphertext only attack, known plaintext attack, chosen plaintext or ciphertext attack.

In the case of the outer key K, as we have n^2 elements, and as each element can be represented in terms of 7 binary bits, the size of the corresponding key space is 2^{7n^2}. For the inner key, the size of the key space is 2^{13n^2} (as the a_{ij}s are odd numbers). Thus the size of the entire key space is 2^{20n^2}. This is a formidable entity, and hence the bruteforce attack is ruled out. In the case of the known plaintext attack, we know as many pairs of plaintext and ciphertext as we desire. Here also it is possible to form an equation of the form

$$Y = KX \bmod 128,$$

which is similar to that in the case of the Hill cipher. Nevertheless, in all the columns of X, we have the components of the inner key constituted by a_{ij} and b_{ij}. The size of the key space corresponding to this key is 2^{13n^2}. This is also a very large number when $n \geq 3$. Of course, in the present analysis, we have taken n=4. Thus the cipher under consideration cannot be broken by known plaintext attack.

Lastly, in the case of chosen plaintext or ciphertext attack also, we intuitively find that the inner key containing a_{ij}s and b_{ij}s totally precludes the breaking of the cipher.

Thus we conclude that the cipher cannot be broken by any cryptanalytic attack.

VI. Analysis of a Large Block Cipher Using Interlacing and Iteration

In this we consider a block of 32 characters taken from (4.1).The block can be mentioned as:

we␢have␢granted␢one␢billion␢doll (6.1)

The process of encryption and the process of decryption of this block can be carried out by adopting the procedures depicted in the schematic diagram given in Fig.1.

In the process of encryption, the plaintext containing 32 characters is divided into two blocks, each containing 16 characters. Then the procedure of encryption, discussed earlier, is applied on the left side block as well as on the right side block. The ciphertext in the left side, and the ciphertext in the right side, obtained in terms of decimal numbers, are now converted into binary bits and they are interlaced as per the procedure given below.

Let b_1 b_2 b_3 …be the binary bits of the left side ciphertext, and d_1 d_2 d_3 …be the binary bits corresponding to the right side ciphertext. We place these binary bits one after another as shown below.

b_1d_1 $b_2d_2b_3d_3$……. .

Then we divide these bits into two blocks wherein each one is containing 112 binary bits. They are again converted into decimal numbers and used in the subsequent round. This process is continued for 16 rounds, and we get the ciphertext ultimately. The ciphertext corresponding to the plaintext (6.1) is obtained as

01000000010111100000101101100001110001011111010110
00011100101000010101011101111010100111010110110011
011000111100 (6.2)

The process of decomposition used in decryption is a reverse process to that of interlacing which is mentioned above. On adopting the process of decryption we get back the original plaintext.

VII. Computations and Conclusions

In this paper, we have modified the Hill cipher by introducing an inner key which transforms the plaintext in an effective manner. In the example discussed in this analysis, the outer key is of length 112 bits, and the inner key is of length 224 bits. We may say the length of the secret key as 336 bits. The lengths of the plaintext in the examples under consideration are 112 bits and 224 bits.

