http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet
Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 6 (3): 396-404, 2007
ISSN 1812-5638

A Block Cipher Involving Interlacing and Decomposition

[1]S. Udaya Kumar, [1]V.U.K. Sastry and [2]A. Vinaya babu
[1]SreeNidhi Institute of Science and Technology, Hyderabad, India
[2]JNT University, Hyderabad, India

Abstract: In this study, we have developed a block cipher for a block of size 112 bits by introducing the basic concepts interlacing and decomposition. Here, we have taken the key in terms of a set of matrices and the plaintext also in the form of matrices, wherein all the matrices are containing binary bits. In the process of encryption, we have employed an iterative procedure. In the process of decryption, we have used the modular arithmetic inverses of the key matrices. The cryptanalysis carried out in this paper clearly shows that the cipher cannot be broken by any cryptanalytic attack.

Key words: Block cipher, ciphertext, plaintext, key matrix, modular arithmetic inverse

INTRODUCTION

In the classical literature of cryptography, Hill cipher (Stalling, 2002) 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 matrix and performing mod 26.

Following Hill, (Feistel, 1973; Feistel *et al*., 1975), made an attempt to develop a block cipher, wherein both 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. However, he has found that the cipher can be broken by the known plaintext attack.

In the present research, our objective is to develop a block cipher, wherein we employ a process involving iteration, interlacing and decomposition. In this, the plaintext and the key are represented in terms of matrices consisting of binary bits. Here, we take that the number of key matrices is equal to the number of plaintext matrices. In this, our interest is to develop a cipher, which cannot be broken by any cryptanalytic attack.

Interlacing and decomposition: Let us illustrate the process of interlacing by considering a typical example. Let x_i, i = 1 to 4 be four matrices given by

$$x_i, = [x_{ijk}],\ j = 1 \text{ to } 7,\ k = 1 \text{ to } 4, \qquad (1)$$

where i is the matrix number, j, the row number and k is the column number.

Now (1) can be written as

$$X_1 = \begin{bmatrix} x_{111} & x_{112} & x_{113} & x_{114} \\ x_{121} & x_{122} & x_{123} & x_{124} \\ x_{131} & x_{132} & x_{133} & x_{134} \\ x_{141} & x_{142} & x_{143} & x_{144} \\ x_{151} & x_{152} & x_{153} & x_{154} \\ x_{161} & x_{162} & x_{163} & x_{164} \\ x_{171} & x_{172} & x_{173} & x_{174} \end{bmatrix}, X_2 = \begin{bmatrix} x_{211} & x_{212} & x_{213} & x_{214} \\ x_{221} & x_{222} & x_{223} & x_{224} \\ x_{231} & x_{232} & x_{233} & x_{234} \\ x_{241} & x_{242} & x_{243} & x_{244} \\ x_{251} & x_{252} & x_{253} & x_{254} \\ x_{261} & x_{262} & x_{263} & x_{264} \\ x_{271} & x_{272} & x_{273} & x_{274} \end{bmatrix},$$

$$X_3 = \begin{bmatrix} x_{311} & x_{312} & x_{313} & x_{314} \\ x_{321} & x_{322} & x_{323} & x_{324} \\ x_{331} & x_{332} & x_{333} & x_{334} \\ x_{341} & x_{342} & x_{343} & x_{344} \\ x_{351} & x_{352} & x_{353} & x_{354} \\ x_{361} & x_{362} & x_{363} & x_{364} \\ x_{371} & x_{372} & x_{373} & x_{374} \end{bmatrix}, X_4 = \begin{bmatrix} x_{411} & x_{412} & x_{413} & x_{414} \\ x_{421} & x_{422} & x_{423} & x_{424} \\ x_{431} & x_{432} & x_{433} & x_{434} \\ x_{441} & x_{442} & x_{443} & x_{444} \\ x_{451} & x_{452} & x_{453} & x_{454} \\ x_{461} & x_{462} & x_{463} & x_{464} \\ x_{471} & x_{472} & x_{473} & x_{474} \end{bmatrix}, \qquad (2)$$

The process of interlacing can be described as follows.

The last element of the fourth column of the fourth matrix i.e., x_{474} is placed as the first element of the first row of a new first matrix. The last but one element of the fourth column of the fourth matrix (x_{464}) is placed as the first element of the first row of a new second matrix. Then the x_{454} and the x_{444} are placed as the first elements of the first rows of the new third and the new fourth matrices respectively. In a similar manner all the other elements of the four matrices x_i, i = 1 to 4, are placed in the four new matrices $<x_i>$. Here, the symbol < > denotes interlacing.

Corresponding Author: S. Udaya Kumar, SreeNidhi Institute of Science and Technology, Hyderabad, India

$$<X_1>=\begin{bmatrix} x_{474} & x_{434} & x_{463} & x_{423} \\ x_{452} & x_{412} & x_{441} & x_{374} \\ x_{334} & x_{363} & x_{323} & x_{352} \\ x_{312} & x_{341} & x_{274} & x_{234} \\ x_{263} & x_{223} & x_{252} & x_{212} \\ x_{241} & x_{174} & x_{134} & x_{163} \\ x_{123} & x_{152} & x_{112} & x_{141} \end{bmatrix}, <X_2>=\begin{bmatrix} x_{464} & x_{424} & x_{453} & x_{413} \\ x_{442} & x_{471} & x_{431} & x_{364} \\ x_{324} & x_{353} & x_{313} & x_{342} \\ x_{371} & x_{331} & x_{264} & x_{224} \\ x_{253} & x_{213} & x_{242} & x_{271} \\ x_{231} & x_{164} & x_{124} & x_{153} \\ x_{113} & x_{142} & x_{171} & x_{131} \end{bmatrix}, <X_3>=\begin{bmatrix} x_{454} & x_{414} & x_{443} & x_{472} \\ x_{432} & x_{461} & x_{421} & x_{354} \\ x_{314} & x_{343} & x_{372} & x_{332} \\ x_{361} & x_{321} & x_{254} & x_{214} \\ x_{243} & x_{272} & x_{232} & x_{261} \\ x_{221} & x_{154} & x_{114} & x_{143} \\ x_{172} & x_{132} & x_{161} & x_{121} \end{bmatrix}, <X_4>=\begin{bmatrix} x_{444} & x_{473} & x_{433} & x_{462} \\ x_{422} & x_{451} & x_{411} & x_{344} \\ x_{373} & x_{333} & x_{362} & x_{322} \\ x_{351} & x_{311} & x_{244} & x_{273} \\ x_{233} & x_{262} & x_{222} & x_{251} \\ x_{211} & x_{144} & x_{173} & x_{133} \\ x_{162} & x_{122} & x_{151} & x_{111} \end{bmatrix} \tag{3}$$

