A Block Cipher Obtained By Blending Modified Feistel Cipher And Advanced Hill Cipher Involving A Pair Of Key Matrices

[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 investigation, we have developed a block cipher by blending a modified Feistel cipher and the advanced Hill cipher. In this analysis, we have made use of a pair of involutory matrices, say A and B which include the keys K and L. Here the size of the plaintext is 1024 binary bits and the size of the keys (both put together) is 256 binary bits. The involutory matrices A and B, the modular arithmetic inverse, the XOR operation, and the functions Shift ( ) and Mix ( ) are playing a vital role in strengthening the cipher. The cryptanalysis carried out in this investigation clearly shows that the strength of the cipher is quite considerable, and the cipher cannot be broken by any attack.

Key words: Encryption, Decryption, Key matrix, Shift, Mix, XOR Operation.

Introduction

In the recent investigations [1], we have developed a block ciphers by generalizing the classical Feistel cipher [2], wherein we have considered a plaintext which can be represented in the form of a pair of matrices instead of a pair of binary strings that was used in the case of classical Feistel cipher.

In this development, we have made use of an involutory matrix to multiply both the sides of the plaintext matrix. In addition to this, we have made use of the operations Mix ( ) and Shift ( ) and XOR operation. The avalanche effect and the cryptanalysis discussed in this analysis effectively indicate that the cipher is a strong one.

In the present investigation, our objective is to develop the modified Feistel cipher using the features of Advanced Hill cipher [3] with multiple keys.

The basic equations governing the encryption and the decryption of this cipher are given by

$$\left.\begin{array}{l} P_i = (K\,Q_{i-1}\,L) \bmod N \\ Q_i = P_{i-1} \oplus P_i \end{array}\right\} \quad i = 1 \text{ to } n. \qquad (1.1)$$

and

$$\left.\begin{array}{l} Q_{i-1} = (K\,P_i\,L) \bmod N \\ P_{i-1} = Q_i \oplus P_i \end{array}\right\} \quad i = n \text{ to } 1. \qquad (1.2)$$

Here, P_i and Q_i are the plaintext matrices at the i^{th} stage of the iteration, K and L are the involutory key matrices and N is a positive integer chosen appropriately. Here n denotes the number of iterations. In the development of this cipher, we have utilized the functions Mix ( ) and Shift ( ), and XOR operation.

We now present the plan of the paper. In section 2, we discuss the development of a pair of involutory matrices. In section 3, we discuss the development of the cipher and present the flowcharts and the algorithms describing the cipher. Section 4 is devoted to an illustration of the cipher, and in this we have determined the avalanche effect. We investigate the cryptanalysis in section 5. Finally in section 6, we have given the details about the computations and conclusions.

1. Development of the Involutory Matrix

An involutory matrix is a square matrix whose inverse is same as the original matrix.
Let $A = [a_{ij}]$ and $B = [b_{ij}]$ be two square matrices of size n.
Let the involutory matrices of matrices A and B be denoted as

$$A = \begin{bmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{bmatrix} \qquad (2.1)$$

and

$$B = \begin{bmatrix} B_{11} & B_{12} \\ B_{21} & B_{22} \end{bmatrix} \qquad (2.2)$$

Where all the sub matrices A_{11}, A_{12}, A_{21} and A_{22} B_{11},B_{12},B_{21} and B_{22} are square matrices of size n/2.

As the modular arithmetic inverse of an involutory matrix given in (2.1) is governed by the relations

$$(A A^{-1}) \bmod N = I, \quad (2.3)$$

and $A = A^{-1}$ (2.4)

Thus we have, $A^2 \bmod N = I$ (2.5)

From (2.1) and (2.5) we get,

$$A_{22} \bmod N = - A_{11} \bmod N, \quad (2.5)$$

$$A_{12} = [\, d\,(I - A_{11})] \bmod N \quad (2.6)$$

$$A_{21} = [\, w\,(I + A_{11})\,] \bmod N \quad (2.7)$$

where $(dw) \bmod N = 1$ (2.8)

Given A_{11}, on selecting d, where d lies in the interval $0 < d < N$, firstly we obtain w from (2.8), then we determine A_{22}, A_{12} and A_{21} by satisfying the relations (2.5) to (2.7).

