Journal of Computer Science 2 (9): 698-703, 2006
ISSN 1549-3636

A Large Block Cipher Using Modular Arithmetic Inverse of a Key Matrix and Mixing of the Key Matrix and the Plaintext

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

Abstract: In this paper, we have developed a block cipher by applying an iterative method. In the process of encryption, we have used a key matrix (K) in which all the elements are binary bits. In the process of decryption, we have utilized the modular arithmetic inverse (K^{-1}). In the process of encryption, the elements of the plaintext and the elements of the key are thoroughly mixed so that the strength of the algorithm increases remarkably. In this we have obtained the ciphertext for large blocks of plaintext.

Key words: block cipher, ciphertext, plaintext, modular arithmetic inverse, security measures

INTRODUCTION

In the literature of cryptography, we find a number of block ciphers[1]. In the development of all the ciphers, the basic ideas involved are substitution, diffusion, permutation and mixing. In all these ciphers though the encryption and decryption processes are fully known to all, the secrecy of the key(s), on which the cipher mainly depends upon, does not allow any cryptanalytic attack.

The Hill cipher[1] is described by the equations $C = KP \bmod 26$ and $P = K^{-1}C \bmod 26$, where K is the key matrix, P the plaintext vector, C the ciphertext vector and K^{-1} is the modular arithmetic inverse of K. By using the known plaintext attack, this cipher could be broken by writing an equation of the form

$$Y = KX \bmod 26, \quad (1.1)$$

where X and Y are matrices containing plaintext vectors and the corresponding ciphertext vectors respectively. Here K (= $YX^{-1} \bmod 26$) could be obtained by determining X^{-1}, where X^{-1} is the modular arithmetic inverse of X. All this has happened as the plaintext matrix X is not thoroughly mixed with the key matrix K although diffusion is present.

In the present paper, our interest is to develop a cipher for a large block size. Following Feistel, we have developed a block cipher, wherein the key matrix and the plaintext vector are converted into binary bits and mod 2 operation is carried out to obtain the ciphertext. In this we have shown that a thorough mixing of the elements of the key matrix and the plaintext matrix will lead to a cipher, which cannot be broken by any cryptanalytic attack.

2. Development of the cipher: Consider a plaintext containing n characters. Let us represent each character as a number given by its ASCII code. Then each number is represented in its binary form. We now form a matrix of size n x 7, wherein each element of the matrix is a binary bit. Thus the plaintext assumes the form of a matrix given by

$$[P_{ij}],\ i = 1 \text{ to } n,\ j = 1 \text{ to } 7. \quad (2.1)$$

Let us now consider a key matrix K consisting of binary bits, whose size is n x n. Let us denote the ciphertext by C, where C is an n x 7 matrix. Thus we get the ciphertext C by using the relation

$$C = KP \bmod 2. \quad (2.2)$$

Here we introduce an iterative scheme in order to achieve a thorough mixing of the plaintext and the key, so that it enhances the strength of the cipher. Before we proceed to the iterative scheme in the process of encryption, we denote P and C by P^0 and C^0 respectively.

Hence, we rewrite (2.2) in the form

$$C^0 = KP^0 \bmod 2. \quad (2.3)$$

The iterative scheme under consideration is given by

$$P^i = C^{i-1} \oplus E_i, \quad (2.4)$$

$$C^i = KP^i \bmod 2, \quad (2.5)$$

where i takes the values 1 to n and E_i is the transpose of the matrix formed by taking the i^{th} row to the r^{th} row of the matrix K. Here

$$r = \begin{cases} (i+6) \text{ if } (i+6) \le n, \\ (i+6-n) \text{ otherwise.} \end{cases}$$

Further, we use the relations

$$D^0 = C^n, \quad (2.6)$$

$$Q^j = D^{j-1} \oplus F_j, \quad (2.7)$$

$$D^j = KQ^j \bmod 2, \quad (2.8)$$

where j takes the values 1 to n and F_j is the matrix formed by taking the j^{th} column to the s^{th} column of the matrix K. Here

$$s = \begin{cases} (j+6) \text{ if } (j+6) \le n, \\ (j+6-n) \text{ otherwise.} \end{cases}$$

Thus we get D^n, which may be denoted as C.

Now we take $C = D^n$. (2.9)

Corresponding Author: V.U.K.Sastry, SreeNidhi Institute of Science & Technology University, Hyderabad, India

On the whole, we have performed 2n iterations, in which the first 'n' are concerned to the elements of the rows of K and the other 'n' are related to the elements of the columns of K. The process of decryption is carried out by adopting the same procedure in the reverse order and this leads to the original plaintext. Here also, the number of iterations is 2n. In what follows, we design algorithms for encryption and decryption and also describe a method for obtaining the modular arithmetic inverse[2].

