ISSN:0975-9646

A Modified Feistel Cipher Involving a Pair of Key Matrices, Supplemented with XOR Operation, and Blending of the Plaintext in each Round of the Iteration Process

[1]V.U.K. Sastry, [2]K. Anup Kumar

[1]Director School of Computer Science and Informatics, Dean (R & D), Dean (Admin),

Department of Computer Science and Engineering,

Sreenidhi Institute of Science and Technology, Ghatkesar, Hyderabad, 501301, Andhra Pradesh, India.

[2]Associate Professor, Department of Computer Science and Engineering,

Sreenidhi Institute of Science and Technology, Ghatkesar, Hyderabad, 501301, Andhra Pradesh, India.

Abstract: In this paper, we have devoted our attention to the study of a block cipher which is obtained by modifying the classical Feistel cipher. In this, the plaintext block is divided into two matrices of equal size, and one of the matrices is multiplied by one key on the left side and the other key on the right side. The resulting expression is subjected to modulo operation. After interchanging the portions of the plaintext, they are blended very thoroughly (by converting the decimal numbers into binary bits) in each round of the iteration process. The avalanche effect shows that the cipher is reliable, and the cryptanalysis firmly confirms that the cipher is a strong one.

Key words: ***Encryption, Decryption, key, plaintext, cipher text, Blending, Avalanche Effects etc.***

Introduction

The study of the Feistel cipher [1-2] brought in a revolution in the area of cryptography. It lead to the development of several prominent block ciphers such as, DES [3], Double DES [4], and Triple DES [5]. In all these ciphers, iteration, mixing and substitution play a vital role in strengthening the cipher under consideration. Nevertheless, basically in all these block ciphers, the length of the plaintext is much less (64 bits or128 bits or 192 bits), and the length of the key is 56 bits.

In a recent investigation, Sastry et al [6-7] have studied a pair of block ciphers obtained on modifying the Feistel cipher. In their analysis, they have considered a plaintext (containing 128 characters) in the form of a matrix of size 8x16, and taken a key matrix of size 8x8. In view of these facts, the length of the plaintext is 1024 bits and the length of the key is 512 bits. In a recent development, we [8-9] have included a pair of functions called Mix ( ) and Permute ( ), in the process of encryption, and have shown that the strength of the cipher increases significantly on account of the diffusion and the confusion caused by these functions.

In the present paper, our objective is to develop a block cipher, called modified Feistel cipher, by including a pair of key matrices, wherein, the key matrices are used for multiplying a portion the plaintext from both the sides. In this analysis, we use a function called Blend ( ) for the blending of the binary bits of the key matrices and the plaintext matrix in a through manner at each stage of the iteration process. This sort of blending is expected to strengthen the cipher in a remarkable manner.

Here we mention the plan of the paper. Section 2 deals with the development of the cipher. In this, we present the flow charts and the algorithms describing the encryption and decryption. Section 3 is devoted to an illustration of the cipher. In this we have discussed the avalanche effect. In section 4, we have studied the cryptanalysis. Finally in section 5, we have focused our attention on the details of the computations and drawn conclusions obtained in this investigation.

1. Development of the cipher

Consider a plaintext P which contains $2m^2$ characters. We use EBCIDIC code and write P in the form of a pair of square matrices called P_0 and Q_0, whose size

is m. Let us take a pair of square matrices K and L of size m, as key matrices, and assume that the elements of K and L are lying in [0-255].
In this analysis, the process of encryption is governed by the relations

$$\left.\begin{aligned} P_i &= Q_{i-1}\ , \\ Q_i &= (\ P_{i-1} \oplus (KQ_{i-1}L)\ ) \bmod N, \end{aligned}\right\} \text{for i = 1 t} \qquad (2.1)$$

Here N=256, and n denotes the number of rounds in the iteration process.

Further, (2.1) is supplemented with a function called Blend ( ) which includes the process of blending of the plaintext portions in each round of the iteration process. The details of the function Blend ( ) are explained later.