If A_{11} is the key represented by square matrix A of size n/2, then we get the involutory matrix K of size n.

Now let us consider the modular arithmetic inverse of an involutory matrix given in (2.2) governed by the relations

$$(B B^{-1}) \bmod N = I, \quad (2.9)$$

and $B = B^{-1}$

Thus we have, $B^2 \bmod N = I$ (2.11)

From (2.2) and (2.11) we get,

$$B_{22} \bmod N = - B_{11} \bmod N, \quad (2.12)$$

$$B_{12} = [\, s\,(I - B_{11})] \bmod N \quad (2.13)$$

$$B_{21} = [\, t\,(I + B_{11})\,] \bmod N \quad (2.14)$$

where $(st) \bmod N = 1$ (2.15)

Given B_{11}, on selecting s, where s lies in the interval $0 < s < N$, firstly we obtain t from (2.15), then we determine B_{22}, B_{12} and B_{21} by satisfying the relations (2.12) to (2.14). If B_{11} is the key represented by square matrix B of size n/2, then we get the involutory matrix L of size n.

2. Development of the Cipher

Let P be the plaintext consisting of $2m^2$ characters. On employing the EBCIDIC code, the plaintext can be written in the form of a pair of square matrices P_0 and Q_0, wherein, each one is of size m. Let us consider a key matrices K and L, whose size is mxm.

In the development of this cipher, encryption and decryption are governed by the relations (1.1) and (1.2) respectively. We now present the flow charts and the algorithms describing the encryption and the decryption processes.

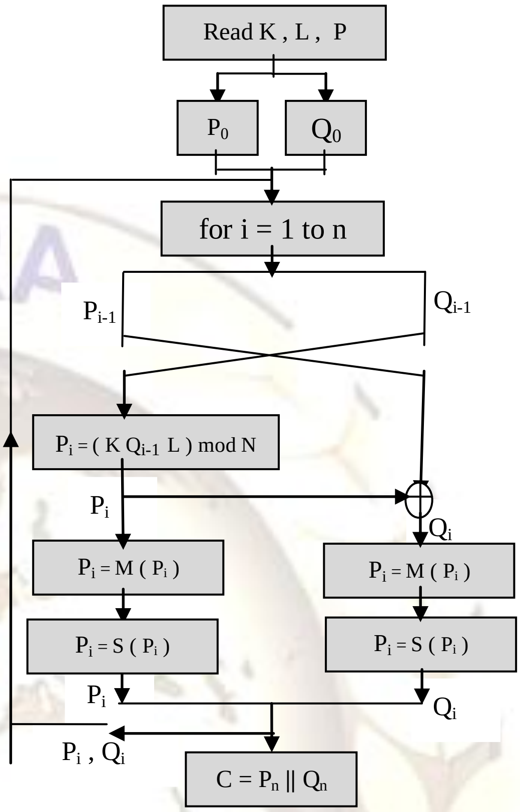

Fig 1. The process of Encryption

In the matrices P_i and Q_i, all the numbers are lying in the interval [0-255]. Here K and L are two involutory matrices of the key matrices and A and B respectively. In this analysis, we have taken n equal to 16.

In the flowchart, for the sake of elegance, we have written the functions Mix ( ) and Shift ( ), arising in encryption, as M ( ) and S ( ) respectively. The reverse processes represented by IMix ( ) and IShift ( ), arising in decryption, are denoted by IM ( ) and IS ( ).