Algorithms

3.1 Algorithm for encryption

{
1. Read n, K and P^0
2. $C^0 = KP^0 \bmod 2$
3. for i =1 to n
{
$P^i = C^{i-1} \oplus E_i$
$C^i = KP^i \bmod 2$
}
4. $D^0 = C^n$
5. for j = 1 to n
{
$Q^j = D^{j-1} \oplus F_j$
$D^j = KQ^j \bmod 2$
}
6. $C = D^n$
7. Write C
}

3.2 Algorithm for decryption

{
1. Read n, K and C
2. Find the modular arithmetic inverse of K. Let it be denoted by K^{-1}.
3. $D^n = C$
4. for j = n to 1
{
$Q^j = K^{-1} D^j \bmod 2$
$D^{j-1} = Q^j \oplus F_j$
}
5. $C^n = D^0$
6. for i = n to 1
{
$P^i = K^{-1} C^i \bmod 2$
$C^{i-1} = P^i \oplus E_i$
}
7. $P^0 = K^{-1}C^0 \bmod 2$
}

3.3 Modular arithmetic inverse of a matrix

{
Find the determinant of A. Let it be denoted by Δ.
2. Find the inverse of A. The inverse is given by $A^{-1} = \frac{[A_{ji}]}{\Delta}$ 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.
for i = 1 to n,
{
if ((iΔ) mod N = 1) d = i;
break
}
4. B = [dA_{ji}] mod N. // B is the modular arithmetic inverse.
}

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 K such that $KK^{-1} \bmod 2 = K^{-1}K \bmod 2 = I$.

4. Illustration of the cipher: Let us consider the plaintext "Pay more money", which is consisting of 14 characters including the blank spaces. By using the ASCII code, we represent each character of the plaintext in terms of seven binary bits. Thus placing the binary bits of each character in a row, the plaintext matrix P is given by

$$P = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 1 \end{bmatrix} \quad (4.1)$$

Let us now consider a key K_0 comprising 28 numbers. This is given by

K_0 = [65, 71, 95, 121, 48, 31, 99, 81, 42, 19, 23, 41, 37, 19, 17, 67, 87, 105, 119, 13, 27, 31, 118, 117, 4, 110, 98, 35]. (4.2)

Here, we have selected these numbers such that each of them can be represented by a seven bit binary number, i.e. each number is at the most 127 and repetitions are allowed. We place the 28 numbers of the key in the form of a 14 x 2 matrix such that the first two numbers are in the first row, the next two numbers are in the second row and so on.

On converting these numbers into their binary form, we get a 14 x 14 matrix given by

$$K = \begin{bmatrix} 1&0&0&0&0&0&1&1&0&0&0&1&1&1 \\ 1&0&1&1&1&1&1&1&1&1&1&0&0&1 \\ 0&1&1&0&0&0&0&0&0&1&1&1&1&1 \\ 1&1&0&0&0&1&1&1&0&1&0&0&1&1 \\ 0&1&0&1&0&1&0&0&0&1&0&0&0&1 \\ 0&0&1&0&1&1&1&0&1&0&1&0&0&1 \\ 0&1&0&0&1&0&1&0&0&1&0&0&1&1 \\ 0&0&1&0&0&0&1&1&0&0&0&0&1&1 \\ 1&0&1&0&1&1&1&1&1&0&1&0&0&1 \\ 1&1&1&0&1&1&1&0&0&0&1&1&0&1 \\ 0&0&1&1&0&1&1&0&0&1&1&1&1&1 \\ 1&1&1&0&1&1&0&1&1&1&0&1&0&1 \\ 0&0&0&0&1&0&0&1&1&0&1&1&1&0 \\ 1&1&0&0&0&1&1&0&1&0&0&0&1&1 \end{bmatrix} \quad (4.3)$$

Then by adopting the algorithm given in section 3.3, we obtain the modular arithmetic inverse K^{-1}, satisfying the relations $KK^{-1} \bmod 2 = K^{-1}K \bmod 2 = I$, is given by

$$K^{-1} = \begin{bmatrix} 0&0&1&0&0&1&0&1&0&0&0&1&0&0 \\ 1&1&1&1&0&0&1&1&1&0&1&1&0&1 \\ 0&0&1&0&0&0&0&1&1&1&0&1&1&1 \\ 0&1&1&0&1&0&0&1&1&1&1&0&1&1 \\ 1&1&0&1&1&0&0&1&1&0&0&1&0&1 \\ 1&0&0&0&0&0&0&0&1&1&0&0&0&1 \\ 0&0&1&1&1&0&1&0&1&0&1&1&1&1 \\ 0&0&1&0&0&0&0&1&1&0&0&1&0&0 \\ 0&1&0&1&0&1&1&1&0&0&1&0&1&0 \\ 0&0&1&0&1&0&0&1&0&1&1&0&1&1 \\ 0&1&1&0&0&1&0&1&0&0&1&1&1&0 \\ 1&0&0&0&0&1&0&1&1&1&0&0&1&1 \\ 0&1&0&0&1&1&1&1&1&1&0&1&0&0 \\ 0&1&1&1&0&1&0&0&0&0&1&0&0&0 \end{bmatrix} \quad (4.4)$$