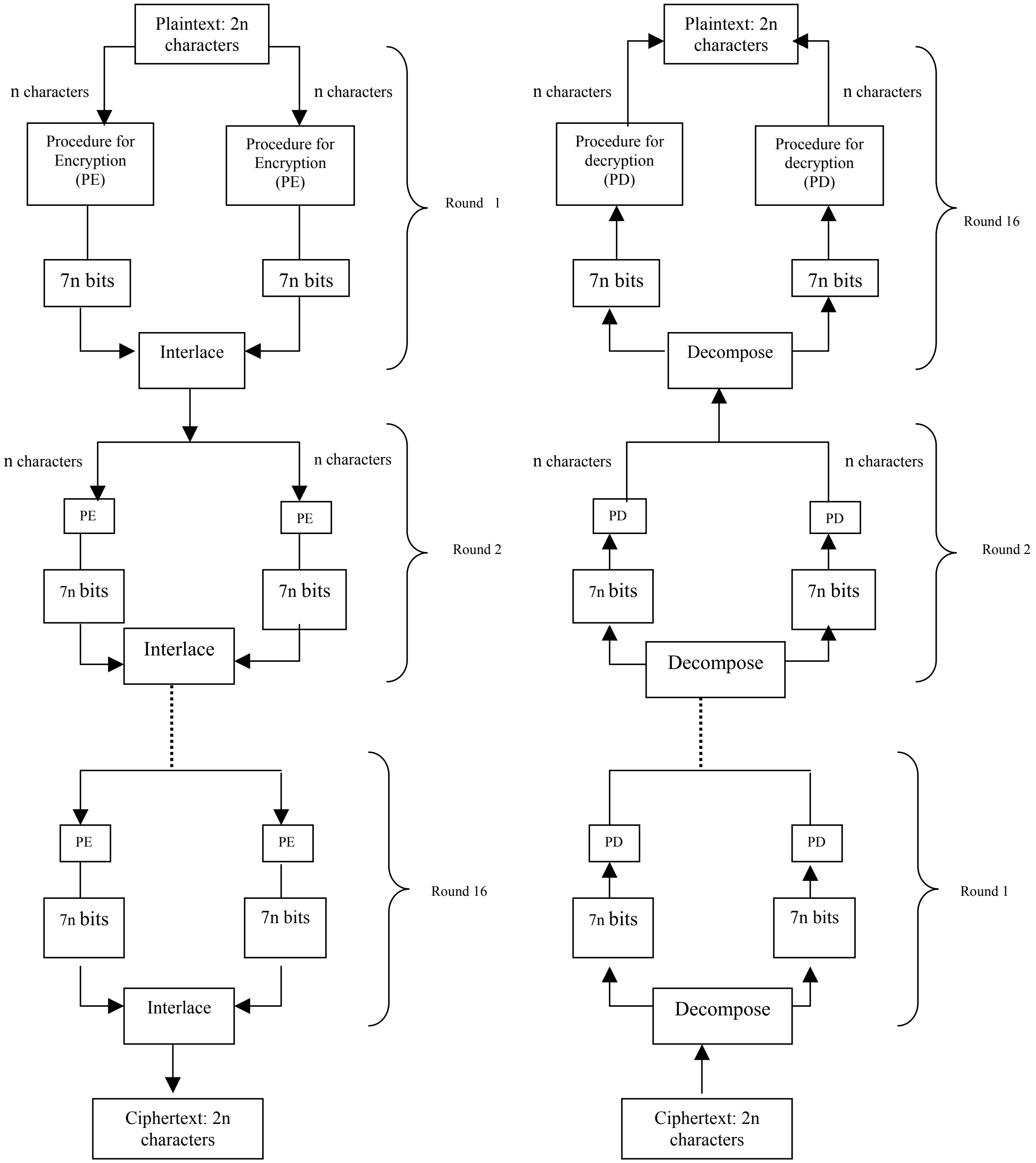
The algorithms developed in this analysis, for encryption and decryption, are written in C language.

The ciphertext corresponding to the entire plaintext given by (4.1) is obtained (in hexadecimal notation) in the form

20 17 41 36 0E 17 6B 07 14 15 3B 6A 2A 14 6C 3C 5F 6B 2D
3F 4C 5F 07 0C 15 36 02 4E 15 17 37 70 68 55 38 5D 1C 2F 48
58 4D 24 6F 76 15 11 75 69 2B 07 2D 79 73 1B 20 24 60 1E 51
3E 55 40 26 1A 3C 04 74 52 10 4E 46 3E 64 2D 36 52 3B 44
3A 6E 58 1D 4D 7A 09 46 3C 64 3A 38 68 33 4D 2D 1D 6F 40
4A 25 15 21 02 31 3C 40 0B 79 3F 24 67 68 7C 10 79 3F 03 4D
6E 68 23 1D 46 0E 12 3A 51.

It may be noted here that padding is to be done to make a complete block wherever it is required.

From the above analysis, we conclude that the inner key , arising on account of the linear congruences, together with the outer key, already existing in the Hill cipher, plays a vital role in strengthening the cipher.



(a) Process of encryption

(b) Process of decryption

Fig.1. Schematic diagram of the cipher

REFERENCES

[1] V.U.K.Sastry, V.Janaki, A block cipher using linear congruences, accepted for publication in Journal of Computer Science, Science publications, Newcity, NewYork.

[2] William Stallings, “Cryptography and Network Security”, 3rd Edition, Pearson Education.

[3] V.U.K.Sastry, V.Janaki., ”On the Modular Arithmetic Inverse in the Cryptology of Hill cipher“, Proceedings of North American Technology and Business Conference, September 2005, Canada.