A Modified Feistel Cipher Involving Modular Arithmetic Addition and Modular Arithmetic Inverse of a Key Matrix

Dr. V. U. K Sastry
Dean R & D, Dept. of Computer Science and Engineering,
Sreenidhi Institute of Science and Technology,
Hyderabad, India.

K. Anup Kumar
Associate Professor, Dept. of Computer Science and Engg
Sreenidhi Institute of Science and Technology,
Hyderabad, India

Abstract— **In this investigation, we have modified the Feistel cipher by taking the plaintext in the form of a pair of square matrices. Here we have introduced the operation multiplication with the key matrices and the modular arithmetic addition in encryption. The modular arithmetic inverse of the key matrix is introduced in decryption. The cryptanalysis carried out in this paper clearly indicate that this cipher cannot be broken by the brute force attack and the known plaintext attack.**

Keywords- Encryption; Decryption; Key matrix; Modular Arithmetic Inverse.

I. INTRODUCTION

In a recent investigation [1], we have developed a block cipher by modifying the Feistel cipher. In this, we have taken the plaintext (P) in the form of a pair of matrices P_0 and Q_0, and introduced a key matrix (K) as a multiplicant of Q_0 on both its sides. In this analysis the relations governing the encryption and the decryption are given by

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

and

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

Here, multiplication of the key matrix, mod operation and XOR are the fundamental operations in the development of the cipher. The modular arithmetic inverse of the key plays a vital role in the process of the decryption. Here N is a positive integer, chosen appropriately, and n denotes the number of iterations employed in the development of the cipher.

In the present paper, our objective is to develop a block cipher by replacing the XOR operation in the preceding analysis by modular arithmetic addition. The iteration process that will be used in this cipher is expected to offer a strong modification to the plaintext before it becomes finally the cipher text.

Now, we present the plan of the paper. We introduce the development of the cipher, and present the flowcharts and the algorithms, required in this analysis, in section 2. In section 3, we deal with an illustration of the cipher and discuss the avalanche effect, then in section 4 we study the cryptanalysis of the cipher. Finally, in section 5, we mention the computations carried out in this analysis and draw conclusions.

II. DEVELOPMENT OF THE CIPHER

Let us now consider a plaintext P. On using the EBCIDIC code, the plaintext can be written in the form of a matrix which has m rows and 2m columns. This is split into a pair of square matrices P_0 and Q_0, wherein both the matrices are of size m.

The basic equations governing the encryption and the decryption, in the present investigation, assume the form

$$\left.\begin{aligned} P_i &= (K Q_{i-1} K) \bmod N, \\ Q_i &= (P_{i-1} + P_i) \bmod N \end{aligned}\right\} \quad i = 1 \text{ to } n \qquad (2.1)$$

and

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

The flowcharts depicting the encryption and the decryption processes of the cipher are presented in Figures 1and 2.

Here it may be noted that the symbol || is used for placing one matrix adjacent to the other. The corresponding algorithms can be written in the form as shown below.

Algorithm for Encryption

1. Read P, K, n, N
2. P_0 = Left half of P.
3. Q_0 = Right half of P.
4. for i = 1 to n
   begin
   $P_i = (K Q_{i-1} K) \bmod N$
   $Q_i = (P_{i-1} + (K Q_{i-1}K)) \bmod N$
   end
5. $C = P_n \| Q_n$ /* || represents concatenation */
6. Write(C)