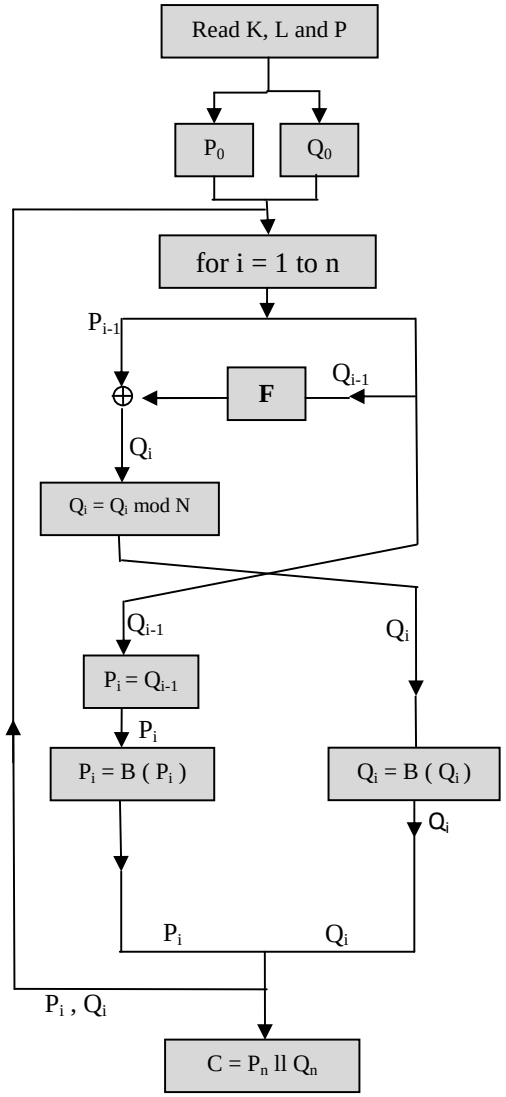

Fig 1. The process of encryption

In the above flow chart, the function F involves K, Q_{i-1} and L.

The process of decryption can be written in the form

$$\left.\begin{aligned} Q_{i-1} &= P_i, \\ P_{i-1} &= (\ Q_i \oplus (\ K\ P_i\ L)\ ) \bmod N, \end{aligned}\right\} \text{for i = n to 1.} \qquad (2.2)$$

In the process of decryption we use the function IBlend ( ) which denotes the reverse process of Blend ( ). The flowcharts displaying the encryption and the decryption processes are given Fig 1. and Fig 2.

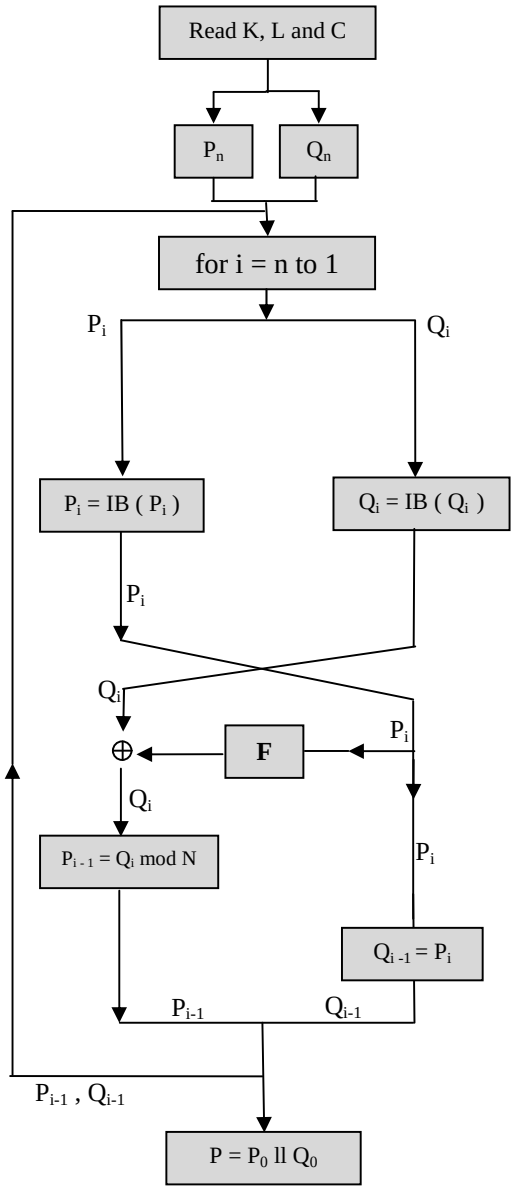

Fig 2. The process of Decryption

The algorithms corresponding to encryption and decryption are given below.