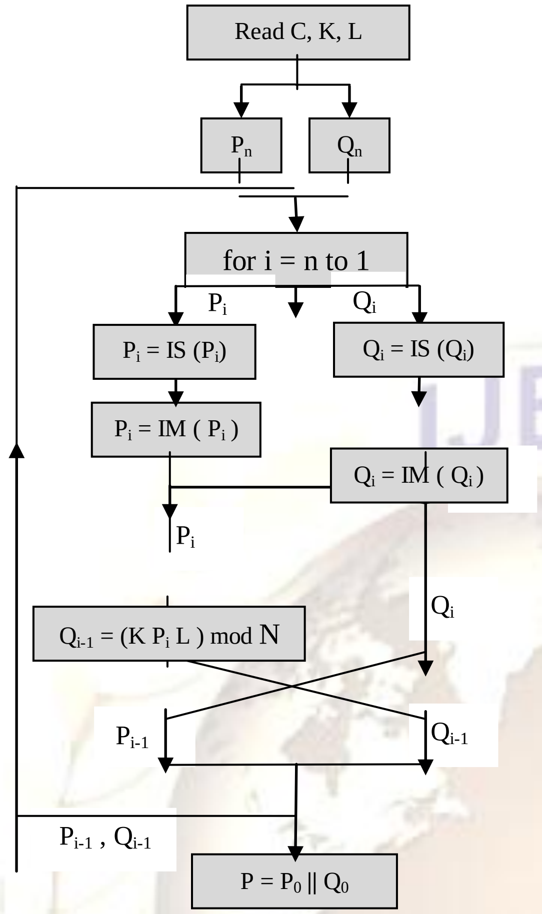

Fig 2. The process of Decryption

The processes of encryption and decryption depicted in the flow charts are described by the algorithms given below.

Algorithm for Encryption

1.Read P, A, n and N.

2.K = Involute (A,d)

3.L = Involute (B,s)

4. P_0 = Left half of P.

Q_0 = Right half of P.

5. for i = 1 to n

begin

P_i = (K Q_{i-1} L) mod N

Q_i = P_{i-1} $\oplus P_i$

P_i = M (P_i)

P_i = S (P_i)

Q_i = M (Q_i)

Q_i = S (Q_i)

end

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

7. Write(C)

Algorithm for Decryption

1.Read C, A, n and N.

2.K = Involute (A,d)

3.L = Involute (B,s)

4. P_n = Left half of C

Q_n = Right half of C

5. for i = n to 1

begin

P_i = IS (P_i)

P_i = IM (P_i)

Q_i = IS (Q_i)

Q_i = IM (Q_i)

Q_{i-1} = (K P_i L) mod N

P_{i-1} = Q_i $\oplus P_i$

end

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

7. Write (P)

For the sake of elegance, in the iteration process when we come across the function Mix ( ) and Shift ( ) during encryption, they are denoted as M ( ) and S ( ) respectively, and the functions IMix ( ) and IShift ( ) during decryption are denoted as IM ( ) and IS ( ). For a detailed explanation of these functions see [1].

3. Illustration of Cipher

Consider the plaintext given below.

Dear brother! India is well known for mines. There are many mines from which gold iron and silver can be obtained very easily. This is the basic reason for some Indians to become rich. Do remember in India right from the ancient times even upto today Indians fight among themselves. Even brothers cannot remain united! Right from the time of mahabharata even upto today same is the story of brothers. They do not think about their progress in a conjoint manner. Each one is a selfish fellow. Tell our brothers; one day or the other day we have to win over this country and rule again. (4.1)

Consider the first 128 characters of the plaintext. Thus we have

Dear brother! India is well known for mines. There are many mines from which gold iron and silver can be obtained very easily. T (4.2)

On converting each character of the plaintext in (4.2) into its EBCIDIC code form, we get the plaintext matrix P as