Now let us discuss the process of decomposition, which is a reverse process to that of interlacing. Consider the matrices y_i, i = 1 to 4 given by

$$y_i = [y_{ijk}],\ j = 1 \text{ to } 7,\ k = 1 \text{ to } 4. \tag{4}$$

Here i is the number of the matrix, j, the row number and k is the column number.
Let us consider the matrices y_i, i = 1 to 4, given by

$$y_1=\begin{bmatrix} y_{111} & y_{112} & y_{113} & y_{114} \\ y_{121} & y_{122} & y_{123} & y_{124} \\ y_{131} & y_{132} & y_{133} & y_{134} \\ y_{141} & y_{142} & y_{143} & y_{144} \\ y_{151} & y_{152} & y_{153} & y_{154} \\ y_{161} & y_{162} & y_{163} & y_{164} \\ y_{171} & y_{172} & y_{173} & y_{174} \end{bmatrix}, y_2=\begin{bmatrix} y_{211} & y_{212} & y_{213} & y_{214} \\ y_{221} & y_{222} & y_{223} & y_{224} \\ y_{231} & y_{232} & y_{233} & y_{234} \\ y_{241} & y_{242} & y_{243} & y_{244} \\ y_{251} & y_{252} & y_{253} & y_{254} \\ y_{261} & y_{262} & y_{263} & y_{264} \\ y_{271} & y_{272} & y_{273} & y_{374} \end{bmatrix}, y_3=\begin{bmatrix} y_{311} & y_{312} & y_{313} & y_{314} \\ y_{321} & y_{322} & y_{323} & y_{324} \\ y_{331} & y_{332} & y_{333} & y_{334} \\ y_{341} & y_{342} & y_{343} & y_{344} \\ y_{351} & y_{352} & y_{353} & y_{354} \\ y_{361} & y_{362} & y_{363} & y_{364} \\ y_{371} & y_{372} & y_{373} & y_{374} \end{bmatrix}, y_4=\begin{bmatrix} y_{411} & y_{412} & y_{413} & y_{414} \\ y_{421} & y_{422} & y_{423} & y_{424} \\ y_{431} & y_{432} & y_{433} & y_{434} \\ y_{441} & y_{442} & y_{443} & y_{444} \\ y_{451} & y_{452} & y_{453} & y_{454} \\ y_{461} & y_{462} & y_{463} & y_{464} \\ y_{471} & y_{472} & y_{473} & y_{474} \end{bmatrix}, \tag{5}$$

Let $y_i = <x_i>$, i = 1 to 4. Thus

$$\begin{bmatrix} y_{111} & y_{112} & y_{113} & y_{114} \\ y_{121} & y_{122} & y_{123} & y_{124} \\ y_{131} & y132 & y_{133} & y_{134} \\ y_{141} & y_{142} & y_{143} & y_{144} \\ y_{151} & y_{152} & y_{153} & y_{154} \\ y_{161} & y_{162} & y_{163} & y_{164} \\ y_{171} & y_{172} & y_{173} & y_{174} \end{bmatrix}=\begin{bmatrix} x_{474} & x_{434} & x_{463} & x_{423} \\ x_{452} & x_{412} & x_{441} & x_{374} \\ x_{334} & x_{363} & x_{323} & x_{352} \\ x_{312} & x_{341} & x_{274} & x_{234} \\ x_{263} & x_{223} & x_{252} & x_{212} \\ x_{241} & x_{174} & x_{134} & x_{163} \\ x_{123} & x_{152} & x_{112} & x_{141} \end{bmatrix}, \begin{bmatrix} y_{211} & y_{212} & y_{213} & y_{214} \\ y_{221} & y_{222} & y_{223} & y_{224} \\ y_{231} & y_{232} & y_{233} & y_{234} \\ y_{241} & y_{242} & y_{243} & y_{244} \\ y_{251} & y_{252} & y_{253} & y_{254} \\ y_{261} & y_{262} & y_{263} & y_{264} \\ y_{271} & y_{272} & y_{273} & y_{274} \end{bmatrix}=\begin{bmatrix} x_{464} & x_{424} & x_{453} & x_{214} \\ x_{442} & x_{471} & x_{431} & x_{364} \\ x_{324} & x_{353} & x_{313} & x_{342} \\ x_{371} & x_{331} & x_{264} & x_{224} \\ x_{253} & x_{213} & x_{242} & x_{271} \\ x_{231} & x_{164} & x_{124} & x_{153} \\ x_{113} & x_{142} & x_{171} & x_{131} \end{bmatrix},$$

$$\begin{bmatrix} y_{311} & y_{312} & y_{313} & y_{314} \\ y_{321} & y_{322} & y_{323} & y_{324} \\ y_{331} & y_{332} & y_{333} & y_{334} \\ y_{341} & y_{342} & y_{343} & y_{344} \\ y_{351} & y_{352} & y_{353} & y_{354} \\ y_{361} & y_{362} & y_{363} & y_{364} \\ y_{371} & y_{372} & y_{373} & y_{374} \end{bmatrix}=\begin{bmatrix} x_{454} & x_{414} & x_{443} & x_{472} \\ x_{432} & x_{461} & x_{421} & x_{354} \\ x_{314} & x_{343} & x_{372} & x_{332} \\ x_{361} & x_{321} & x_{254} & x_{214} \\ x_{243} & x_{272} & x_{232} & x_{261} \\ x_{221} & x_{154} & x_{114} & x_{143} \\ x_{172} & x_{132} & x_{161} & x_{121} \end{bmatrix}, \begin{bmatrix} y_{414} & y_{412} & y_{413} & y_{414} \\ y_{421} & y_{422} & y_{423} & y_{424} \\ y_{431} & y_{432} & y_{433} & y_{434} \\ y_{441} & y_{442} & y_{443} & y_{444} \\ y_{451} & y_{452} & y_{453} & y_{454} \\ y_{461} & y_{462} & y_{463} & y_{464} \\ y_{471} & y_{472} & y_{473} & y_{474} \end{bmatrix}=\begin{bmatrix} x_{444} & x_{473} & x_{433} & x_{462} \\ x_{422} & x_{451} & x_{411} & x_{344} \\ x_{373} & x_{333} & x_{362} & x_{322} \\ x_{351} & x_{311} & x_{244} & x_{273} \\ x_{233} & x_{262} & x_{222} & x_{251} \\ x_{211} & x_{144} & x_{173} & x_{133} \\ x_{162} & x_{122} & x_{151} & x_{111} \end{bmatrix} \tag{6}$$