Algorithm for Encryption

1. Read P, K, L.

2. P_0 = Left half of P.

3. Q_0 = Right half of P.

4. for i = 1 to n

begin

$P_i = Q_{i-1}$

$Q_i = (P_{i-1} \oplus (K\ Q_{i-1}\ L)) \bmod N$

$P_i = B(P_i)$, $Q_i = B(Q_i)$ } The Process of Blending

end

5. $C = P_n \| Q_n$ /* ‖represents concatenation */

6. Write(C)

Algorithm for Decryption

1. Read C, K and L.

2. P_n = Left half of C

3. Q_n = Right half of C

4. for i = n to 1

Begin

$P_{i-1} = IB(P_i)$, $Q_{i-1} = IB(Q_i)$ } The Process of Reverse Blending

Qi-1 = Pi

Pi-1 = (Qi $\oplus$ (K P_i L)) mod N

end

5. $P = P_0 \| Q_0$ /* ‖ represents concatenation */

6. Write (P)

For the sake of elegance, we have written the functions Blend ( ) and IBlend ( ) as B ( ) and IB ( ) respectively. In this analysis we have taken n=16.

The process of blending represented by the function Blend ( ), can be explained as follows.

Let U and V be a pair of matrices (corresponding to P_i and Q_i) given by

$U = [U_{ij}]$, i = 1 to m, j =1 to m and

$V = [V_{ij}]$, i = 1 to m, j =1 to m

On interchanging the even columns of U and V we get the matrices given by

$$\begin{bmatrix} U_{11} & V_{12} & U_{13} & V_{14} & \dots & U_{1m-1} & V_{1m} \\ U_{21} & V_{22} & U_{23} & V_{24} & \dots & U_{2m-1} & V_{2m} \\ \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots \\ U_{m1} & V_{m2} & U_{m3} & V_{m4} & \dots & U_{m,m-1} & V_{mm} \end{bmatrix} \quad (2.3)$$

$$\begin{bmatrix} V_{11} & U_{12} & V_{13} & U_{14} & \dots & V_{1m-1} & U_{1m} \\ V_{21} & U_{22} & V_{23} & U_{24} & \dots & V_{2m-1} & U_{2m} \\ \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots \\ V_{m1} & U_{m2} & V_{m3} & U_{m4} & & V_{m,m-1} & U_{mm} \end{bmatrix} \quad (2.4)$$

Now we call the matrices (2.3) and (2.4) as U and V again.

On converting the currently obtained matrices U and V into their binary form, we get

$$U = \begin{bmatrix} U_{111}\,U_{112}\ldots..U_{117}\,U_{118} & U_{121}\,U_{122}\ldots..U_{127}\,U_{128} & \ldots\ldots\ldots\ldots\ldots\ldots\ldots & U_{1m1}\,U_{1m2}\ldots..U_{1m7}\,U_{1m8} \\ U_{211}\,U_{212}\ldots..U_{217}\,U_{218} & U_{221}\,U_{222}\ldots..U_{227}\,U_{228} & \ldots\ldots\ldots\ldots\ldots\ldots\ldots & U_{2m1}\,U_{2m2}\ldots...U_{2m7}\,U_{2m8} \\ \vdots & \vdots & & \vdots \\ \vdots & \vdots & & \vdots \\ \vdots & \vdots & & \vdots \\ \vdots & \vdots & & \vdots \\ U_{m11}U_{m12}\ldots.U_{m17}\,U_{m18} & U_{m21}U_{m22}\ldots.U_{m27}\,U_{m28} & \ldots\ldots\ldots\ldots\ldots\ldots\ldots & U_{mm1}\,U_{mm2}\ldots.U_{mm7}\,U_{mm8} \end{bmatrix} \quad (2.5)$$

and

$$V = \begin{bmatrix} V_{111}\,V_{112}\ldots..V_{117}\,V_{118} & V_{121}\,V_{122}\ldots..V_{127}\,V_{128} & \ldots\ldots\ldots\ldots\ldots\ldots\ldots & V_{1m1}\,V_{1m2}\ldots..V_{1m7}\,V_{1m8} \\ V_{211}\,V_{212}\ldots..V_{217}\,V_{218} & V_{221}\,V_{222}\ldots..V_{227}\,V_{228} & \ldots\ldots\ldots\ldots\ldots\ldots\ldots & V_{2m1}\,V_{2m2}\ldots...V_{2m7}\,V_{2m8} \\ \vdots & \vdots & & \vdots \\ \vdots & \vdots & & \vdots \\ \vdots & \vdots & & \vdots \\ \vdots & \vdots & & \vdots \\ V_{m11}V_{m12}\ldots.V_{m17}\,V_{m18} & V_{m21}V_{m22}\ldots.V_{m27}\,V_{m28} & \ldots\ldots\ldots\ldots\ldots\ldots\ldots & V_{mm1}\,V_{mm2}\ldots.V_{mm7}\,V_{mm8} \end{bmatrix} \quad (2.6)$$

