A Novel Feistel Cipher Involving a Bunch of Keys supplemented with Modular Arithmetic Addition

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

Mr. K. Anup Kumar
Associate Professor, Department of Computer Science and Engineering, Sreenidhi Institute of Science & Tech.
Hyderabad, India

Abstract— **In the present investigation, we developed a novel Feistel cipher by dividing the plaintext into a pair of matrices. In the process of encryption, we have used a bunch of keys and modular arithmetic addition. The avalanche effect shows that the cipher is a strong one. The cryptanalysis carried out on this cipher indicates that this cipher cannot be broken by any cryptanalytic attack and it can be used for secured transmission of information.**

Keywords- encryption; decryption; cryptanalysis; avalanche effect; modular arithmetic addition.

I. INTRODUCTION

In the development of block ciphers in cryptography, the study of Feistel cipher and its modifications is a fascinating area of research. In a recent investigation [1], we have developed a novel block cipher by using a bunch of keys, represented in the form of a matrix, wherein each key is having a modular arithmetic inverse. In this analysis, we have seen that the multiplication of different keys with different elements of the plaintext, supplemented with the iteration process, has resulted in a strong block cipher, this fact is seen very clearly by the avalanche effect and the cryptanalysis carried out in this investigation.

In this paper, we have modified the block cipher developed in [1] by replacing the XOR operation with modular arithmetic addition. Here our interest is to study how the modular arithmetic addition influences the iteration process and the permutation process involving in the analysis.

In what follows, we present the plan of the paper. In section 2, we deal with the development of the cipher and introduce the flow charts and the algorithms required in this analysis. We have illustrated the cipher in section 3, and depicted the avalanche effect. Then in section 4, we carry out the cryptanalysis which establishes the strength of the cipher. Finally, we have computed the entire plaintext by using the cipher and have drawn conclusions obtained in this analysis.

Development Of The Cipher

Consider a plaintext containing 2m2 characters. Let us represent this plaintext in the form of a matrix P by using EBCIDIC code. We divide this matrix into two square matrices P0 and Q0, where each one is matrix of size m.

The equations governing this block cipher can be written in the form

$$[\, P_{jk}^{\,i} \,] = [\, e_{jk}\; Q_{jk}^{\,i-1} \,] \bmod 256, \qquad (2.1)$$

and

$$[\, Q_{jk}^{\,i} \,] = ([e_{jk}\, P_{jk}^{\,i-1}] \bmod 256 + [Q_{jk}^{\,i-1}]) \bmod 256\;, \qquad (2.2)$$

where j= 1 to m , k = 1 to m and i =1 to n, in which n is the number of rounds.

the equations describing the decryption are obtained in the form

$$[\, Q_{jk}^{\,i-1} \,] = [\, d_{jk}\, P_{jk}^{\,i} \,] \bmod 256, \qquad (2.3)$$

and

$$[\, P_{jk}^{\,i-1} \,] = [d_{jk}(\,[\, Q_{jk}^{\,i} \,] - [\, Q_{jk}^{\,i-1} \,]\,)\,] \bmod 256 \qquad (2.4)$$

where j= 1 to m , k = 1 to m and i = n to 1,

Here ejk , j = 1 to m and k = 1 to m, are the keys in the encryption process, and djk j = 1 to m and k = 1 to m, are the corresponding keys in the decryption process. The keys ejk and djk are related by the relation

$$(\, e_{jk}\; d_{jk} \,) \bmod 256 = 1, \qquad (2.5)$$

that is, d_{jk} is the multiplicative inverse of the given e_{jk} . Here it is to be noted that both e_{jk} and d_{jk} are odd numbers which are lying in [1-255].

For convenience, we may write

$$E = [\, e_{jk} \,]\;, \quad j = 1 \text{ to } m \text{ and } k = 1 \text{ to } m.$$

and

$$D = [\, d_{jk} \,]\;, \quad j = 1 \text{ to } m \text{ and } k = 1 \text{ to } m.$$

where E and D are called as key bunch matrices.