We know that $x_i = [x_{ijk}]$. On using the relations (6), we get

$$X_1 = \begin{bmatrix} x_{111} & x_{112} & x_{113} & x_{114} \\ x_{121} & x_{122} & x_{123} & x_{124} \\ x_{131} & x_{132} & x_{133} & x_{134} \\ x_{141} & x_{142} & x_{143} & x_{144} \\ x_{151} & x_{152} & x_{153} & x_{154} \\ x_{161} & x_{162} & x_{163} & x_{164} \\ x_{171} & x_{172} & x_{173} & x_{174} \end{bmatrix} = \begin{bmatrix} y_{474} & y_{173} & y_{271} & y_{363} \\ y_{374} & y_{472} & y_{171} & y_{263} \\ y_{274} & y_{372} & y_{464} & y_{163} \\ y_{174} & y_{272} & y_{364} & y_{462} \\ y_{473} & y_{172} & y_{246} & y_{362} \\ y_{373} & y_{471} & y_{164} & y_{262} \\ y_{273} & y_{371} & y_{463} & y_{162} \end{bmatrix}, X_2 = \begin{bmatrix} x_{211} & x_{212} & x_{213} & x_{214} \\ x_{221} & x_{222} & x_{223} & x_{224} \\ x_{231} & x_{232} & x_{233} & x_{234} \\ x_{241} & x_{242} & x_{243} & x_{244} \\ x_{251} & x_{252} & x_{253} & x_{254} \\ x_{261} & x_{262} & x_{263} & x_{264} \\ x_{271} & x_{272} & x_{273} & x_{274} \end{bmatrix} = \begin{bmatrix} y_{461} & y_{154} & y_{252} & y_{344} \\ y_{361} & y_{453} & y_{152} & y_{244} \\ y_{261} & y_{353} & y_{451} & y_{144} \\ y_{161} & y_{253} & y_{351} & y_{443} \\ y_{454} & y_{153} & y_{251} & y_{343} \\ y_{354} & y_{452} & y_{151} & y_{243} \\ y_{255} & y_{352} & y_{444} & y_{143} \end{bmatrix},$$

$$X_3 = \begin{bmatrix} x_{311} & x_{312} & x_{313} & x_{314} \\ x_{321} & x_{322} & x_{323} & x_{324} \\ x_{331} & x_{332} & x_{333} & x_{334} \\ x_{341} & x_{342} & x_{343} & x_{344} \\ x_{351} & x_{352} & x_{353} & x_{354} \\ x_{361} & x_{362} & x_{363} & x_{364} \\ x_{371} & x_{372} & x_{373} & x_{374} \end{bmatrix} = \begin{bmatrix} y_{442} & y_{141} & y_{223} & y_{331} \\ y_{342} & y_{434} & y_{133} & y_{231} \\ y_{242} & y_{334} & y_{432} & y_{131} \\ y_{142} & y_{234} & y_{332} & y_{424} \\ y_{441} & y_{134} & y_{232} & y_{324} \\ y_{341} & y_{433} & y_{132} & y_{224} \\ y_{241} & y_{333} & y_{431} & y_{124} \end{bmatrix}, X_4 = \begin{bmatrix} x_{444} & x_{473} & x_{433} & x_{462} \\ x_{422} & x_{451} & x_{411} & x_{344} \\ x_{373} & x_{333} & x_{362} & x_{322} \\ x_{351} & x_{311} & x_{244} & x_{273} \\ x_{233} & x_{262} & x_{222} & x_{251} \\ x_{211} & x_{144} & x_{173} & x_{133} \\ x_{162} & x_{122} & x_{151} & x_{111} \end{bmatrix} = \begin{bmatrix} y_{423} & y_{122} & y_{214} & y_{312} \\ y_{323} & y_{421} & y_{114} & y_{212} \\ y_{223} & y_{321} & y_{413} & y_{112} \\ y_{123} & y_{221} & y_{313} & y_{411} \\ y_{422} & y_{121} & y_{213} & y_{311} \\ y_{322} & y_{414} & y_{113} & y_{211} \\ y_{222} & y_{314} & y_{412} & y_{111} \end{bmatrix}. \quad (7)$$

Thus we have $x_i = >y_i<$, where $> <$ denotes decomposition.

Development of the cipher: Let us consider a block of a plaintext consisting of 16 characters. By using the ASCII code, each character can be represented in terms of seven binary bits. Then the block comprising 112 binary bits is represented as four matrices, wherein each matrix is of size 7×4. In these matrices, the first column of the first matrix contains the seven binary bits corresponding to the first character of the plaintext; the second column of the matrix contains the binary bits corresponding to the second character and so on.

Let us take a key containing twenty-eight numbers, wherein each number lies between 0 and 127. Thus each number can be represented in the form of seven binary bits. Then we can have four matrices each of size 7×7, formed from the given key. Let us denote the key matrices by K_i, I = 1 to 4 and the plaintext matrices by P_i, i = 1 to 4.

Before we proceed to the process of iteration, let P_i^0 ($P_i^0 = P^0$), i = 1 to 4, be the initial (given) plaintext matrices. In the process of encryption, after the first iteration, on multiplying P_i^0 by K_i, we get

$$Q^1_i = K_i P^0_i \bmod 2, \; i = 1 \text{ to } 4, \quad (8)$$

where each one of the Q^1_i s is a matrix (consisting of binary bits) of size 7×4.