Here, it is to be noted that the modular arithmetic inverse (K^{-1}) exists only when the determinant of K is non-zero and it is relatively prime to 2. In this case, the value of the determinant is -85 and hence the above conditions are satisfied. On using the algorithm 3.1 for encryption, the ciphertext corresponding to the plaintext "Pay more money" can be obtained as

11010111001101100110111011101101001010000011010000110010100110010111101000010101111011110000110111. (4.5)

The receiver who has obtained the key from the sender uses the decryption algorithm and finds the original plaintext.

As the process of the encryption involving the iterative scheme contains equations, which mix the plaintext and the key very thoroughly, it can be anticipated that the cipher cannot be broken by any cryptanalytic attack. Now we discuss the cryptanalysis.

5. Cryptanalysis: The key matrix given by (4.2) contains 196 elements. Thus the size of the key space is $2^{196} \approx (2^{10})^{20} \approx 10^{60}$. This indicates very clearly that the brute force attack is not possible.

Let us now consider the known plaintext attack. In this case, we can have as many plaintext and ciphertext pairs as we require. However, we do not have a simple relation between the ciphertext and the plaintext as we have in the case of Hill cipher[2].

Now let us see the relation between P and C. From (2.3) to (2.5), we get

$C^0 = KP^0 \bmod 2$.

$P^1 = C^0 \oplus E_1$.

$C^1 = KP^1 \bmod 2 = K (KP^0 \bmod 2 \oplus E_1) \bmod 2 = K^2 P^0 \bmod 2 \oplus KE_1 \bmod 2$.

$P^2 = C^1 \oplus E_2$.

$C^2 = K P^2 \bmod 2 = K (K^2 P^0 \bmod 2 \oplus KE_1 \bmod 2 \oplus E_2) \bmod 2$

$= K^3 P^0 \bmod 2 \oplus K^2 E_1 \bmod 2 \oplus KE_2 \bmod 2$.

Similarly we obtain,

$C^{14} = K^{15} P^0 \bmod 2 \oplus K^{14} E_1 \bmod 2 \oplus K^{13} E_2 \bmod 2 \oplus K^{12} E_3 \bmod 2 \oplus K^{11} E_4 \bmod 2$
$\oplus K^{10} E_5 \bmod 2 \oplus K^9 E_6 \bmod 2 \oplus K^8 E_7 \bmod 2 \oplus K^7 E_8 \bmod 2 \oplus K^6 E_9 \bmod 2$
$\oplus K^5 E_{10} \bmod 2 \oplus K^4 E_{11} \bmod 2 \oplus K^3 E_{12} \bmod 2 \oplus K^2 E_{13} \bmod 2$
$\oplus KE_{14} \bmod 2$. (5.1)

Now on using the relations (2.6) to (2.8) and (5.1), finally we get

$C = K^{29} P^0 \bmod 2 \oplus K^{28} E_1 \bmod 2 \oplus K^{27} E_2 \bmod 2 \oplus K^{26} E_3 \bmod 2$
$\oplus \ldots \oplus K^{16} E_{13} \bmod 2$
$\oplus K^{15} E_{14} \bmod 2$
$\oplus K^{14} F_1 \bmod 2$
$\oplus K^{13} F_2 \bmod 2$
$\oplus K^{12} F_3 \bmod 2$
$\oplus \ldots \oplus K^2 F_{13} \bmod 2 \oplus KF_{14} \bmod 2$. (5.2)

Let G be the ciphertext corresponding to the plaintext H^0, where H^0 is a matrix of size 14x7. Then we have

$G = K^{29} H^0 \bmod 2 \oplus K^{28} E_1 \bmod 2 \oplus K^{27} E_2 \bmod 2 \oplus K^{26} E_3 \bmod 2$
$\oplus \ldots \oplus K^{16} E_{13} \bmod 2 \oplus K^{15} E_{14} \bmod 2 \oplus K^{14} F_1 \bmod 2 \oplus K^{13} F_2 \bmod 2$
$\oplus K^{12} F_3 \bmod 2 \oplus \ldots \oplus K^2 F_{13} \bmod 2 \oplus KF_{14} \bmod 2$. (5.3)

On XORing (5.2) and (5.3), we get

$C \oplus G = K^{29} P^0 \bmod 2 \oplus K^{29} H^0 \bmod 2 = K^{29} (P^0 \oplus H^0) \bmod 2$. (5.4)

Here we readily notice that the rest of the terms in (5.2) and (5.3) cancel each other as they are the same in both the equations. Equation (5.4) can be written as

$S = K^{29} \varphi \bmod 2$, (5.5)

where $S = C \oplus G$ and $\varphi = P^0 \oplus H^0$.