We now interchange the even columns of (2.5) and (2.6) and obtain a pair of matrices given by

$$U = \begin{bmatrix} U_{111}\,V_{112}\ldots..U_{117}\,V_{118} & U_{121}\,V_{122}\ldots..U_{127}\,V_{128} & \ldots\ldots\ldots\ldots\ldots\ldots\ldots & U_{1m1}\,V_{1m2}\ldots..U_{1m7}\,V_{1m8} \\ U_{211}\,V_{212}\ldots..U_{217}\,V_{218} & U_{221}\,V_{222}\ldots..U_{227}\,V_{228} & \ldots\ldots\ldots\ldots\ldots\ldots\ldots & U_{2m1}\,V_{2m2}\ldots...U_{2m7}\,V_{2m8} \\ \vdots & \vdots & & \vdots \\ \vdots & \vdots & & \vdots \\ \vdots & \vdots & & \vdots \\ \vdots & \vdots & & \vdots \\ U_{m11}V_{m12}\ldots.U_{m17}\,V_{m18} & U_{m21}V_{m22}\ldots.U_{m27}\,V_{m28} & \ldots\ldots\ldots\ldots\ldots\ldots\ldots & U_{mm1}\,V_{mm2}\ldots.U_{mm7}\,V_{mm8} \end{bmatrix} \quad (2.7)$$

$$V = \begin{bmatrix} V_{111}\,U_{112}\ldots..V_{117}\,U_{118} & V_{121}\,U_{122}\ldots..V_{127}\,U_{128} & \ldots\ldots\ldots\ldots\ldots\ldots\ldots & V_{1m1}\,U_{1m2}\ldots..V_{1m7}\,U_{1m8} \\ V_{211}\,U_{212}\ldots..V_{217}\,U_{218} & V_{221}\,U_{222}\ldots..V_{227}\,U_{228} & \ldots\ldots\ldots\ldots\ldots\ldots\ldots & V_{2m1}\,U_{2m2}\ldots...V_{2m7}\,U_{2m8} \\ \vdots & \vdots & & \vdots \\ \vdots & \vdots & & \vdots \\ \vdots & \vdots & & \vdots \\ \vdots & \vdots & & \vdots \\ V_{m11}U_{m12}\ldots.V_{m17}\,U_{m18} & V_{m21}U_{m22}\ldots.V_{m27}\,U_{m28} & \ldots\ldots\ldots\ldots\ldots\ldots\ldots & V_{mm1}\,U_{mm2}\ldots.V_{mm7}\,U_{mm8} \end{bmatrix} \quad (2.8)$$

On converting each 8 bits of (2.7), by taking the bits in a row wise manner, into the corresponding decimal number, we get a square matrix of size m. we call this as U. On handling (2.8) in a similar manner, we get another square matrix of size m, and we call this as V. This is the process of Blending which is represented by the function Blend ( ). On reversing the aforementioned process, we can construct the function IBlend ( ) comfortably.

2. Illustration of the cipher

Consider the plaintext given below

Dear father! I reached India very safely, and I have travelled in almost all the parts of this country. Before independence, as you told me, this country was well known for the development in Sanskrit literature and literature in many local languages. After independence, this country has started advancement in science and technology and is now richly equipped with several engineering designs and developments. However, the country is now having several political parties and the people are divided like anything. (3.1)

Now let us confine our attention to the first 128 characters of the plaintext (3.1). This is given by

Dear father! I reached India very safely, and I have travelled in almost all the parts of this country. Before independence, as (3.2)