On adopting the process of interlacing, we get

$$P^1_i = <Q^1_i>, \; i = 1 \text{ to } 4. \quad (9)$$

On performing the second iteration and interlacing we have

$$Q^2_i = K_i P^1_i \bmod 2, \; i = 1 \text{ to } 4, \quad (10)$$

and

$$P^2_i = <Q^2_i>. \quad (11)$$

Thus the process of encryption, which includes iteration and interlacing, can in general be written as follows.

$$Q^j_i = K_i P^{j-1}_i \bmod 2, \quad (12)$$

$$\text{and } P^j_i = <Q^j_i>, \quad (13)$$

where i = 1 to 4 and j = 1 to m, in which m denotes the number of iterations.

$$\text{Let } C_i = P^m_i, \; i = 1 \text{ to } 4. \quad (14)$$

Let us now concatenate the elements of the four matrices of C_i in a column wise manner as follows.

$$\begin{matrix} C_{111} & C_{121} & \cdots & C_{171} & C_{112} & C_{122} & \cdots & C_{172} & C_{113} & C_{123} & \cdots & C_{173} & C_{114} & C_{124} & \cdots & C_{174} \\ C_{211} & C_{221} & \cdots & C_{271} & C_{212} & C_{222} & \cdots & C_{272} & C_{213} & C_{223} & \cdots & C_{273} & C_{214} & C_{224} & \cdots & C_{274} \\ C_{311} & C_{321} & \cdots & C_{371} & C_{312} & C_{322} & \cdots & C_{372} & C_{313} & C_{323} & \cdots & C_{373} & C_{314} & C_{324} & \cdots & C_{374} \\ C_{411} & C_{421} & \cdots & C_{471} & C_{412} & C_{422} & \cdots & C_{472} & C_{413} & C_{423} & \cdots & C_{473} & C_{414} & C_{424} & \cdots & C_{474} \end{matrix} \quad (15)$$

The above string of binary bits is the ciphertext C corresponding to the given plaintext P. Now let us consider the process of decryption. This depends upon iteration and decomposition (a procedure opposite to that of interlacing) is carried out by reversing all the above steps, one after another, starting from the last step. Consider the ciphertext C. Divide this into four matrices, namely, C_i, i = 1 to 4 (each matrix is of size 7×4), by placing the first twenty-eight elements of (15) in the first matrix, the second twenty-eight elements of (15) in the second matrix and so on. The matrices assume the form given by

$$C_i = [C_{irs}],\ i = 1 \text{ to } 4,\ r = 1 \text{ to } 7,\ s = 1 \text{ to } 4. \quad (16)$$

We may now write

$$Q^m_i = >C_i<=> P^m_i<. \quad (17)$$

On obtaining the modular arithmetic inverse (Sastry and Janaki, 2005) of each K_i, denoted by K^{-1}_i, i = 1 to 4 and using the Eq. (12), we get

$$P^{m-1}_i = K_i^{-1}\, Q^m_i \bmod 2 \quad (18)$$
for j = m.

It may be noted that $K_i\ K_i^{-1} \bmod 2 = K_i\, K_i^{-1} \bmod 2 = I$. Now the process of iteration governing decryption, which involves the decomposition procedure, can be written as follows.

$$Q^j_i = > P^j_i<, \quad (19)$$

and

$$P^{j-1}_i = K_i^{-1}\, Q^{j-1}_i \bmod 2, \quad (20)$$

where i = 1 to 4 and j = m to 1.
At the end of the iteration, we get the plaintext P^0_i.

Let us now design algorithms for the encryption and the decryption and write a procedure for obtaining the modular arithmetic inverse of the key matrix.

Algorithms

Algorithm for encryption:

{
1. for i =1 to 4 read P^0_i and K_i
2. for j = 1 to m
{
3. for i = 1 to 4 $Q^j_i = K_i\, P^{j-1}_i \bmod 2$
4. Interlace Q^j_i, i = 1 to 4
5. for i = 1 to 4 $P^j_i = <Q^j_i>$
}
6. Find C by concatenating P^m_i.
7. Write C.
}

Algorithm for decryption:

{
1. Read C
2. Divide C into 4 sub strings and obtain P^m_i for i = 1 to 4.
3. for i =1 to 4
{
Read K_i
Find K^{-1}_i
}
4. for j = m to 1
{
5. Decompose P^j_i, i =1 to 4
For i = 1 to 4 $Q^j_i = > P^j_i <$
6. for i =1 to 4 $P^j_I = K^{-1}_i Q^j_i \bmod 2$
}
7. for i =1 to 4 write P^0_i.
}

Algorithm for the modular arithmetic inverse:

{
1. Let n = 4.
2. for i = 1 to n
{
Read K_i
Find K^{-1}_i by calling the procedure for the modular arithmetic inverse
}

3. Procedure for the modular arithmetic inverse
{
I. Let A = K.
ii. Find the inverse of A by using the Gauss-Jordan elimination method.
iii. The inverse is given by $A^{-1} = [A_{ji}]/\Delta$ i =1 to n, j = 1 to n,

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

iii. for i = 1 to n
{
if ((iΔ) mod N = 1) d = i;
break;
}
B = [dA_{ji}] mod N. // B is the modular arithmetic inverse of A.
}
}

Here it is to be noted that the modular arithmetic inverse 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 A such that AB mod 2 = BA mod 2 = I.

Illustration of the cipher: Let us take a key K_0 in the form

$$K_0 = \{79, 65, 98, 37, 55, 119, 123, 29, 79, 94, 86, 55, 69, 125, 59, 91, 43, 86, 35, 69, 25, 39, 19, 23, 86, 95, 49, 75\} \quad (21)$$

This key consists of 28 numbers, wherein each number lies between 0 and 127. Here, repetition of the numbers is allowed. Let us divide this key into four sub-keys, wherein each sub-key consists of 7 numbers. We form the first sub-key K_1 by taking the first seven numbers of (21) and the second sub-key K_2 by taking the second seven numbers and so on till we exhaust all the 28 numbers.