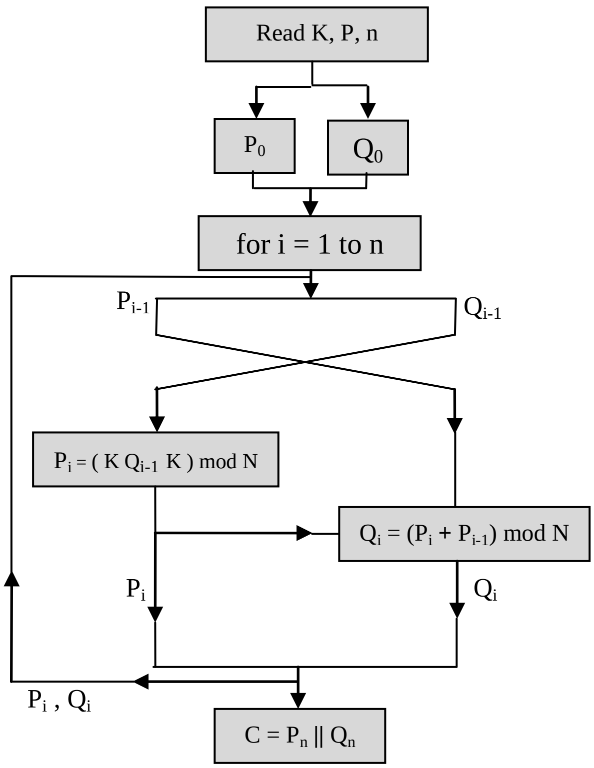

Fig 1. The process of Encryption

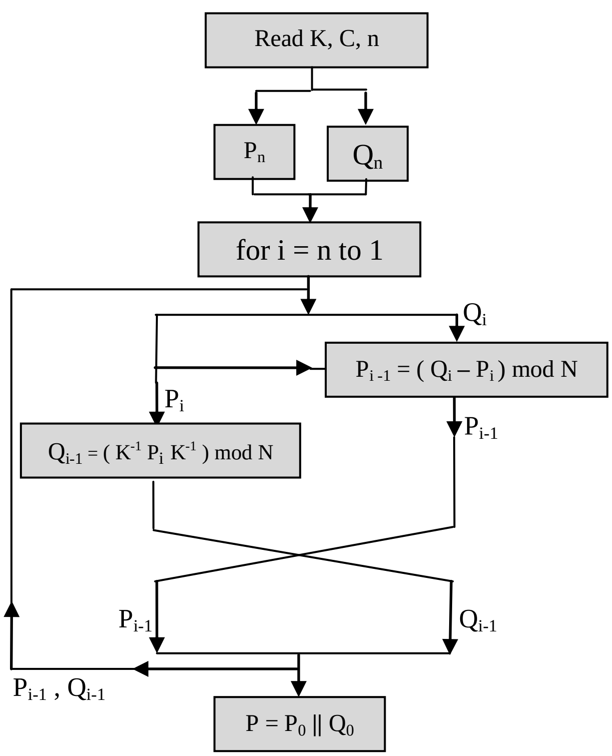

Fig 2. The process of Decryption

Algorithm for Decryption

1. Read C, K, n, N
2. P_n = Left half of C
3. Q_n = Right half of C
4. for i = n to 1

begin

$Q_{i-1} = (K^{-1} P_i K^{-1}) \bmod N$

$P_{i-1} = (Q_i - P_i) \bmod N$

end

5. $P = P_0 \| Q_0$ /* $\|$ represents concatenation */
6. Write (P)

III. ILLUSTRATION OF THE CIPHER

Let us now consider the plain text given below.

Dear Janaki, I have received your letter. You sent me a wonderful cryptography program and a letter along with that. I started working six years back on web security. Really I am finding it very difficult to hit upon an interesting problem. As the complexity of network security is growing in all directions. I am slowly losing my hope; I am thinking now whether I would really contribute in a significant manner and get a Ph.D. Please come and join me, so that, we shall lead a comfortable life. (3.1)

Consider the first 128 characters of the above plaintext. This is given by

Dear Janaki, I have received your letter. You sent me a wonderful cryptography program and a letter along with that. I started w (3.2)

On using the EBCIDIC code we get

$$\begin{bmatrix} 68 & 101 & 97 & 114 & 32 & 74 & 97 & 110 & 97 & 107 & 105 & 44 & 32 & 73 & 32 & 104 \\ 97 & 118 & 101 & 32 & 114 & 101 & 99 & 101 & 105 & 118 & 101 & 100 & 32 & 121 & 111 & 117 \\ 114 & 32 & 108 & 101 & 116 & 116 & 101 & 114 & 46 & 32 & 89 & 111 & 117 & 32 & 115 & 101 \\ 110 & 116 & 32 & 109 & 101 & 32 & 97 & 32 & 119 & 111 & 110 & 100 & 101 & 114 & 102 & 117 \\ 108 & 32 & 99 & 114 & 121 & 112 & 116 & 111 & 103 & 114 & 97 & 112 & 104 & 121 & 32 & 112 \\ 114 & 111 & 103 & 114 & 97 & 109 & 32 & 97 & 110 & 100 & 32 & 97 & 32 & 108 & 101 & 116 \\ 116 & 101 & 114 & 32 & 97 & 108 & 111 & 110 & 103 & 32 & 119 & 105 & 116 & 104 & 32 & 116 \\ 104 & 97 & 116 & 46 & 32 & 73 & 32 & 115 & 116 & 97 & 114 & 116 & 101 & 100 & 32 & 119 \end{bmatrix} \quad (3.3)$$