Let U^0 and V^0 be two more plaintexts, represented in the form of matrices of size 14x7 and L and M be the two corresponding ciphertexts. Then on applying the above procedure, adopted on C and G, we get

$R = K^{29} \psi \bmod 2$, (5.6)

where $R = L \oplus M$ and $\psi = U^0 \oplus V^0$.

Now on combining equations (5.5) and (5.6) so that φ is the first seven columns of a 14x14 matrix (say

X) and ψ is the next seven columns of the same matrix, we get an equation of the form

$$Y = K^{29} X \bmod 2, \quad (5.7)$$

where X and Y are the related plaintext and the ciphertext matrices respectively.

From (5.7) we obtain,

$$X^{-1}Y \bmod 2 = (K^{29} (X^{-1}X \bmod 2)) \bmod 2.$$

Thus we get

$$X^{-1}Y \bmod 2 = K^{29} \bmod 2.$$

i.e. $$(K^{29} - X^{-1}Y) \bmod 2 = 0. \quad (5.8)$$

As this is a non-linear equation of degree 29 in K, it is not possible to obtain the key matrix K. Thus, the cipher cannot be broken in the case of known plaintext attack.

6. Cipher for larger block size: Let us consider the plaintext: Almighty saves the Universe. (6.1)

This consists of twenty-eight characters including three blank spaces and a full stop (period). As each character can be represented by its ASCII code, we have seven binary bits for each character. Thus we can represent the twenty-eight characters in terms of a 28 x 7 matrix such that each row contains seven binary bits corresponding to a character. The matrix corresponding to the plaintext under consideration is given by

$$P = \begin{bmatrix} 1&0&0&0&0&0&1\\ 1&1&0&1&1&0&0\\ 1&1&0&1&1&0&1\\ 1&1&0&1&0&0&1\\ 1&1&0&0&1&1&1\\ 1&1&0&1&0&0&0\\ 1&1&1&0&1&0&0\\ 1&1&1&1&0&0&1\\ 0&1&0&0&0&0&0\\ 1&1&1&0&0&1&1\\ 1&1&0&0&0&0&1\\ 1&1&1&0&1&1&0\\ 1&1&0&0&1&0&1\\ 1&1&1&0&0&1&1\\ 0&1&0&0&0&0&0\\ 1&1&1&0&1&0&0\\ 1&1&0&1&0&0&0\\ 1&1&0&0&1&0&1\\ 0&1&0&0&0&0&0\\ 1&0&1&0&1&0&1\\ 1&1&0&1&1&1&0\\ 1&1&0&1&0&0&1\\ 1&1&1&0&1&1&0\\ 1&1&0&0&1&0&1\\ 1&1&1&0&0&1&0\\ 1&1&1&0&0&1&1\\ 1&1&0&0&1&0&1\\ 0&1&0&1&1&1&0 \end{bmatrix}. \quad (6.2)$$

Let us form a key matrix of size 28 x 28. It can be represented in the form

$$K = \begin{bmatrix} Q & R \\ Y & Z \end{bmatrix}, \quad (6.3)$$

where Q, R, Y, Z are the matrices of size 14 x 14. In this Q is formed by taking a key, containing twenty-eight numbers as follows:

[65, 71, 95, 121, 48, 31, 99, 81, 122, 119, 23, 41, 37, 11, 114, 67, 87, 105, 117, 115, 127, 31, 118, 116, 124, 113, 98, 35]. (6.4)