On writing each number in terms of binary bits, the first sub-key can be written in the form of a matrix of size 7×7. Similarly, we can write the other sub-keys also in terms of matrices of size 7×7. Thus we have four matrices, K_i, i = 1 to 4, given by

$$K_1 = \begin{bmatrix} 1&0&0&1&1&1&1\\ 1&0&0&0&0&0&1\\ 1&1&0&0&0&1&0\\ 0&1&0&0&1&0&1\\ 0&1&1&0&1&1&1\\ 1&1&1&0&1&1&1\\ 1&1&1&1&0&1&1 \end{bmatrix}, K_2 = \begin{bmatrix} 0&0&1&1&1&0&1\\ 1&0&0&1&1&1&1\\ 1&0&1&1&1&1&0\\ 1&0&1&0&1&1&0\\ 0&1&1&0&1&1&1\\ 1&0&0&0&1&0&1\\ 1&1&1&1&1&0&1 \end{bmatrix}, K_3 = \begin{bmatrix} 0&1&1&1&0&1&1\\ 1&0&1&1&0&1&1\\ 0&1&0&1&0&1&1\\ 1&0&1&0&1&1&0\\ 0&1&0&0&0&1&1\\ 1&0&0&0&1&0&1\\ 0&0&1&1&0&0&1 \end{bmatrix}, K_4 = \begin{bmatrix} 0&1&0&0&1&1&1\\ 0&0&1&0&0&1&1\\ 0&0&1&0&1&1&1\\ 1&0&1&0&1&1&0\\ 1&0&1&1&1&1&1\\ 0&1&1&0&0&0&1\\ 1&0&0&1&0&1&1 \end{bmatrix} \quad (22)$$

Consider the plaintext: All the enemies are killed, no worry for the country. (23)

Let us now take the first sixteen characters of the plaintext namely, All ␣ the ␣ enemies ␣ into consideration. This includes three blank spaces.

On using the ASCII code, the above sixteen characters can be represented as four matrices each of size 7x4. Here P^0_1 includes the first four characters of the plaintext, wherein the first column represents the ASCII code of the first character in its binary form, the second column represents the ASCII code of the second character in its binary form and so on. In a similar manner P^0_2 P^0_3 and P^0_4 are formed. The four matrices are given by

$$P^0_1 = \begin{bmatrix} 1&1&1&0\\ 0&1&1&0\\ 0&0&0&0\\ 0&1&1&1\\ 0&1&1&0\\ 0&0&0&0\\ 1&0&0&0 \end{bmatrix}, P^0_2 = \begin{bmatrix} 1&1&1&0\\ 1&0&1&0\\ 1&0&0&0\\ 0&1&0&1\\ 1&0&1&0\\ 0&0&0&0\\ 0&0&1&0 \end{bmatrix}, P^0_3 = \begin{bmatrix} 1&1&1&1\\ 1&1&1&1\\ 0&0&0&0\\ 0&1&0&1\\ 1&1&1&1\\ 0&1&0&0\\ 1&0&1&1 \end{bmatrix}, P^0_4 = \begin{bmatrix} 1&1&1&0\\ 1&1&1&0\\ 0&0&1&0\\ 1&0&0&1\\ 0&1&0&0\\ 0&0&1&0\\ 1&1&1&0 \end{bmatrix} \quad (24)$$

On applying the encryption algorithm described earlier, taking m = 16 and carrying out sixteen iterations, we get the ciphertext given by

$$11000101010110010100100111010101111110010100111110000111110100101001111010100110111000111000011111101111101101 0. \quad (25)$$

On adopting the procedure for obtaining the modular arithmetic inverse
we get

$$K_1^{-1} = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \end{bmatrix}, K_2^{-1} = \begin{bmatrix} 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}, K_3^{-1} = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 \end{bmatrix}, K_4^{-1} = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 \end{bmatrix} \quad (26)$$

We can readily find that $K_i K_i^{-1} \bmod 2 = K^{-1}_i K_i \bmod 2 = I$.

On using the decryption algorithm presented earlier
we get back the plaintext All ৬ the ৬ enemies ৬.

On applying the encryption algorithm for the entire plaintext given by (23), we get the corresponding ciphertext as

11000101010110010100100111010101111111010101001111100001111101001010011110101001101110001110000111111011111101101011111101001001011110001110011101100111111100000110111110000000001110101010101101100111000000100000011101100000100011001010100101101010001000111001001100110010110011010100000010000000011000110100111010110110010100110110100000101010000000100101100110010111000100111100110000100100000011010110110000000010111111010011010110110100010110011010.
(27)

Then by applying the decryption algorithm on (27), we get back the plaintext given by (23).

Cryptanalysis: The various cryptanalytic attacks available in the literature depend upon the facts that the ciphertext is known or pairs of plaintext-ciphetrext are known or they are chosen in a special manner.

When the ciphetext only is known, the breaking of the cipher depends upon the size of the key space and this is carried out by brute force attack. When the pairs of plaintext and ciphertext are known, the cipher can be broken if the key can be determined.

In what follows, we examine the brute force attack and the known plaintext attack, wherein we show that the brute force attack is formidable and the known plaintext attack leads to a system of nonlinear equations from which the key cannot be determined.

Brute force attack: In this cipher, the key K_0 consists of twenty-eight numbers, given by (21), wherein each number lies between 0 and 127. Thus the key is represented in terms of 196 bits (four matrices, each of size 7×7). Thus the search space of the key under consideration is of size

$$2^{196} = (2^{10})^{19.6} \approx (10^3)^{19.6} \approx 10^{59}. \Rightarrow x^{196} = (2^{10})1^{9.6} \approx (10^3)^{19.6} \approx 10^{59}$$

Hence, the cipher cannot be broken by brute force attack.

Known plaintext attack: In the process of encryption, from (12), we have

$$Q^j_i = K_i P^{j-i}_i \bmod 2, \quad (28)$$

and

$$P^j_i = Q^j_i \quad (29)$$

When i = 1 and j = 1, we have

$$Q^1_1 = K_1 P^0_1 \bmod 2 = [K_{1rs}] [P^0_{1st}] \bmod 2 = [K_{1rs} P^0_{1st}] \bmod 2 \quad (30)$$

where r = 1 to 7, s = 1 to 7 and t = 1 to 4.

Here, it is to be noted that the expression $K_{1rs} P^0_{1st}$ represents the summation given by

$$\sum_{s=1}^{7} K_{Irs} P^{0}_{1st} \tag{31}$$

Similarly, we can write Q^1_i, i = 2 to 4.