The flow charts describing the encryption and the decryption processes are given by

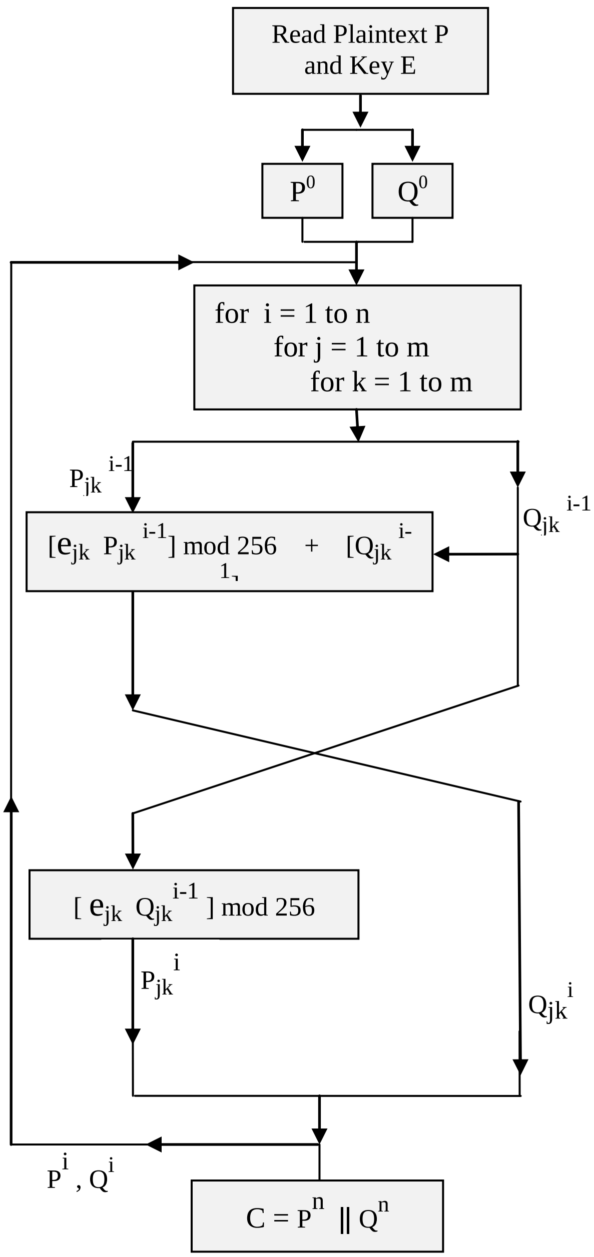

Figure 1. The Process of Encryption

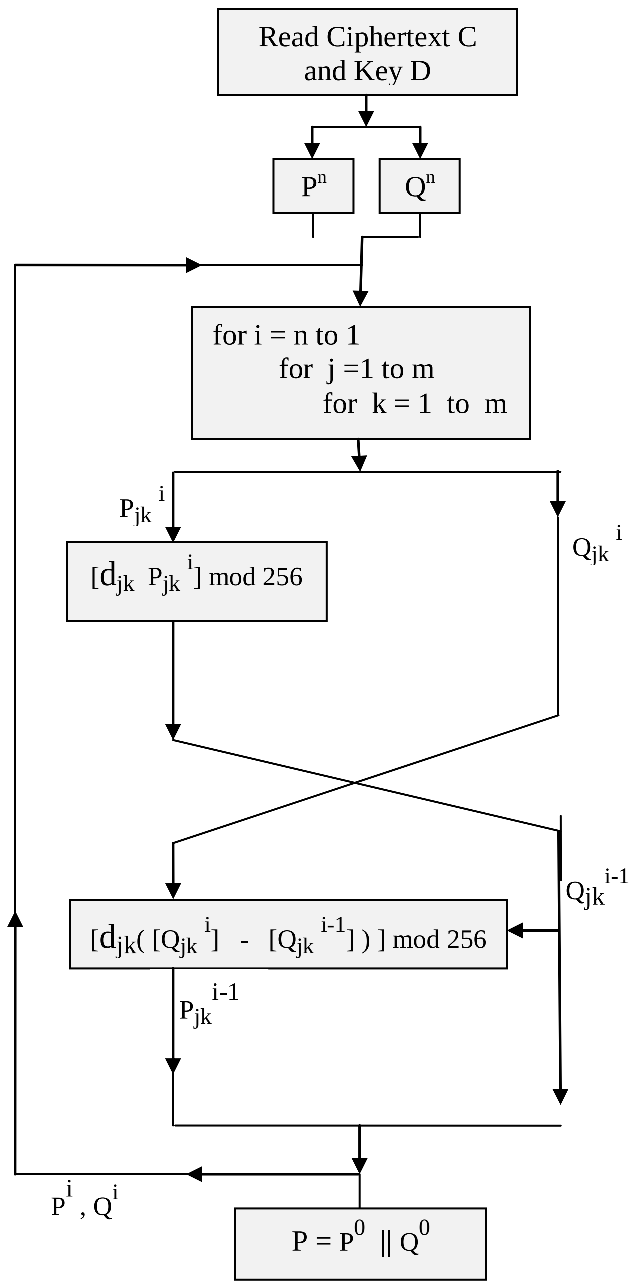

Figure 2. The process of Decryption

The corresponding algorithms are written in the form given below.