P can be written in the form

$$P = \quad P_0 = \begin{bmatrix} 68 & 101 & 97 & 114 & 32 & 74 & 97 & 110 \\ 97 & 118 & 101 & 32 & 114 & 101 & 99 & 101 \\ 114 & 32 & 108 & 101 & 116 & 116 & 101 & 114 \\ 110 & 116 & 32 & 109 & 101 & 32 & 97 & 32 \\ 108 & 32 & 99 & 114 & 121 & 112 & 116 & 111 \\ 114 & 111 & 103 & 114 & 97 & 109 & 32 & 97 \\ 116 & 101 & 114 & 32 & 97 & 108 & 111 & 110 \\ 104 & 97 & 116 & 46 & 32 & 73 & 32 & 115 \end{bmatrix} \quad (3.4)$$

and

$$Q_0 = \begin{bmatrix} 97 & 107 & 105 & 44 & 32 & 73 & 32 & 104 \\ 105 & 118 & 101 & 100 & 32 & 121 & 111 & 117 \\ 46 & 32 & 89 & 111 & 117 & 32 & 115 & 101 \\ 119 & 111 & 110 & 100 & 101 & 114 & 102 & 117 \\ 103 & 114 & 97 & 112 & 104 & 121 & 32 & 112 \\ 110 & 100 & 32 & 97 & 32 & 108 & 101 & 116 \\ 103 & 32 & 119 & 105 & 116 & 104 & 32 & 116 \\ 116 & 97 & 114 & 116 & 101 & 100 & 32 & 119 \end{bmatrix} \quad (3.5)$$

Now we take

$$K = \begin{bmatrix} 53 & 62 & 124 & 33 & 49 & 118 & 107 & 43 \\ 45 & 112 & 63 & 29 & 60 & 35 & 58 & 11 \\ 88 & 41 & 46 & 30 & 48 & 32 & 105 & 51 \\ 47 & 99 & 36 & 42 & 112 & 59 & 27 & 61 \\ 57 & 20 & 06 & 31 & 106 & 126 & 22 & 125 \\ 56 & 37 & 113 & 52 & 03 & 54 & 105 & 21 \\ 36 & 40 & 43 & 100 & 119 & 39 & 55 & 94 \\ 14 & 81 & 23 & 50 & 34 & 70 & 07 & 28 \end{bmatrix} \quad (3.6)$$

On using the encryption algorithm, given in section 2, and the key matrix K given by (3.6), we get the cipher text C in the form

$$C = \begin{bmatrix} 171 & 52 & 200 & 66 & 75 & 118 & 174 & 146 & 146 & 70 & 219 & 232 & 147 & 05 & 228 & 153 \\ 219 & 71 & 135 & 111 & 124 & 241 & 1 & 102 & 49 & 181 & 189 & 173 & 118 & 54 & 213 & 177 \\ 105 & 81 & 156 & 242 & 71 & 215 & 198 & 229 & 102 & 250 & 92 & 229 & 191 & 250 & 75 & 21 \\ 102 & 153 & 07 & 111 & 124 & 241 & 01 & 102 & 34 & 120 & 123 & 72 & 231 & 163 & 185 & 48 \\ 225 & 211 & 60 & 192 & 123 & 186 & 119 & 217 & 144 & 231 & 45 & 222 & 228 & 160 & 237 & 239 \\ 146 & 32 & 44 & 192 & 01 & 115 & 110 & 95 & 150 & 150 & 48 & 237 & 165 & 108 & 06 & 173 \\ 245 & 54 & 204 & 145 & 111 & 90 & 186 & 111 & 47 & 145 & 200 & 237 & 59 & 124 & 253 & 241 \\ 146 & 113 & 248 & 95 & 118 & 65 & 54 & 177 & 183 & 71 & 216 & 214 & 199 & 126 & 230 & 49 \end{bmatrix} \quad (3.7)$$

On using the cipher text (3.6) and the decryption algorithm, we get back the original plaintext (3.2)