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

$$K = \begin{bmatrix}
1&0&0&0&0&0&1&1&0&0&0&1&1&1&1&1&0&0&0&1&0&0&1&0&0&0&0&1&1\\
1&0&1&1&1&1&1&1&1&1&1&0&0&1&1&1&1&1&1&1&0&0&1&1&1&0&0&0&1\\
0&1&1&0&0&0&0&0&0&1&1&1&1&1&1&1&1&1&0&1&1&0&1&1&1&1&0&1&0&0\\
1&1&0&0&0&1&1&1&0&1&0&0&0&1&1&1&1&1&1&1&1&1&0&0&1&1&1&1&1&1\\
1&1&1&0&1&0&1&1&1&0&1&1&1&1&1&1&1&1&1&0&1&0&1&1&1&1&0&0&1&1\\
0&0&1&0&1&1&1&0&1&0&1&0&0&1&1&0&1&0&1&1&1&1&1&1&0&1&0&0&0&1\\
0&1&0&0&1&0&1&0&0&0&1&0&1&1&1&1&1&1&0&0&1&0&1&0&1&0&0&0&0&1&1\\
1&1&1&0&0&1&0&1&0&0&0&0&1&1&0&1&0&0&1&1&1&0&1&0&1&0&0&0&1&0&1\\
1&0&1&0&1&1&1&1&1&0&1&0&0&1&0&0&1&0&1&1&1&0&1&0&1&0&0&0&1&0&1\\
1&1&1&0&1&0&1&1&1&1&0&0&1&1&1&1&1&1&1&0&1&0&1&1&1&0&1&1&1&1\\
1&1&1&1&1&1&1&1&0&0&1&1&1&1&1&1&1&0&0&0&1&1&1&0&1&0&0&0&0&1\\
1&1&1&0&1&1&0&1&1&1&0&1&0&0&0&1&1&0&0&0&0&0&0&1&1&1&1&1&1&1\\
1&1&1&1&1&0&0&1&1&1&0&0&0&1&1&0&1&1&1&1&1&1&1&1&1&0&0&0&1&1\\
1&1&0&0&0&1&0&0&1&0&0&0&1&1&1&0&0&0&0&0&1&1&0&0&0&1&1&1&1&1\\
1&1&1&1&1&1&1&1&1&1&1&1&1&0&1&1&1&1&0&0&1&1&1&1&1&1&1&1&1&1\\
1&0&1&0&1&0&1&1&0&1&1&0&0&1&0&0&1&1&1&0&1&1&0&1&1&1&1&1&1&1\\
1&0&1&0&1&0&0&0&0&0&1&1&0&0&0&1&1&0&1&1&0&1&1&1&1&1&1&1&1&0\\
0&1&1&0&0&1&1&0&1&0&1&0&0&0&0&1&0&0&1&0&0&0&0&0&1&0&1&1&0&1\\
0&1&1&1&1&0&0&0&0&0&1&1&1&1&0&0&1&0&0&0&1&1&0&1&1&1&1&1&1&0\\
0&1&0&0&1&1&0&0&1&1&0&1&1&1&0&1&0&1&1&1&0&1&1&0&1&1&0&1&1&0\\
1&1&0&1&1&0&0&1&1&1&0&1&1&0&1&1&0&1&0&1&1&0&1&1&1&1&0&0&0&0\\
1&1&0&1&0&1&1&0&1&1&1&1&0&0&0&1&1&1&0&0&1&0&1&1&0&0&1&1&1&0\\
0&1&0&1&1&1&0&1&1&0&1&1&0&1&0&1&0&0&1&1&0&0&1&1&0&1&1&1&1&1\\
0&1&0&0&0&1&1&0&1&1&1&1&1&0&0&1&1&1&1&0&0&0&0&1&1&1&1&0&1&0\\
0&1&0&0&1&0&0&0&0&0&0&1&0&1&0&0&1&1&1&0&1&1&1&0&1&0&0&0&0&0\\
0&1&1&0&1&1&0&1&1&1&1&1&1&0&1&0&1&0&1&0&0&0&0&0&1&1&0&0&1&0\\
0&0&1&1&1&0&1&1&0&1&1&1&1&1&1&0&1&0&1&0&1&1&0&1&1&0&0&1&0&1\\
1&1&0&1&1&0&0&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&0&1&1&1&1
\end{bmatrix}. \quad (6.5)$$

Now on using the key matrix K given by (6.5) and the plaintext given by (6.2), we perform the encryption (see section 3.1) and obtain the ciphertext given below:

0001100110001110110110100010000111100111111011101111100000100100111010000010111110010100100010001010001101001011010001011010101101001111000110110111111101011010111100010110011100110111101001111110. (6.6)

As the determinant of K, denoted by Δ = 71576.967967 ≈ 71577, it is relatively prime to 2. Thus the modular arithmetic inverse of K can be obtained by applying the procedure given in section 3.3.