Thus on interlacing the four matrices Q^1_i, i = 1 to 4, we get

$$P^1_1 = <Q^1_1> = \begin{bmatrix} K_{47s}P^0_{4s4} & K_{43s}P^0_{4s4} & K_{46s}P^0_{4s3} & K_{42s}P^0_{4s3} \\ K_{45s}P^0_{4s2} & K_{41s}P^0_{4s2} & K_{44s}P^0_{4s1} & K_{37s}P^0_{3s4} \\ K_{33s}P^0_{3s4} & K_{36s}P^0_{3s3} & K_{32s}P^0_{3s3} & K_{35s}P^0_{3s2} \\ K_{31s}P^0_{3s2} & K_{34s}P^0_{3s1} & K_{27s}P^0_{2s4} & K_{23s}P^0_{2s4} \\ K_{26s}P^0_{2s3} & K_{22s}P^0_{2s3} & K_{25s}P^0_{2s2} & K_{21s}P^0_{2s2} \\ K_{24s}P^0_{2s1} & K_{17s}P^0_{1s4} & K_{13s}P^0_{1s4} & K_{16s}P^0_{1s3} \\ K_{12s}P^0_{1s3} & K_{15s}P^0_{1s2} & K_{11s}P^0_{1s2} & K_{14s}P^0_{1s1} \end{bmatrix}, P^1_2 = <Q^1_2> = \begin{bmatrix} K_{46s}P^0_{4s4} & K_{42s}P^0_{4s4} & K_{45s}P^0_{4s3} & K_{41s}P^0_{4s3} \\ K_{44s}P^0_{4s2} & K_{47s}P^0_{4s1} & K_{43s}P^0_{4s1} & K_{36s}P^0_{3s4} \\ K_{32s}P^0_{3s4} & K_{35s}P^0_{3s3} & K_{31s}P^0_{3s3} & K_{34s}P^0_{3s2} \\ K_{37s}P^0_{3s1} & K_{33s}P^0_{3s1} & K_{26s}P^0_{2s4} & K_{22s}P^0_{2s4} \\ K_{25s}P^0_{2s3} & K_{21s}P^0_{2s3} & K_{24s}P^0_{2s2} & K_{27s}P^0_{2s1} \\ K_{23s}P^0_{2s1} & K_{16s}P^0_{1s4} & K_{12s}P^0_{1s4} & K_{15s}P^0_{1s3} \\ K_{11s}P^0_{1s3} & K_{14s}P^0_{1s2} & K_{17s}P^0_{1s1} & K_{13s}P^0_{1s1} \end{bmatrix},$$

$$P^1_3 = <Q^1_3> = \begin{bmatrix} K_{45s}P^0_{4s4} & K_{41s}P^0_{4s4} & K_{44s}P^0_{4s3} & K_{47s}P^0_{4s2} \\ K_{43s}P^0_{4s2} & K_{46s}P^0_{4s1} & K_{42s}P^0_{4s1} & K_{35s}P^0_{3s4} \\ K_{31s}P^0_{3s4} & K_{34s}P^0_{3s3} & K_{37s}P^0_{3s2} & K_{33s}P^0_{3s2} \\ K_{36s}P^0_{3s1} & K_{32s}P^0_{3s1} & K_{25s}P^0_{2s4} & K_{21s}P^0_{2s4} \\ K_{24s}P^0_{2s3} & K_{27s}P^0_{2s2} & K_{23s}P^0_{2s2} & K_{26s}P^0_{2s1} \\ K_{22s}P^0_{2s1} & K_{15s}P^0_{1s4} & K_{11s}P^0_{1s4} & K_{14s}P^0_{1s3} \\ K_{17s}P^0_{1s2} & K_{13s}P^0_{1s2} & K_{16s}P^0_{1s1} & K_{12s}P^0_{1s1} \end{bmatrix}, P^1_4 = <Q^1_4> = \begin{bmatrix} K_{44s}P^0_{4s4} & K_{47s}P^0_{4s3} & K_{43s}P^0_{4s3} & K_{46s}P^0_{4s2} \\ K_{42s}P^0_{4s2} & K_{45s}P^0_{4s1} & K_{41s}P^0_{4s1} & K_{34s}P^0_{3s4} \\ K_{37s}P^0_{3s3} & K_{33s}P^0_{3s3} & K_{36s}P^0_{3s2} & K_{32s}P^0_{3s2} \\ K_{35s}P^0_{3s1} & K_{31s}P^0_{3s1} & K_{24s}P^0_{2s4} & K_{27s}P^0_{2s3} \\ K_{23s}P^0_{2s3} & K_{26s}P^0_{2s2} & K_{22s}P^0_{2s2} & K_{25s}P^0_{2s1} \\ K_{21s}P^0_{2s1} & K_{14s}P^0_{1s4} & K_{17s}P^0_{1s3} & K_{13s}P^0_{1s3} \\ K_{16s}P^0_{1s2} & K_{12s}P^0_{1s2} & K_{15s}P^0_{1s1} & K_{11s}P^0_{1s1} \end{bmatrix}, \tag{32}$$

Fof j = 2, from (28) and (25) we have

$$Q^2_i = K_i P^1_i \bmod 2, \text{ i = 1 to 4.} \tag{33}$$

$$P^2_i = <Q^2_i> \tag{34}$$

$$\text{Let } D_i = K_i P^1_i \tag{35}$$

On applying the process of interlacing on the matrices D_i, i = 1 to 4, we have

$$<D_1> = \begin{bmatrix} D_{474} & D_{434} & D_{463} & D_{423} \\ D_{452} & D_{412} & D_{441} & D_{374} \\ D_{334} & D_{363} & D_{323} & D_{352} \\ D_{312} & D_{341} & D_{274} & D_{234} \\ D_{263} & D_{223} & D_{252} & D_{212} \\ D_{241} & D_{174} & D_{134} & D_{163} \\ D_{123} & D_{152} & D_{112} & D_{141} \end{bmatrix}, <D_2> = \begin{bmatrix} D_{464} & D_{424} & D_{453} & D_{413} \\ D_{442} & D_{471} & D_{431} & D_{364} \\ D_{324} & D_{353} & D_{313} & D_{342} \\ D_{371} & D_{331} & D_{264} & D_{224} \\ D_{253} & D_{213} & D_{242} & D_{271} \\ D_{231} & D_{164} & D_{124} & D_{153} \\ D_{113} & D_{142} & D_{171} & D_{131} \end{bmatrix},$$