Now let us study the avalanche effect. To this end, we change 4th row, 2nd column element from 116 to 117 in (3.3). On using this modified plaintext and the encryption algorithm we get the corresponding cipher text in the form

$$C = \begin{bmatrix} 49 & 86 & 105 & 144 & 118 & 247 & 209 & 224 & 146 & 221 & 232 & 156 & 241 & 01 & 102 & 49 \\ 181 & 189 & 173 & 118 & 54 & 213 & 177 & 105 & 81 & 156 & 242 & 71 & 215 & 198 & 229 & 102 \\ 250 & 92 & 229 & 191 & 250 & 75 & 21 & 102 & 153 & 07 & 111 & 124 & 241 & 01 & 102 & 34 \\ 120 & 123 & 72 & 231 & 163 & 185 & 48 & 225 & 211 & 60 & 192 & 123 & 186 & 119 & 217 & 144 \\ 231 & 45 & 222 & 228 & 160 & 237 & 239 & 146 & 32 & 44 & 192 & 01 & 115 & 110 & 95 & 150 \\ 150 & 48 & 237 & 165 & 108 & 06 & 173 & 245 & 54 & 204 & 145 & 111 & 90 & 186 & 111 & 47 \\ 145 & 200 & 237 & 59 & 124 & 253 & 241 & 146 & 113 & 248 & 95 & 118 & 65 & 54 & 177 & 183 \\ 71 & 216 & 214 & 199 & 126 & 230 & 49 & 87 & 73 & 146 & 103 & 100 & 146 & 54 & 222 & 23 \end{bmatrix} \quad (3.8)$$

On comparing (3.7) and (3.8) in their binary form, we notice that they differ by 514 bits out of 1024 bits.

Let us now consider a one bit change in the key. This is achieved by replacing 4th row , 4th column element 42of K by 43 .

Now on using the modified key and the encryption algorithm we get the cipher text C in the form

$$C = \begin{bmatrix} 51 & 145 & 164 & 146 & 108 & 237 & 147 & 173 & 155 & 18 & 82 & 72 & 85 & 155 & 19 & 71 \\ 182 & 102 & 90 & 237 & 150 & 142 & 218 & 60 & 11 & 150 & 219 & 226 & 237 & 177 & 36 & 100 \\ 29 & 189 & 243 & 189 & 173 & 249 & 204 & 211 & 32 & 232 & 175 & 176 & 67 & 93 & 141 & 188 \\ 229 & 191 & 232 & 29 & 183 & 173 & 255 & 124 & 161 & 166 & 246 & 118 & 206 & 121 & 35 & 235 \\ 250 & 182 & 111 & 165 & 66 & 204 & 99 & 105 & 37 & 234 & 64 & 211 & 32 & 48 & 239 & 29 \\ 201 & 135 & 11 & 01 & 179 & 196 & 69 & 249 & 177 & 87 & 71 & 115 & 111 & 135 & 182 & 223 \\ 61 & 50 & 174 & 153 & 231 & 235 & 146 & 127 & 150 & 41 & 53 & 136 & 07 & 187 & 229 & 187 \\ 218 & 92 & 206 & 251 & 60 & 191 & 135 & 184 & 94 & 234 & 109 & 154 & 235 & 72 & 216 & 185 \end{bmatrix} \quad (3.9)$$

On comparing (3.7) and (3.9), after converting them into their binary form, we find that the two cipher texts under consideration differ by 518 bits out of 1024 bits. From the above analysis, we conclude that the cipher is expected to be a strong one.

IV. CRYPTANALYSIS

The different approaches existing for cryptanalysis in the literature are

1. Cipher text only attack(Brute Force Attack)
2. Known plaintext attack
3. Chosen plaintext attack
4. Chosen cipher text attack

In this analysis, the key is a square matrix of size m.

Thus the size of the key space = $(2)^{8m2}$

If we assume that the time required for encryption is 10^{-7} seconds then the time required for the computation with all the keys in the key space [1]

$$= 3.12 \times 10^{(2.4m^2 - 15)} \text{ Years} \quad (4.1)$$

When m = 8 , the time required for the entire computation can be obtained as

$$3.12 \times 10^{138.6} \text{ Years}$$

As this time is very large, the cipher under consideration cannot be broken by the brute force attack. Now let us examine the known plaintext attack. In the case of this attack, we know as many plaintext cipher text pairs as we require. In the light of this fact, we have P_0, Q_0 and P_n, Q_n in as many instances as we want. Keeping the quotations governing the encryption in view (see algorithm for encryption), we can write the following equations connecting the plaintext and the cipher text at different stages of the iteration process.