A. Algorithm for Encryption

1. Read P, E, and n
2. P^0 = Left half of P.
   Q^0 = Right half of P.
3. for i = 1 to n
   begin
      for j = 1 to m
      begin
         for k = 1 to m
            begin
               $[P_{jk}^{i}] = [e_{jk} Q_{jk}^{i-1}] \bmod 256,$
               $[Q_{jk}^{i}] = [e_{jk} P_{jk}^{i-1}] \bmod 256 + [Q_{jk}^{i-1}],$
            end
      end
   end
6. C = $P^n \| Q^n$ ‖ /* represents concatenation */
7. Write(C)

B. Algorithm for Decryption

1. Read C, D, and n.
2. P^n = Left half of C
   Q^n = Right half of C
3. for i = n to 1
begin
   for j = 1 to m
      begin
         for k = 1 to m
            begin
            $[Q_{jk}^{i-1}] = [d_{jk} P_{jk}^{i}] \bmod 256,$
            $[P_{jk}^{i-1}] = [d_{jk} ([Q_{jk}^{i}] - [Q_{jk}^{i-1}]] \bmod 256$
            end
      end
end
6. P = $P^0 \| Q^0$ /*‖ represents concatenation */
7. Write (P)

II. Illustration Of The Cipher

Consider the plaintext given below

Sister! What a pathetic situation! Father, who joined congress longtime back, he cannot accept our view point. That's how he remains isolated. Eldest brother who have become a communist, having soft corner for poor people, left our house longtime back does not come back to our house! Second brother who joined Telugu Desam party in the time of NTR does not visit us at any time. Our brother in law who is in Bharathiya Janata Party does never come to our house. Mother is very unhappy! (3.1)

Let us focus our attention on the first 32 characters of the above plaintext. This is given by

Plaintext (3.2)

On using the EBCIDIC code, we obtain

$$P = \begin{bmatrix} 083 & 105 & 115 & 116 & 101 & 114 & 033 & 032 \\ 087 & 104 & 097 & 116 & 032 & 097 & 032 & 112 \\ 097 & 116 & 104 & 101 & 116 & 105 & 099 & 032 \\ 115 & 105 & 116 & 117 & 097 & 116 & 105 & 111 \end{bmatrix} \quad (3.3)$$

This can be written in the form

$$P^0 = \begin{bmatrix} 083 & 105 & 115 & 116 \\ 087 & 104 & 097 & 116 \\ 097 & 116 & 104 & 101 \\ 115 & 105 & 116 & 117 \end{bmatrix} \quad (3.4)$$

and

$$Q^0 = \begin{bmatrix} 101 & 114 & 033 & 032 \\ 032 & 097 & 032 & 112 \\ 116 & 105 & 099 & 032 \\ 097 & 116 & 105 & 111 \end{bmatrix} \quad (3.5)$$

Let us now take the key bunch matrix E in the form

$$E = \begin{bmatrix} 125 & 133 & 057 & 063 \\ 005 & 135 & 075 & 015 \\ 027 & 117 & 147 & 047 \\ 059 & 107 & 073 & 119 \end{bmatrix} \quad (3.6)$$

On using the concept of multiplicative inverse, given by the relation (2.5), we get the key bunch matrix D in the form

$$D = \begin{bmatrix} 213 & 077 & 009 & 191 \\ 205 & 055 & 099 & 239 \\ 019 & 221 & 155 & 207 \\ 243 & 067 & 249 & 071 \end{bmatrix} \quad (3.7)$$

On using (3.4) – (3.6) and applying the encryption algorithm, we get the ciphertext C in the form

$$C = \begin{bmatrix} 036 & 138 & 014 & 142 & 000 & 238 & 090 & 106 \\ 110 & 090 & 214 & 104 & 144 & 118 & 246 & 206 \\ 016 & 022 & 098 & 018 & 194 & 218 & 070 & 114 \\ 108 & 120 & 038 & 118 & 208 & 224 & 146 & 196 \end{bmatrix} \quad (3.8)$$

On using the ciphertext C given by (3.8), the key bunch D given by (3.7), and the decryption algorithm given in section 2, we get back the original plaintext.