$$P=\begin{bmatrix} 68 & 101 & 97 & 114 & 32 & 98 & 114 & 111 & 116 & 104 & 101 & 114 & 33 & 32 & 73 & 110 \\ 100 & 105 & 97 & 32 & 105 & 115 & 32 & 119 & 101 & 108 & 108 & 32 & 107 & 110 & 111 & 119 \\ 110 & 32 & 102 & 111 & 114 & 32 & 109 & 105 & 110 & 101 & 115 & 46 & 32 & 84 & 104 & 101 \\ 114 & 101 & 32 & 97 & 114 & 101 & 32 & 109 & 97 & 110 & 121 & 32 & 109 & 105 & 110 & 101 \\ 115 & 32 & 102 & 114 & 111 & 109 & 32 & 119 & 104 & 105 & 99 & 104 & 32 & 103 & 111 & 108 \\ 100 & 32 & 105 & 114 & 111 & 110 & 32 & 97 & 110 & 100 & 32 & 115 & 105 & 108 & 118 & 101 \\ 114 & 32 & 99 & 97 & 110 & 32 & 98 & 101 & 32 & 111 & 98 & 116 & 97 & 105 & 110 & 101 \\ 100 & 32 & 118 & 101 & 114 & 121 & 32 & 101 & 97 & 115 & 105 & 108 & 121 & 46 & 32 & 84 \end{bmatrix} \quad (4.3)$$

Consider P_0 and Q_0 as two matrices obtained from (4.3), as the left halve and the right halve respectively. Thus we have

$$P_0=\begin{bmatrix} 68 & 101 & 97 & 114 & 32 & 98 & 114 & 111 \\ 100 & 105 & 97 & 32 & 105 & 115 & 32 & 119 \\ 110 & 32 & 102 & 111 & 114 & 32 & 109 & 105 \\ 114 & 101 & 32 & 97 & 114 & 101 & 32 & 109 \\ 115 & 32 & 102 & 114 & 111 & 109 & 32 & 119 \\ 100 & 32 & 105 & 114 & 111 & 110 & 32 & 97 \\ 114 & 32 & 99 & 97 & 110 & 32 & 98 & 101 \\ 100 & 32 & 118 & 101 & 114 & 121 & 32 & 101 \end{bmatrix} \quad (4.4)$$

$$Q_0=\begin{bmatrix} 116 & 104 & 101 & 114 & 33 & 32 & 73 & 110 \\ 101 & 108 & 108 & 32 & 107 & 110 & 111 & 119 \\ 110 & 101 & 115 & 46 & 32 & 84 & 104 & 101 \\ 97 & 110 & 121 & 32 & 109 & 105 & 110 & 101 \\ 104 & 105 & 99 & 104 & 32 & 103 & 111 & 108 \\ 110 & 100 & 32 & 115 & 105 & 108 & 118 & 101 \\ 32 & 111 & 98 & 116 & 97 & 105 & 110 & 101 \\ 97 & 115 & 105 & 108 & 121 & 46 & 32 & 84 \end{bmatrix} \quad (4.5)$$

Let us take a pair of key matrices A and B as

$$A=\begin{bmatrix} 69 & 124 & 27 & 167 \\ 135 & 79 & 99 & 111 \\ 248 & 199 & 209 & 75 \\ 239 & 45 & 255 & 92 \end{bmatrix} \quad (4.6)$$

and

$$B=\begin{bmatrix} 215 & 113 & 19 & 147 \\ 223 & 109 & 254 & 12 \\ 56 & 01 & 127 & 174 \\ 59 & 146 & 189 & 81 \end{bmatrix} \quad (4.7)$$

On using (2.5) to (2.7) and taking d = 99, we get the involutory key matrix K as

$$K=\begin{bmatrix} 69 & 124 & 27 & 167 & 180 & 12 & 143 & 107 \\ 135 & 79 & 99 & 111 & 203 & 214 & 183 & 19 \\ 248 & 199 & 209 & 75 & 24 & 11 & 144 & 255 \\ 239 & 45 & 255 & 92 & 147 & 153 & 99 & \\ 130 & 84 & 233 & 237 & 187 & 132 & 229 & \\ 141 & 112 & 1 & 133 & 121 & 177 & 157 & 145 \\ 168 & 77 & 134 & 249 & 8 & 57 & 47 & 181 \\ 5 & 47 & 181 & 63 & 17 & 211 & 1 & 164 \end{bmatrix} \quad (4.8)$$