$$<D_3> = \begin{bmatrix} D_{454} & D_{414} & D_{443} & D_{472} \\ D_{432} & D_{461} & D_{421} & D_{354} \\ D_{314} & D_{343} & D_{372} & D_{332} \\ D_{361} & D_{321} & D_{254} & D_{214} \\ D_{243} & D_{272} & D_{232} & D_{261} \\ D_{221} & D_{154} & D_{114} & D_{143} \\ D_{172} & D_{132} & D_{161} & D_{121} \end{bmatrix}, <D_4> = \begin{bmatrix} D_{444} & D_{473} & D_{433} & D_{462} \\ D_{422} & D_{451} & D_{411} & D_{344} \\ D_{373} & D_{333} & D_{362} & D_{322} \\ D_{351} & D_{311} & D_{244} & D_{273} \\ D_{233} & D_{262} & D_{222} & D_{251} \\ D_{211} & D_{144} & D_{173} & D_{133} \\ D_{162} & D_{122} & D_{151} & D_{111} \end{bmatrix}, \tag{36}$$

The elements of the above matrices are given by the equations

$$\left.\begin{aligned}
D_{1u1} &= K_{1u1}K_{47s}P^0_{4S4} + K_{1u2}K_{45s}P^0_{4S2} + K_{1u3}K_{33s}P^0_{3S4} + K_{1u4}K_{31s}P^0_{3S2} + K_{1u5}K_{26s}P^0_{2S3} \\
&\quad + K_{1u6}K_{24s}P^0_{2S1} + K_{1u7}K_{12s}P^0_{1S3}, && u = 1 \text{ to } 7 \\
D_{1u2} &= K_{1u1}K_{43s}P^0_{4S4} + K_{1u2}K_{41s}P^0_{4S2} + K_{1u3}K_{36s}P^0_{3s3} + K_{1u4}K_{34s}P^0_{3S1} + K_{1u5}K_{22s}P^0_{2s3} \\
&\quad + K_{1u6}K_{17s}P^0_{1S4} + K_{1u7}K_{15s}P^0_{1s2} && u = 1 \text{to} 7 \\
D_{1u3} &= K_{1u1}K_{46s}P^0_{4S3} + K_{1u2}K_{44s}P^0_{4S1} + K_{1u3}K_{32s}P^0_{3s3} + K_{1u4}K_{27s}P^0_{2s4} + K_{1u5}K_{25s}P^0_{2s2} \\
&\quad + K_{1u6}K_{13s}P^0_{1S4} + K_{1u7}K_{11s}P^0_{1s2}, && u = 1 \text{ to } 7 \\
D_{1u4} &= K_{1u1}K_{42s}P^0_{4s3} + K_{1u2}K_{37s}P^0_{3s4} + K_{1u3}K_{35s}P^0_{3s2} + K_{1u4}K_{23s}P^0_{2s4} + K_{1u5}K_{21s}P^0_{2s2} \\
&\quad + K_{1u6}K_{16s}P^0_{1s3} + K_{1u7}K_{14s}P^0_{1s1} && u = 1 \text{ to } 7
\end{aligned}\right\}$$

$$\left.\begin{aligned}
D_{2u1} &= K_{2u1}K_{46s}P^0_{4s4} + K_{2u2}K_{44s}P^0_{4S2} + K_{2u3}K_{32s}P^0_{3s4} + K_{2u4}K_{37s}P^0_{3s1} + K_{2u5}K_{25s}P^0_{2s3} + K_{2u6}K_{23s}P^0_{2s1} + K_{2u7}K_{11s}P^0_{1s3}, && u = 1 \text{ to } 7 \\
D_{2u2} &= K_{2u1}K_{42s}P^0_{4s4} + K_{2u2}K_{47s}P^0_{4S1} + K_{2u3}K_{35s}P^0_{3s3} + K_{2u4}K_{33s}P^0_{3s1} + K_{2u5}K_{21s}P^0_{2s3} + K_{2u6}K_{16s}P^0_{1s4} + K_{2u7}K_{14s}P^0_{1s2}, && u = 1 \text{ to } 7 \\
D_{2u3} &= K_{2u1}K_{45s}P^0_{4s3} + K_{2u2}K_{43s}P^0_{4s1} + K_{2u3}K_{31s}P^0_{3s3} + K_{2u4}K_{26s}P^0_{2s4} + K_{2u5}K_{24s}P^0_{2s2} + K_{2u6}K_{12s}P^0_{1s4} + K_{2u7}K_{17s}P^0_{1s1}, && u = 1 \text{ to } 7 \\
D_{2u4} &= K_{2u1}K_{41s}P^0_{4s3} + K_{2u2}K_{36s}P^0_{3S4} + K_{2u3}K_{34s}P^0_{3s2} + K_{2u4}K_{22s}P^0_{2s4} + K_{2u5}K_{27s}P^0_{2s1} + K_{2u6}K_{15s}P^0_{1s3} + K_{2u7}K_{13s}P^0_{1s1}, && u = 1 \text{ to } 7 \\
D_{3u1} &= K_{3u1}K_{45s}P^0_{4s4} + K_{3u2}K_{43s}P^0_{4S2} + K_{3u3}K_{31s}P^0_{3s4} + K_{3u4}K_{36s}P^0_{3s1} + K_{3u5}K_{24s}P^0_{2s1} + K_{3u6}K_{22s}P^0_{2s1} + K_{3u7}K_{17s}P^0_{1s2}, && u = 1 \text{ to } 7 \\
D_{3u2} &= K_{3u1}K_{41s}P^0_{4s4} + K_{3u2}K_{46s}P^0_{4S1} + K_{3u3}K_{34s}P^0_{3s3} + K_{3u4}K_{32s}P^0_{3s1} + K_{3u5}K_{27s}P^0_{2s2} + K_{3u6}K_{15s}P^0_{1s4} + K_{3u7}K_{13s}P^0_{1s2}, && u = 1 \text{ to } 7 \\
D_{3u3} &= K_{3u1}K_{44s}P^0_{4s3} + K_{3u2}K_{42s}P^0_{4s1} + K_{3u3}K_{37s}P^0_{3s2} + K_{3u4}K_{25s}P^0_{2s4} + K_{3u5}K_{23s}P^0_{2s2} + K_{3u6}K_{1}{}_{1s}P^0_{1s4} + K_{3u7}K_{16s}P^0_{1s1}, && u = 1 \text{ to } 7 \\
D_{3u4} &= K_{3u1}K_{47s}P^0_{4s2} + K_{3u2}K_{35s}P^0_{3s4} + K_{3u3}K_{33s}P^0_{3s2} + K_{3u4}K_{21s}P^0_{2s4} + K_{3u5}K_{26s}P^0_{2s1} + K_{3u6}K_{14s}P^0_{1s3} + K_{3u7}K_{12s}P^0_{1s1}, && u = 1 \text{ to } 7 \\
D_{4u1} &= K_{4u1}K_{44s}P^0_{4s4} + K_{4u2}K_{42s}P^0_{4s2} + K_{4u3}K_{37s}P^0_{3s3} + K_{4u4}K_{35s}P^0_{3s1} + K_{4u5}K_{23s}P^0_{2s3} + K_{4u6}K_{21s}P^0_{2s1} + K_{4u7}K_{16s}P^0_{1s2}, && u = 1 \text{ to } 7 \\
D_{4u2} &= K_{4u1}K_{47s}P^0_{4s3} + K_{4u2}K_{45s}P^0_{4s1} + K_{4u3}K_{33s}P^0_{3s3} + K_{4u4}K_{31s}P^0_{3s1} + K_{4u5}K_{26s}P^0_{2s2} + K_{4u6}K_{14s}P^0_{1s4} + K_{4u7}K_{12s}P^0_{1s2}, && u = 1 \text{ to } 7 \\
D_{4u3} &= K_{4u1}K_{43s}P^0_{4s3} + K_{4u2}K_{41s}P^0_{4s1} + K_{4u3}K_{36s}P^0_{3s2} + K_{4u4}K_{24s}P^0_{2s4} + K_{4u5}K_{22s}P^0_{2s2} + K_{4u6}K_{17s}P^0_{1s3} + K_{4u7}K_{15s}P^0_{1s1}, && u = 1 \text{ to } 7 \\
D_{4u4} &= K_{4u1}K_{46s}P^0_{4s2} + K_{4u2}K_{34s}P^0_{3s4} + K_{4u3}K_{32s}P^0_{3s2} + K_{4u4}K_{27s}P^0_{2s3} + K_{4u5}K_{25s}P^0_{2s1} + K_{4u6}K_{13s}P^0_{1s3} + K_{4u7}K_{11s}P^0_{1s1}, && u = 1 \text{ to } 7
\end{aligned}\right\} \quad (37)$$