Now let us consider the avalanche effect which predicts the strength of the cipher.

On changing the fourth row, fourth column element of P0 from 117 to 119, we get a one bit change in the plaintext as the EBCIDIC codes of 117 and 119 are 01110101 and 01110111. On using the modified plaintext and the encryption key bunch matrix E we apply the encryption algorithm, and obtain the corresponding ciphertext in the form

$$C = \begin{bmatrix} 060 & 106 & 182 & 142 & 076 & 198 & 038 & 132 \\ 182 & 196 & 242 & 196 & 000 & 034 & 194 & 240 \\ 140 & 252 & 088 & 140 & 108 & 090 & 146 & 124 \\ 042 & 022 & 094 & 180 & 156 & 250 & 206 & 084 \end{bmatrix} \quad (3.9)$$

On comparing (3.8) and (3.9) in their binary form, we find that these two ciphertext differ by 129 bits out of 256 bits. This shows the strength of the cipher is quite considerable.

Now let us consider the one bit change in the key, On changing second row, third column element of E from 75 to 74, we get a one bit change in the key. On using the modified key, the original plaintext (3.2) and the encryption algorithm, we get the cipher text in the form

$$C = \begin{bmatrix} 242 & 248 & 202 & 122 & 058 & 004 & 036 & 154 \\ 022 & 252 & 002 & 206 & 104 & 098 & 116 & 002 \\ 190 & 108 & 190 & 072 & 250 & 106 & 022 & 200 \\ 044 & 114 & 220 & 222 & 050 & 106 & 030 & 220 \end{bmatrix} \quad (3.10)$$

On comparing (3.8) and (3.10), in their binary form, we find that these two ciphertexts differ by 136 bits out of 256 bits. This also shows that the cipher is expected to be a strong one.

III. CRYPTANALYSIS

In the literature of the cryptography the strength of the cipher is decided by exploring cryptanalytic attacks. The basic cryptanalytic attacks that are available in the literature [2] are

1) *Ciphertext only attack (Brute Force Attack),*
2) *Known plaintext attack,*
3) *Chosen plaintext attack, and*
4) *Chosen ciphertext attack.*

In all the investigations generally we make an attempt to prove that a block cipher sustains the first two cryptanalytic attacks. Further, we make an attempt to intuitively find out how far the later two cases are applicable for breaking a cipher.

As the key E is a square matrix of size m, the size of the key space is

$$2^{(8m^2)} = (2^{10})^{0.8\,m^2} \approx (10^3)^{0.8\,m^2} = (10)^{2.4m^2}$$

If we assume that the time required for the encryption with each key in the key space as 10-7 seconds, then the time required for the execution with all the keys in the key space is

$$\frac{10^{(2.4m^2)} \times 10^{-7}}{365 \times 24 \times 60 \times 60} \text{ years} = 3.12 \times 10^{(2.4\,m^2-15)} \text{ years}$$

In the present analysis, as m=4, the time required is given by 3.12 x 10 23.4 years. As this is a formidable quantity we can readily say that this cipher cannot be broken by the brute force approach.

Let us know examine the strength of the known plaintext attack. If we confine our attention to one round of the iteration process, that is if n = 1, the equations governing the encryption are given by

$$[\,P_{jk}^{\;1}\,] = [\,e_{jk}\,Q_{jk}^{\;0}\,] \bmod 256, \quad (4.1)$$

$$[\,Q_{jk}^{\;1}\,] = [\,e_{jk}\;P_{jk}^{\;0}\,] \bmod 256 + [\,Q_{jk}^{\;0}\,], \quad (4.2)$$

where, j = 1 to m, and k = 1 to m.

and

$$C = P^1 \,\|\, Q^1 . \quad (4.3)$$

In the case of this attack, as C, yielding $P_{jk}^{\;1}$ and $Q_{jk}^{\;1}$ and as P yielding $P_{jk}^{\;0}$ and $Q_{jk}^{\;0}$ are known to the attacker, he can readily determine e_{jk} by using the concept of the multiplicative inverse. Thus let us proceed one step further.

On considering the case corresponding to the second round of the iteration (n = 2), we get the following equations in the encryption process.

$$[\,P_{jk}^{\;1}\,] = [\,e_{jk}\,Q_{jk}^{\;0}\,] \bmod 256, \quad (4.4)$$

and

$$[\,Q_{jk}^{\;1}\,] = [\,e_{jk}\;P_{jk}^{\;0}\,] \bmod 256 + [\,Q_{jk}^{\;0}\,], \quad (4.5)$$

$$[\,P_{jk}^{\;2}\,] = [\,e_{jk}\,Q_{jk}^{\;1}\,] \bmod 256, \quad (4.6)$$

and

$$[\,Q_{jk}^{\;2}\,] = [\,e_{jk}\;P_{jk}^{\;1}\,] \bmod 256 + [\,Q_{jk}^{\;1}\,], \quad (4.7)$$

where, j = 1 to m and k = 1 to m.