On using ( ) to ( ) and taking s = 189 , we get the involutory key matrix L as

$$L=\begin{bmatrix} 215 & 113 & 19 & 147 & 02 & 147 & 249 & 121 \\ 223 & 109 & 254 & 12 & 93 & 68 & 122 & 36 \\ 56 & 01 & 127 & 174 & 168 & 67 & 250 & 138 \\ 59 & 146 & 189 & 81 & 113 & 54 & 119 & 240 \\ 184 & 197 & 15 & 143 & 41 & 143 & 237 & 109 \\ 203 & 06 & 214 & 252 & 33 & 147 & 02 & 244 \\ 152 & 149 & 128 & 70 & 200 & 255 & 129 & 82 \\ 87 & 250 & 01 & 186 & 197 & 110 & 67 & 175 \end{bmatrix}$$

(4.9)

On using (4.4) , (4.5) , (4.8) , (4.9) and the encryption algorithm given in section 3 , we get the cipher text C as

C=

28 188 242 196 4 152 196 240 246 144 220
218 18 68 132 224
58 110 90 220 182 222 22 146 102 108 30
8 44 84 154 100
200 58 122 230 136 10 48 140 172 236 106
176 182 172 138 74
140 230 146 62 190 54 42 54 210 230 44
254 210 88 170 52
36 176 86 104 144 118 246 206 16 22 98
18 194 218 70 114
110 94 150 150 48 236 164 108 6 206 70
114 96 194 166 120
182 216 250 66 4 56 202 118 184 38 248
110 168 182 100 138
122 206 126 250 150 62 124 54 110 102 100
124 152 128 122 186

(4.10)

Now on applying the decryption algorithm given in section 3 with necessary inputs, we get back the original plaintext given in (4.3).

Let us now consider the avalanche effect which shows the strength of the cipher in a qualitative manner.

In order to carry out this one, firstly, let us consider a one bit change in plaintext P. This can be done by changing the first row , first column element of (4.3) from 68 to 69.

On using the modified plaintext and without altering the keys K and L and by adopting the encryption algorithm given in section 3, we get the ciphertext as

C =

124 38 238 178 202 230 126 216 94 246 244
122 156 166 178 236
16 146 104 90 188 164 136 6 186 108 152
44 170 126 252 64
248 14 242 200 150 36 236 182 210 2 204
220 152 212 174 166
64 212 198 48 204 138 186 28 204 190 12
156 150 60 48 16
24 108 130 182 204 132 236 232 114 82 86
138 98 72 224 236
244 184 58 120 14 212 176 146 182 142 58
108 102 56 44 144
60 144 244 214 44 90 154 198 76 66 72 98
188 184 184 20
176 190 138 48 140 170 114 110 164 98 234
214 146 190 120 202

(4.11)

On comparing (4.10) and (4.11) in their binary form, we readily notice that these two ciphers differ by 513 bits out of 1024 bits this shows that the cipher is a potential one.

Let us now consider a one bit change in the key K, this can be done by changing the first row, first column element from 69 to 67.

On using the modified key and the encryption algorithm given in section 3 , and by keeping the plaintext as it is , we get the cipher text C as

238 218 42 222 254 174 116 244 154 190 206
46 156 166 178 236
16 146 104 90 188 164 136 6 186 108 152
44 170 126 252 64
248 14 242 218 110 164 10 38 88 146 204
220 152 212 174 166
64 212 198 48 204 138 186 28 204 190 12
156 150 60 48 16
10 218 210 228 164 172 22 198 146 24 108
130 182 204 224 236
244 184 58 120 14 212 176 146 182 142
58 108 102 56 44 144
60 144 244 214 44 146 88 228 184 188
100 212 60 184 184 20
176 190 138 48 140 170 114 110 164 98 234
214 146 190 120 202

(4.12)

On comparing (4.10) and (4.12) in their binary form we notice that they differ by 517 bits out of 1024 bits. This shows that the cipher is a strong one.

4. Cryptanalysis

In the literature of cryptography, the conventional cryptanalytic attacks used are

1. Cipher text only (Brute Force) attack.
2. Known Plaintext attack.
3. Chosen Plaintext attack.
4. Chosen Cipher text attack.