On using the EBCIDIC code, this can be written in the form

$$\begin{bmatrix} 68 & 101 & 97 & 114 & 32 & 102 & 97 & 116 & 104 & 101 & 114 & 33 & 32 & 73 & 32 & 114 \\ 101 & 97 & 99 & 104 & 101 & 100 & 32 & 73 & 110 & 100 & 105 & 97 & 32 & 118 & 101 & 114 \\ 121 & 32 & 115 & 97 & 102 & 101 & 108 & 121 & 44 & 32 & 97 & 110 & 100 & 32 & 73 & 32 \\ 104 & 97 & 118 & 101 & 32 & 116 & 114 & 97 & 118 & 101 & 108 & 108 & 101 & 100 & 32 & 105 \\ 110 & 32 & 97 & 108 & 109 & 111 & 115 & 116 & 32 & 97 & 108 & 108 & 32 & 116 & 104 & 101 \\ 32 & 112 & 97 & 114 & 116 & 115 & 32 & 111 & 102 & 32 & 116 & 104 & 105 & 115 & 32 & 99 \\ 111 & 117 & 110 & 116 & 114 & 121 & 46 & 32 & 66 & 101 & 102 & 111 & 114 & 101 & 32 & 105 \\ 110 & 100 & 101 & 112 & 101 & 110 & 100 & 101 & 110 & 99 & 101 & 44 & 32 & 97 & 115 & 32 \end{bmatrix} \quad (3.3)$$

Thus we have

$$P_0 = \begin{bmatrix} 68 & 101 & 97 & 114 & 32 & 102 & 97 & 116 \\ 101 & 97 & 99 & 104 & 101 & 100 & 32 & 73 \\ 121 & 32 & 115 & 97 & 102 & 101 & 108 & 121 \\ 104 & 97 & 118 & 101 & 32 & 116 & 114 & 97 \\ 110 & 32 & 97 & 108 & 109 & 111 & 115 & 116 \\ 32 & 112 & 97 & 114 & 116 & 115 & 32 & 111 \\ 111 & 117 & 110 & 116 & 114 & 121 & 46 & 32 \\ 110 & 100 & 101 & 112 & 101 & 110 & 100 & 101 \end{bmatrix} \quad (3.4)$$

and

$$Q_0 = \begin{bmatrix} 104 & 101 & 114 & 33 & 32 & 73 & 32 & 114 \\ 110 & 100 & 105 & 97 & 32 & 118 & 101 & 114 \\ 44 & 32 & 97 & 110 & 100 & 32 & 73 & 32 \\ 118 & 101 & 108 & 108 & 101 & 100 & 32 & 105 \\ 32 & 97 & 108 & 108 & 32 & 116 & 104 & 101 \\ 66 & 101 & 102 & 111 & 114 & 101 & 32 & 105 \\ 110 & 99 & 101 & 44 & 32 & 97 & 115 & 09 \\ 110 & 99 & 101 & 44 & 32 & 97 & 115 & 32 \end{bmatrix} \quad (3.5)$$

Let us now choose the key matrices K and L in the form

$$K = \begin{bmatrix} 13 & 58 & 121 & 222 & 63 & 110 & 201 & 61 \\ 55 & 212 & 73 & 69 & 220 & 205 & 15 & 37 \\ 121 & 93 & 85 & 116 & 173 & 19 & 87 & 200 \\ 53 & 76 & 32 & 117 & 89 & 75 & 43 & 197 \\ 108 & 164 & 176 & 50 & 72 & 233 & 210 & 11 \\ 78 & 184 & 250 & 211 & 130 & 15 & 29 & 64 \\ 179 & 124 & 10 & 161 & 14 & 182 & 190 & 217 \\ 100 & 200 & 01 & 36 & 139 & 83 & 172 & 188 \end{bmatrix} \quad (3.6)$$

and

$$L = \begin{bmatrix} 112 & 61 & 130 & 11 & 67 & 94 & 119 & 120 \\ 01 & 09 & 139 & 114 & 150 & 110 & 117 & 173 \\ 156 & 122 & 05 & 36 & 72 & 135 & 176 & 104 \\ 45 & 190 & 21 & 99 & 200 & 86 & 49 & 80 \\ 154 & 200 & 38 & 177 & 134 & 228 & 69 & 55 \\ 112 & 250 & 230 & 247 & 13 & 44 & 206 & 116 \\ 110 & 118 & 69 & 210 & 89 & 109 & 100 & 88 \\ 154 & 170 & 127 & 113 & 99 & 10 & 140 & 189 \end{bmatrix} \quad (3.7)$$