Further we have,

$$C = P^2 \,\|\, Q^2 . \quad (4.8)$$

Here P_{jk}^{0} and Q_{jk}^{0} are known to us, as C is known. We also know P_{jk}^{0} and Q_{jk}^{0} as this is the known plaintext attack. But here, we cannot know P_{jk}^{1} and Q_{jk}^{1} either from the forward side or from the backward side. Thus e_{jk} cannot be determined by any means, and hence this cipher cannot be broken by the known plaintext attack.

As the equations governing the encryption are complex, it is not possible to intuitively either a plaintext or a ciphertext and attack the cipher. Thus the cipher cannot be broken by the last two cases too. Hence we conclude that this cipher is a very strong one.

IV. Computations And Conclusions

In this investigation we have developed a block cipher by modifying the Feistel cipher. In this analysis the modular arithmetic addition plays a fundamental role. The key bunch encryption matrix E and the key bunch decryption matrix D play a vital role in the development of the cipher. The computations involved in this analysis are carried out by writing programs in C language.

On taking the entire plaintext (3.1) into consideration, we have divided it into 14 number of blocks. In the last block, we have included 26 blanks characters to make it a complete block. On taking the encryption key bunch E and carrying out the encryption of the entire plaintext, by applying encryption algorithm given in section 2, we get the ciphertext C in the form given below

128	100	202	018	120	154	146	058	148	244	200	026	152	198	056	176
086	066	184	182	192	178	146	236	224	058	082	198	078	218	060	236
176	156	224	178	070	200	014	090	078	252	230	042	180	108	090	084
102	060	144	244	240	184	088	190	150	056	110	254	146	222	006	206
074	182	128	236	074	024	058	104	242	182	024	140	078	012	184	126
090	088	194	182	170	096	054	122	058	146	014	028	050	204	036	138
178	076	130	182	130	028	228	184	146	044	238	056	250	176	224	136
128	188	188	046	074	076	100	182	014	222	050	134	178	214	228	230
044	254	210	094	076	0 98	216	036	098	236	238	072	254	090	234	108
172	022	198	146	028	182	054	140	154	134	182	054	034	182	054	240
102	048	180	110	076	244	178	014	222	248	226	00 2	204	098	106	122
090	236	108	170	052	200	058	122	098	026	090	218	242	196	004	106
176	182	172	138	074	140	230	146	214	198	228	102	250	112	086	104
124	240	000	246	144	220	116	046	126	250	108	222	206	202	250	048
000	246	116	238	178	244	134	228	058	206	108	190	144	044	152	098
078	050	114	102	082	190	152	00 2	0 82	024	198	054	042	232	118	054
140	198	038	134	220	190	044	044	096	218	084	176	026	060	028	200
134	014	152	230	146	196	088	166	064	218	192	014	114	220	200	022
246	156	252	216	240	196	064	094	222	150	036	038	050	218	006	110
152	194	216	234	114	114	150	254	232	046	166	176	108	146	176	118
246	036	254	044	244	054	214	138	098	072	142	090	154	198	076	066
218	154	144	090	026	248	178	024	218	182	038	250	088	006	110	124
240	000	102	048	180	188	172	118	054	212	176	104	080	156	242	070
214	198	228	102	250	092	228	190	250	074	020	102	152	006	110	076
098	106	122	126	120	128	172	118	054	212	176	104	080	156	242	122
248	220	172	222	078	042	204	046	158	032	030	210	058	174	164	206
222	076	154	216	216	094	102	032	030	238	156	246	126	144	252	134
120	236	182	214	050	156	022	072	248	032	234	072	222	188	228	121

In this we have excluded the ciphertext which is already presented in (3.8)

In the light of this analysis, here we conclude that this cipher is an interesting one and a strong one, and this can be used for the transmission of any information through internet.

References

[1] V.U.K Sastry and K. Anup Kumar " A Novel Feistel Cipher Involving a bunch of Keys Supplemented with XOR Operation" (IJACSA) International Journal of Advanced Computer Science and Applications, 2012.

[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 andWorked in IIT, Kharagpurduring 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.