From the Eq. (33) to (35), we get

$$P^2_i = <D_i> \bmod 2. \quad (38)$$

If we take m = 2 and carryout only two iterations, we get 112 equations (since we have four matrices, each of size 7×4) connecting the elements of the plaintext (P^0_i) and the ciphertext (P^2_i). All these equations are of second degree in the elements of the key matrices and contain mod 2. On solving the system of equations, it must be possible for us to obtain the solution for the elements of the key matrices purely in terms of 0s and 1s. However, this is not possible by any approach, including the brute force attack, as there are 112 elements of the key in the four key matrices.

If we continue the process of iteration and assign a higher number for m, say m = 16, then we get 112 non-linear equations of degree 16. As it is totally impossible to solve such a system of 112 non-linear equations, breaking the cipher is completely ruled out, in this process, either by the known plaintext attack or by any special choice of ciphertext or plaintext. Thus the cipher cannot be broken by the known plaintext attack.

Avalanche effect: Taking the first sixteen characters of the plaintext namely, All ␣ the ␣ enemies ␣ (23), we have obtained the ciphertext given by (5.5). On changing the first character of the above plaintext from A to C (the ASCII codes of A and C in their binary form differ in one bit), we obtain the corresponding ciphertext as

01110111100111001100000110101010100111 1
11010110011011000101101101111110000110 1
00010001110011100001101101100000000. (39)

Comparing (25) and (39), we notice that the two ciphertexts differ in 63 bits out of 112 bits. This shows that the algorithm exhibits a strong avalanche effect.

Now we change the key in one bit. This is achieved by changing the number 91 to 90 in the key K_0 given by (5.1). Then we obtain the corresponding ciphertext for the plaintext -All ␣ the ␣ enemies ␣. This is given by

01101101011001101000010001100111100001 0
11010110110110100111011101101011111000
01001101110001100101001100010000000. (40)

On comparing (39) and (25), we readily notice that the ciphertexts differ in 62 bits out of 112 bits. It may be noted here that though the change in the key is only one bit out of 196 bits, the change in the corresponding ciphertext containing 112 bits is 62 bits. This also shows that the algorithm has a pronounced avalanche effect.

Computational experiments and conclusions: In this research, we have developed a block cipher for a block of size 112 bits. The length of the key is 196 bits and it is represented as four matrices, wherein each matrix is of size 7×7. The plaintext is represented by four matrices, wherein each one is of size 7×4. The development of the cipher essentially depends upon an iterative method involving interlacing and decomposition and the modular arithmetic inverse of each of the key matrices.

The algorithms for the encryption and the decryption, are implemented in C language.

From the cryptanalysis presented earlier, we have found that the cipher cannot be broken by any cryptanalytic attack.

Based on the analysis presented in this research, we have seen that the cipher exhibits a strong avalanche effect.

Keeping all the above aspects in view, we conclude that the cipher is a very interesting one and it cannot be broken by any cryptanalytic attack.

REFERENCES

Feistel, H., 1973. Cryptography and computer privacy. Scientific American, 228: 15-23.

Feistel, H., W. Notz. and J. Smith, 1975. Some cryptographic techniques for machine-to-machine data communication. Proceedings of the IEEE, 63: 1545-1554.

Sastry, V.U.K., V. Janaki, 2005. On the Modular Arithmetic Inverse in the Cryptology of Hill Cipher. Proceedings of North American Technology and Business Conference, September 2005, Montreal, Canada.

Stallings, W., 2002. Cryptography and Network Security: Principles and Practices. Chp. 3' 3rd Edn., Fourth Indian reprint, 2002, Pearson Prentice Hall), pp: 63.