Hence, we have

$$K^{-1} = \begin{bmatrix}
0&0&1&0&0&0&1&0&0&0&1&1&1&1&1&0&1&1&0&0&0&1&0&1&1&1&0&0\\
1&0&1&1&0&1&1&1&0&1&1&1&0&0&1&1&0&1&1&1&0&0&1&1&0&0&0&0\\
0&1&0&1&0&1&0&0&1&0&1&0&0&1&1&1&1&1&1&1&1&1&0&1&1&0&1&1\\
1&0&0&1&0&1&0&1&1&0&1&0&1&0&0&1&1&0&0&1&0&0&1&0&1&1&0&0\\
1&0&0&0&1&1&0&1&1&0&0&0&0&1&0&0&1&0&1&1&0&1&1&1&0&1&1&1\\
1&0&1&0&0&0&1&1&0&1&1&1&1&1&1&0&0&0&1&0&0&1&1&1&1&1&1&1\\
1&1&0&0&0&0&1&0&0&1&0&0&0&1&0&0&1&1&0&1&1&0&0&0&0&0&0&0\\
0&1&0&0&1&1&1&0&0&1&1&0&0&1&1&1&0&1&1&1&0&1&1&0&1&0&1&0\\
0&1&1&0&1&1&1&0&1&0&1&1&1&0&0&1&0&1&0&1&0&0&1&1&1&0&0&1\\
0&1&0&0&1&1&1&1&1&0&0&0&1&0&1&0&0&1&1&0&1&0&0&1&0&0&1&1\\
0&1&1&1&0&1&0&1&0&1&0&1&0&1&0&1&1&0&0&0&0&1&0&0&1&1&0&0\\
1&1&0&1&1&0&0&1&0&1&0&0&0&0&1&1&1&0&0&0&1&0&0&0&1&1&0&0\\
0&1&0&0&1&1&0&1&1&1&0&0&0&1&1&1&1&0&0&0&1&1&0&1&0&1&0&1\\
1&1&1&0&1&1&1&1&1&1&1&0&0&1&0&1&0&0&1&1&0&1&0&0&1&0&1&1\\
1&1&1&1&0&0&0&1&0&0&0&1&0&0&0&0&1&1&1&0&1&1&0&1&1&0&1&0\\
1&0&0&0&1&1&0&1&1&0&0&0&1&1&1&1&0&1&1&1&0&1&1&0&1&0&1&0\\
1&1&1&1&1&0&1&1&0&0&0&1&0&1&1&1&1&1&1&1&1&0&0&1&0&0&0&1\\
1&0&0&0&1&0&0&1&0&0&0&0&1&1&0&0&0&0&0&0&0&1&1&0&1&1&0&0\\
1&0&0&1&1&0&0&1&1&1&0&0&1&0&0&1&0&1&0&1&1&1&0&1&1&1&1&1\\
0&1&1&1&0&1&0&1&1&1&0&1&1&0&1&0&0&1&1&1&0&0&1&0&1&0&1&0\\
0&1&0&0&0&1&1&1&1&1&0&0&1&0&1&0&0&1&0&0&0&1&1&0&1&0&0&1\\
1&0&1&0&1&0&1&0&1&0&1&1&1&0&1&1&0&0&1&0&0&0&0&1&1&0&1&0\\
0&0&0&0&1&0&1&0&0&1&1&0&1&1&0&0&1&1&0&0&0&0&1&1&1&1&1&1\\
1&0&0&0&1&1&1&0&1&1&0&0&1&0&1&0&1&0&1&0&1&1&0&0&0&1&1&1\\
1&0&0&1&1&1&1&1&1&1&1&0&1&1&1&1&1&1&0&1&0&0&0&1&1&0&0&1&0
\end{bmatrix}. \quad (6.7)$$

It can be readily seen that $K K^{-1} \bmod 2 = K^{-1} K \bmod 2 = I$.

On using the K^{-1} given in (6.7) and the ciphertext given in (6.6), we apply the decryption algorithm