The primary goal of all these cryptanalytic attacks is to break the cipher by obtaining the key used for encryption.

Let us now consider the brute force attack first, in the development of this cipher, as we have used a pair of key matrices A and B, each one having size 4x4. There are 32 decimal number in the key. As each element of the key can be represented with 8 binary bits in its EBCIDIC code form, the total length of the key is 256 bit.

Hence the size of the key space is

$$2^{256} = (2^{10})^{25.6} \approx (10^3)^{25.6} = 10^{76.8}$$

If the time required to get the plaintext by using one value of the key in the key space is 10^{-7} seconds, then the time required to execute the cipher with all possible keys in key space is

$$\frac{10^{76.8} \times 10^{-7}}{365 \times 24 \times 60 \times 60} = 3.171 \times 10^{61.8} \text{ years.}$$

As this number is very large, it is impractical to break the cipher by using this attack.

Let us examine the known plaintext attack, to carry out this attack, assume that the attacker knows the plaintext P ciphertext C pairs as many as required.

If we confine our attention to only one round of the iteration process i.e r = 1. Then the relations governing the encryption process for one round can be written as

$$P_1 = (K\, Q_0\, L) \bmod N \quad (5.1)$$
$$Q_1 = P_0 \oplus P_1 \quad (5.2)$$
$$P_1 = M (P_1) \quad (5.3)$$
$$P_1 = S (P_1) \quad (5.4)$$
$$Q_1 = M (Q_1) \quad (5.6)$$
$$Q_1 = S (Q_1) \quad (5.7)$$
$$C = P_1 \,\|\, Q_1 \quad (5.8)$$

Here we know P_0, Q_0 and C and the encryption algorithm. As the functions Shift ( ) and Mix ( ) are known, using (5.8) to (5.3), we get P_1 and Q_1 occurring on the left hand side of (5.1) and (5.2) As P_0 and the Q_0 occurring on the right hand side of (5.1) and (5.2) are known to the attacker, the key K or the key L can not be obtained due to the modulo of N used in (5.1). Thus the cipher cannot be broken by the known plaintext attack even if we confine our attention only to the first round of the iteration process. This shows that it is impossible to break the final cipher obtained after sixteen rounds of the iteration process by using the known plaintext attack.

Intuitively choosing a plaintext or ciphertext and determining the key or a function of the key is a formidable task in the case of this cipher.

Thus from the above discussion we conclude that this cipher is not breakable by all the possible attacks that are available in the cryptography.

5. Computations and Conclusions

In present paper, we have developed the modified Fesitel cipher. To introduce confusion and diffusion, we have used a pair of functions namely Shift ( ) and Mix( ), and the modulo operation in every round of the iteration. As these features thoroughly mix the plaintext at every stage of the iteration process, the strength of the cipher is good which is proved by the avalanche effect discussed in section 4. Further, as we have increased the key space by considering a pair of keys, the strength of the cipher has increased enormously. The programs required for encryption and decryption are written in C Language.

5. References

[1] V. U. K. Sastry, K. Anup Kumar, “A Block Cipher Obtained by Blending Modified Feistel Cipher and Advanced Hill Cipher Involving a Single Key Matrix” (Sent for Publication) IJERA, Aug 2012

[2] William Stallings, Cryptography and Network Security, Principles and Practice, Third Edition, Pearson, 2003.

[3] Bhibhudendra Acharya, Saroj Kumar Pahigrahy, Sarat Kumar Parta, and Ganapati Panda, “Image encryption using Advanced Hill cipher Algorithm”, International Journal of Recent Trends in Engineering, Vol . 1(1), May 2009.

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 done his M.Tech (CSE) from Osmania university, Hyderabad. He is now pursuing his PhD from JNTU, Hyderabad, India, under the supervision of Dr. V.U.K. Sastry in the area of Information Security and Cryptography. He has 10 years of teaching experience and his interest in research area includes, Cryptography, Steganography and Parallel Processing Systems.