$P_1 = (K\ Q_0\ \ K) \bmod N$
$Q_1 = (P_0 + (K\ Q_0\ K)) \bmod N$

$P_2 = (K ((P_0 + (K\ Q_0\ K)) \bmod N) K) \bmod N$
$Q_2 = (((K\ Q_0\ \ K) \bmod N) + (K ((P_0 + (K\ Q_0\ K)) \bmod N) K)) \bmod N$

$P_3 = (K ((((K\ Q_0\ \ K) \bmod N) + (K ((P_0 + (K\ Q_0\ K)) \bmod N) K)) \bmod N) K) \bmod N$
$Q_3 = (((K ((P_0 + (K\ Q_0\ K)) \bmod N) K) \bmod N) + (K\ ((((K\ Q_0\ \ K) \bmod N) + (K ((P_0 + (K\ Q_0\ K)) \bmod N) K)) \bmod N) K)) \bmod N$

In view of the above system of equations we can write the entities at the n^{th} stage of the iteration as follows:

$$\left. \begin{aligned} P_n &= F (P_0, Q_0, K, \bmod N), \\ Q_n &= F (P_0, Q_0, K, \bmod N), \end{aligned} \right\} \qquad (4.2)$$

Here it is to be noted that, the initial plaintext can be obtained by concatenating P_0 and Q_0. The cipher text which we get at the end of the iteration by concatenating P_n and Q_n.

Though we have as many relations as we want between the cipher text and the plain text, the key matrix K cannot be determined as the equations (4.2) are nonlinear and involving mod N. In the light of the above discussion, we conclude that this cipher cannot be broken by the known plaintext attack.

In the literature of the cryptography [2], it is well known that a cipher must be designed such that it withstands at least the first two attacks. As the relations given in (4.2) are very complex, it is not possible either to choose a plaintext or to choose a cipher text to attack the cipher. In the light of the afore mentioned facts, we conclude that this cipher is a strong one and it cannot be broken by any means.

V. Computations And Conclusions

In this paper, we have developed a block cipher by modifying the Feistel cipher, in this modification, the plaintext is taken in the form of a matrix of size mx(2m). The iteration process is carried out by dividing this matrix into two equal halves wherein each one is of size mxm. In this analysis, we have used multiplication of a portion of the plaintext (Q_0) with a key matrix on both the sides of Q_0. Here we have made use of modular arithmetic addition as a primary operation in the cipher. The modular arithmetic inverse of the key is used in the decryption process.

Programs are written for encryption and decryption in C language. The entire plaintext given in (3.1) is divided into 4 blocks. Wherein each block contains 128 characters. We have appended the portion of the last block with 15 characters so that it becomes a full block. On carrying out encryption (by using the key and the algorithm for encryption), we get the ciphertext corresponding to the complete plaintext (3.1).

93 182 36 140 131 239 117 164 120 23 185 108 246 130 229 66
73 111 117 219 124 93 182 36 140 131 183 190 119 181 191 57
154 100 29 21 246 8 107 177 183 156 183 253 3 182 245 191
239 148 52 222 206 217 207 36 125 127 86 205 244 168 89 140
109 36 189 72 26 100 6 29 227 185 48 225 96 54 120 136
191 54 42 232 238 109 240 246 219 231 166 85 211 60 253 114
79 242 197 38 177 0 247 124 183 123 75 153 223 103 151 240
247 11 221 77 179 95 103 108 157 23 11 150 226 179 98 14
244 150 126 209 11 27 146 209 224 146 88 220 191 104 132 183
182 207 104 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 3 76 128 195 188 119 38 28 44 6 207
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 30 225 123 169 182 107 236 237 147 162 225 114 220 86 108
65 222 146 253 162 49 185 45 9 58 210 23 184 69 163 193
36 183 186 210 49 123 150 207 104 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 3 76 128 195 188
119 38 28 44 6 207 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 30 225 123 169 182 107 236 237 147
162 225 114 220 86 108 65 222 146 203 27 146 209 224 94 229
179 218 71 237 16 92 182 223 27 223 59 218 223 156 205 50
14 138 251 4 53 216 219 206 91 254 129 219 122 223 247 202
26 111 103 108 231 146 62 191 171 102 250 84 44 198 54 146
94 164 13 50 3 14 241 220 152 112 176 27 60 68 95 155
21 116 119 54 248 123 109 243 211 42 233 158 126 185 39 249
98 147 88 128 123 190 91 189 165 204 239 179 203 248 123 133
238 166 217 175 179 182 78 139 133 203 113 89 177 7 122 75

This cipher has acquired a lot of strength in view of the multiplication with key matrix, the modular arithmetic addition and mod operation. From the cryptanalysis, it is worth noticing that the cipher is a strong one.

References

[1] A modified Feistel cipher involving XOR operation and modular arithmetic inverse of a key matrix (Accepted for publication, IJACSA, Vol 3, No 7)

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

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, 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.