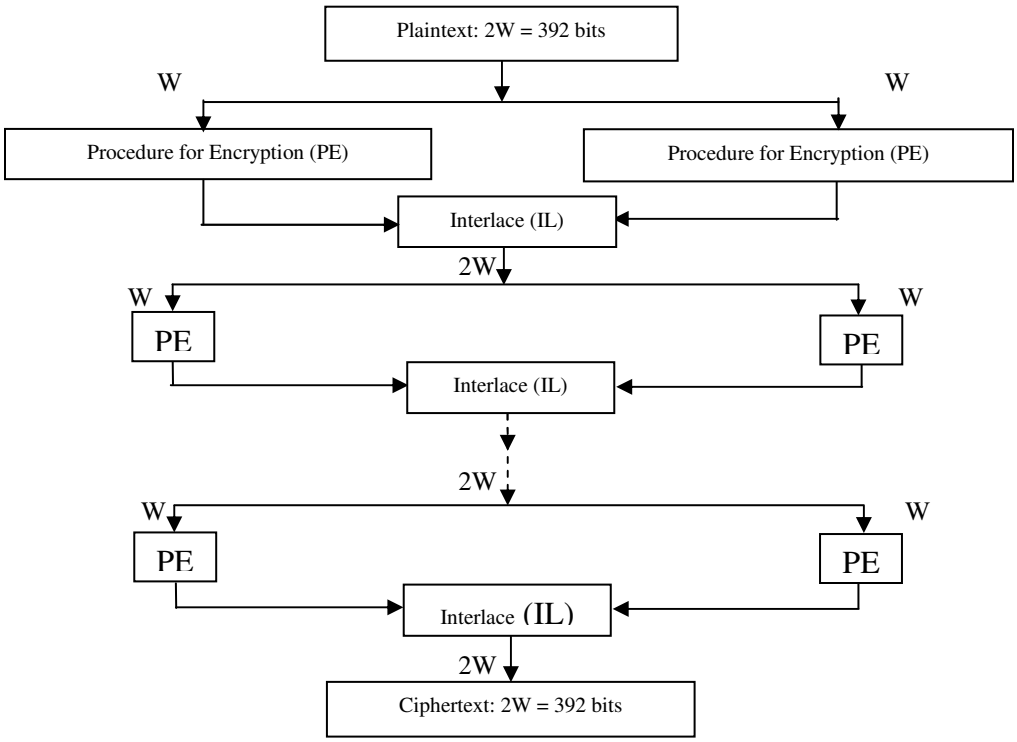

Fig. 1: Process of encryption for 392 bits plaintext

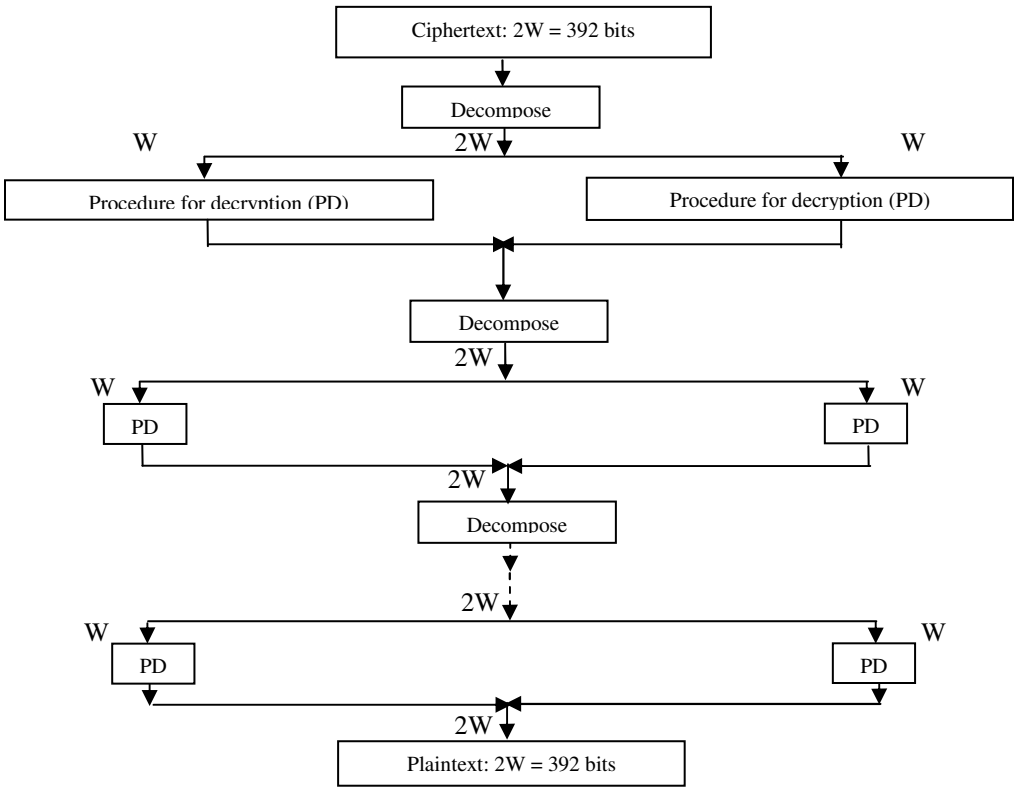

Fig. 2: Process of Decryption for 392 bits Ciphertext

(section 3.2) and obtain the original plaintext. In this case, the length of the plaintext is 196 bits.

We know very well that the strength of a cipher increases significantly as the length of the block increases. Thus let us consider a block of size 392 bits, which is double that of the previous block. The processes of encryption and decryption for the 392 bits block are shown in Fig. 1 and 2 respectively.