On applying the encryption algorithm, we get the cipher text C in the form

$$\begin{bmatrix} 50 & 78 & 63 & 14 & 253 & 207 & 156 & 253 & 242 & 57 & 37 & 139 & 133 & 212 & 143 & 108 \\ 194 & 82 & 71 & 102 & 45 & 35 & 114 & 42 & 205 & 136 & 59 & 104 & 240 & 46 & 91 & 111 \\ 139 & 182 & 196 & 145 & 144 & 118 & 247 & 206 & 246 & 183 & 231 & 51 & 76 & 131 & 162 & 190 \\ 193 & 13 & 118 & 54 & 243 & 150 & 255 & 160 & 118 & 222 & 183 & 253 & 242 & 134 & 155 & 217 \\ 219 & 57 & 228 & 143 & 175 & 234 & 217 & 190 & 149 & 11 & 49 & 141 & 164 & 151 & 169 & 03 \\ 76 & 128 & 195 & 188 & 119 & 38 & 28 & 44 & 06 & 207 & 17 & 23 & 230 & 197 & 93 & 29 \\ 205 & 190 & 30 & 219 & 124 & 244 & 202 & 186 & 103 & 159 & 174 & 73 & 254 & 88 & 164 & 214 \\ 32 & 30 & 239 & 150 & 239 & 105 & 115 & 59 & 236 & 242 & 254 & 30 & 225 & 123 & 169 & 182 \end{bmatrix} \quad (3.8)$$

On applying the decryption algorithm on the cipher text (3.8), we get back the original plaintext (3.2).

Let us now study the avalanche effect. To carry out this one, we change the first character of the plaintext (3.2) from D to E. As the EBCIDIC codes of these two characters are 68 and 69, they differ by one binary bit. On using the modified plaintext, obtained in the aforementioned manner, the keys K and L given by (3.6) and (3.7) and the encryption algorithm, we get the corresponding cipher text C in the form

$$\begin{bmatrix} 67 & 44 & 198 & 54 & 181 & 206 & 139 & 169 & 200 & 229 & 61 & 147 & 233 & 88 & 147 & 191 \\ 98 & 251 & 178 & 09 & 181 & 253 & 186 & 62 & 198 & 178 & 206 & 232 & 146 & 104 & 91 & 189 \\ 165 & 136 & 07 & 186 & 109 & 153 & 44 & 75 & 219 & 120 & 243 & 158 & 95 & 55 & 38 & 117 \\ 43 & 233 & 144 & 53 & 49 & 140 & 115 & 98 & 174 & 159 & 06 & 199 & 115 & 103 & 37 & 143 \\ 12 & 68 & 57 & 193 & 100 & 142 & 193 & 219 & 230 & 66 & 195 & 146 & 146 & 180 & 91 & 150 \\ 219 & 211 & 26 & 79 & 15 & 103 & 173 & 201 & 219 & 192 & 118 & 165 & 140 & 157 & 180 & 121 \\ 219 & 99 & 107 & 223 & 205 & 240 & 04 & 63 & 156 & 168 & 202 & 201 & 153 & 01 & 168 & 220 \\ 178 & 213 & 185 & 188 & 59 & 219 & 158 & 72 & 250 & 107 & 55 & 34 & 182 & 55 & 243 & 114 \end{bmatrix} \quad (3.9)$$

On comparing (3.8) and (3.9), after converting them into their binary form, we notice that these two differ by 511 binary bits (out of 1024 bits). This shows that the strength of the cipher is considerable.

Now let us examine the effect of one bit change in the key. To this end, let us change the second row, first column element of the key K (given by (3.6)) from 55 to 54. Thus we have one bit change in the key. On using the modified key, the original plaintext (3.2) and the encryption algorithm, we obtain the cipher text C in the form

$$\begin{bmatrix} 107 & 236 & 237 & 147 & 250 & 204 & 216 & 100 & 150 & 244 & 222 & 95 & 57 & 29 & 167 & 111 \\ 159 & 190 & 155 & 101 & 80 & 237 & 239 & 114 & 192 & 197 & 93 & 37 & 36 & 141 & 183 & 133 \\ 228 & 153 & 219 & 71 & 130 & 75 & 119 & 162 & 76 & 85 & 154 & 100 & 29 & 189 & 243 & 196 \\ 05 & 152 & 198 & 214 & 246 & 181 & 216 & 219 & 86 & 197 & 165 & 70 & 115 & 201 & 31 & 95 \\ 27 & 149 & 155 & 233 & 115 & 150 & 255 & 233 & 44 & 85 & 154 & 100 & 29 & 189 & 243 & 196 \\ 05 & 152 & 137 & 225 & 237 & 35 & 158 & 142 & 228 & 195 & 135 & 76 & 243 & 01 & 238 & 233 \\ 223 & 102 & 67 & 156 & 183 & 123 & 146 & 131 & 183 & 190 & 72 & 128 & 179 & 00 & 05 & 205 \\ 185 & 126 & 90 & 88 & 195 & 182 & 149 & 176 & 26 & 183 & 212 & 219 & 50 & 69 & 189 & 106 \end{bmatrix} \quad (3.10)$$

On converting (3.8) and (3.10) into their binary form, and comparing them we find that, they differ by 505 bits (out of 1024 bits). This also clearly indicates that the cipher is a strong one.