In Fig. 1, the plaintext of length 2W is divided into two halves, wherein each half (W) contains 196 bits. These bits are arranged in the form of a 28x7 matrix. Then PE, the procedure for encryption of 196 bits mentioned earlier is applied on both the Ws. After that the left side W and the right side W are interlaced as follows.

Each W containing 196 bits is arranged again in the form of a matrix of size 28x7. Let us now represent the left side and the right side matrices as A and B respectively.

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

For a thorough mixing of the matrices A and B, we mix the elements of the first column of A, as they are, with the elements of the last column of B taken in the reverse order. Similarly, elements of the second column of A are mixed with the elements of the last but one column of B. This process is continued till all the columns of A and B are exhausted. It is to be noted that the elements of the first column of A and the elements of the last but one column of B are mixed in the following manner. The last element of the last column of B is placed next to the first element of the first column of A; the last but one element of the last column of B is placed next to the second element of the first column of A and so on. Then we get the elements in the form

$a_{1\,1}\ b_{28\,7}\ a_{2\,1}\ b_{27\,7}\ a_{3\,1}\ b_{26\,7}\ a_{4\,1}\ b_{25\,7}\ \ldots$

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

In Fig. 2, PD is the procedure for the decryption of a block of size 196 bits and Decompose is a function which acts in an opposite way to interlacing.

Let us consider the plaintext: Almighty saves the Universe as all are his own children! (6.8)

Including the blank spaces the total number of characters in the plaintext is 56. By adopting the encryption procedure depicted in Fig. 1, we get the ciphertext given by

10000111000011100011110101001000110000101001001101
11101010111101111110011100011011010010101001000010
10011011011000100101111010111000000000111101001001
10101000000001000101100111000011010010000010111100
01100011110000010110110110100111110111101110101101
11110010111100110100011110011101111010000101001101
01011001110101111100110100111001111000110100100111
11001011001111000101000101001000101111010. (6.9)

Now on applying the decryption process given in Fig. 2, we readily get back the original plaintext.

7. Avalanche effect: Let us focus our attention on the plaintext given by (6.8). Let the ASCII code representation of the plaintext be changed by one bit, by changing the character A in the word "Almighty" to C. Now, on applying the encryption procedure to the modified plaintext, we get the ciphertext in the form given by

10010010100101100110100010010101011110100011100101
00110001000001101000000100001010010010001111100000
00011101011101110110010000100111100110110001010110
00011100001100101111000110010010011010111110101110
10001101100010000011000011110100101000000010111000
11010111110001000011010011001001001011001101111001
01101100101100010011010110111001000000011100001111
00000100100111101111110010111101111001101 (7.1)

On comparing (7.1) and (6.9), we notice that these two ciphertexts differ in 193 bits out of 392 bits. The avalanche effect found here is highly significant. This shows that the strength of the algorithm is quite considerable.

Now, let us consider the case wherein the key is changed in one bit position. This is achieved by replacing the number 48 by 50 in the key given by (6.4). Thus the new key assumes the form

[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] (7.2)

Using (7.2) we get the key matrix. Then the ciphertext for the plaintext given in (6.8) using the key given by (7.2) is obtained as

00010100101001000111010000110001100010101011000100
11111100101100001111010001011000111010011110001011
10111110111111111010010100001000001101101100000101 0
10100110010100101010100001101101101011101101001001
10001001010000111010001101101010010000011101001001
11101110010010010100010000110110100010100110010101
11110111111011010001101101101000000011111101010110
10100100011100101101100011001011011101110. (7.3)

From (7.3) and (6.9), it can be seen that these two ciphertexts differ in 192 bits out of 392 bits. This also indicates that the avalanche effect is conspicuous.

RESULTS AND CONCLUSION

In this study, we have developed a block cipher for blocks of sizes 98 bits, 196 bits and 392 bits. The plaintext is represented in the form of a matrix of size 14x7 or 28x7 depending upon the requirement. The algorithms developed for encryption and decryption depend upon iterative procedures, wherein the elements of the key are thoroughly mixed with the elements of the plaintext. These algorithms are implemented in C language. In this analysis, the mixing of the key and the plaintext in several stages has enabled us to obtain a very strong cipher, which cannot be broken by any cryptanalytic attack. From the above analysis, we conclude that the cipher is a potential one and it can be used effectively for secure transfer of information.

REFERENCES

1. Stallings, W., (Fourth Indian reprint, 2002, Pearson Prentice Hall). Cryptography and Network Security: Principles and Practices. Third Edn. Chp. 3, pp: 63.
2. Sastry, V.U.K. and V. Janaki, 2005. On the Modular Arithmetic Inverse in the Cryptology of Hill Cipher. Proc. North American Technology and Business Conf., Montreal, Canada.