4. Cryptanalysis

In the literature of cryptography, it is well known that the different types of attacks that are made use of by attackers are

1. Cipher text only (Brute Force) attack.

2. Known Plaintext attack.

3. Chosen Plaintext attack.

4. Chosen Cipher text attack.

In the study of the cryptanalysis, it is assumed that the cipher text and the algorithm are fully known to the attacker. Generally a cipher is designed [ ] to withstand the first two attacks, while the later two are applied rarely as they are found to be more complex.

Let us now consider the brute force attack. In this analysis we have two keys namely K and L, wherein each one is containing m^2 decimal numbers. Thus the total length of the equivalent single key can be taken as 2^{m2} decimal numbers wherein each number lies in the interval [0-255]. Thus the size of the key space is

$$2^{16m^2} = \left(10^{3}\right)^{1.6m^2} = 10^{4.8m^2}$$

For the execution of this algorithm if we require 10^{-7} seconds with one value of the key, then the total time required for the completion of the execution, with all possible keys in the key space is

$$10^{4.8m^2} \times 10^{-7} \text{ seconds}$$

$$= \frac{10^{4.8m^2} \times 10^{-7}}{365 \times 24 \times 60 \times 60} \text{ years}$$

$$= 10^{4.8m^2} \times 3.12 \times 10^{-15} \text{ years}$$

$$= 3.12 \times 10^{(4.8m^2 - 15)} \text{ years}$$

In the present analysis as m = 8, the time required for execution is

$$= 3.12 \times 10^{292.2} \text{ years.}$$

As this time is very large, it is not at all possible to break this cipher by the brute force attack.

We now examine the known plaintext attack. In this case, we know as many plaintext and corresponding cipher text pairs as we require for carrying out the analysis.

In the encryption process, the plaintext is divided into two parts, namely P and Q. Here, in each round of the iteration process, Q is multiplied by the keys K and L, and mod operation is carried out. Then the resulting plaintext portions are interchanged. After that, we have carried out a through blending (in an appropriate manner) of the plaintext portions by converting each element of P and Q into binary bits. As the entire process applied in this analysis is quite complex, the relation ship between the final cipher text and the initial plaintext will be in a formidable manner. Thus, the keys K and L involved in the process cannot be determined for breaking the cipher by any means. In view of the above facts, this cipher is a strong one.

5. Computations and Conclusions

In this investigation, we have developed a block cipher by modifying the classical Feistel cipher. Here the plaintext is divided into two square matrices wherein each one is of size m. In this, one of the matrices is multiplied by a pair of keys wherein one of the key is a left multiplicant and the other is right multiplicant, and this result is subjected to modulo operation. After interchanging the resulting matrices, they are thoroughly blended to achieve confusion and diffusion. This process is carried out for sixteen rounds. The programs required in this analysis for encryption and decryptions are written in C language.

Considering the plaintext given in (3.1), we divide it into four blocks, wherein each block is containing 128 characters. On applying the process of encryption, we get the cipher text corresponding to the entire plaintext in the form (3.11).

101	118	111	116	105	111	110	46
32	73	102	32	119	101	32	99
97	110	32	98	111	109	98	97
114	100	32	116	104	101	32	99
108	111	117	100	115	32	97	110
100	32	100	114	105	118	101	32
116	104	101	109	32	111	117	116

32	105	110	116	111	32	66	97
121	32	111	102	32	66	101	110
103	97	108	32	97	110	100	32
112	114	111	116	101	99	116	32
116	104	101	32	102	97	114	109
101	114	115	32	102	114	111	109
32	116	104	101	32	99	97	108
97	109	105	116	121	32	111	102
32	102	108	111	111	100	115	46
120	133	150	120	166	105	121	57
45	77	126	123	18	100	65	82
113	05	202	216	240	39	86	54
176	177	58	198	110	105	76	87
130	122	116	170	205	33	45	198
10	124	125	219	15	45	211	212
56	195	110	128	235	48	159	07
75	199	211	49	216	67	55	92
100	44	115	220	48	59	136	77
135	110	230	22	13	150	177	87
133	154	156	177	190	124	133	58
156	134	12	210	222	13	206	233
11	209	112	237	144	115	119	110
176	187	199	208	211	240	159	110
36	119	100	176	109	11	122	209
10	115	33	76	89	120	205	245
13	13	15	230	12	35	92	54
133	158	117	44	234	122	122	05
45	47	177	198	15	56	11	35
170	99	133	224	250	184	140	07
199	186	205	199	25	92	82	120
11	55	11	36	105	155	111	22
215	200	225	133	32	12	244	200
89	219	244	198	111	79	17	38
220	64	16	145	32	34	100	211
238	76	198	77	97	133	68	132
57	188	145	167	101	18	215	99
98	102	12	12	102	150	220	200
103	255	88	38	102	155	58	36
245	213	78	198	32	36	100	102
200	20	93	11	121	32	105	106
67	60	108	02	222	20	45	88
15	19	83	112	112	45	36	17
18	36	182	55	215	120	198	32
125	54	150	76	110	68	58	33
16	200	112	119	220	192	136	88
210	205	200	220	16	44	44	119
15	67	64	11	117	212	216	33
100	119	92	236	55	213	237	218
99	105	199	122	222	77	59	54
105	12	215	144	45	89	66	255
176	186	17	212	88	144	112	200
92	92	230	17	170	240	116	96
33	74	48	150	66	28	222	104
115	140	219	55	205	96	76	76
220	215	43	156	133	77	215	108

240	101	234	44	108	54	12	216
116	77	89	202	202	110	241	38

On using the decryption algorithm, given in section 2, on the cipher text (3.11), we get back the original plaintext (3.1). The cryptanalysis discussed in section 4, clearly indicates that this cipher is a strong one, and it is quite comparable with any other block cipher in the literature of cryptography.

References:

[1] William Stallings, Cryptography and Network Security, Principles and Practice, Third Edition, Pearson, 2003.
[2] Feistel H, "Cryptography and Computer Privacy", Scientific American, Vol. 228, No.5, pp. 15-23, 1973.
[3] Data Encryption Standard DES, William Stallings, Cryptography and Network Security, Principles and Practice, Third Edition, Pearson, 2003.
[4] Double DES, William Stallings, Cryptography and Network Security, Principles and Practice, Third Edition, Pearson, 2003.
[5] Triple DES, William Stallings, Cryptography and Network Security, Principles and Practice, Third Edition, Pearson, 2003.
[6] V. U. K. Sastry, D. S. R. Murthy, S. Durga Bhavani, "A Block Cipher Involving a Key Applied on Both the Sides of the Plain Text", International Journal of Computer and Network Security (IJCNS), Vol.1, No. 1, pp. 27 -30, Oct. 2009.
[7] V. U. K. Sastry, V. Janaki, "A large block cipher involving a key applied on both sides of the plain text, IJCNS. Vol. 2, No. pp. 10 - 13, Feb 2010.
[8] V. U. K. Sastry, K. Anup Kumar "A Modified Feistel Cipher involving a key as a multiplicant on both the sides of the Plaintext matrix and supplemented with Mixing, Permutation and XOR operation" IJCTA.
[9] V. U. K. Sastry, K. Anup Kumar "A Modified Feistel Cipher Involving a Key as a Multiplicant on Both the Sides of the Plaintext Matrix and Supplemented with Mixing, Permutation, and Modular Arithmetic Addition" IJCTA

Authors profile:

Dr. V. U. K. Sastry is presently working as Professor in the Dept. of Computer Science and Engineering (CSE), Director (SCSI), Dean (R & D), SreeNidhi Institute of Science and Technology (SNIST), Hyderabad, India. He was Formerly Professor in IIT, Kharagpur, India and Worked in IIT, Kharagpur during 1963 – 1998. He guided 12 PhDs, and published more than 40 research papers in various international journals. His research interests are Network Security & Cryptography, Image Processing, Data Mining and Genetic Algorithms.

Mr. K. Anup Kumar is presently working as an Associate Professor in the Department of Computer Science and Engineering, SNIST, Hyderabad India. He obtained his B.Tech (CSE) degree from JNTU Hyderabad and his M.Tech (CSE) from Osmania university, Hyderabad. He is now pursuing his PhD from JNTU, Hyderabad, under the supervision of Dr. V.U.K. Sastry in the area Information Security and Cryptography. He has 10 years of teaching experience and his interest in research area includes Cryptography, Steganography and Parallel Processing Systems.