A Novel Feistel Cipher Involving a Bunch of Keys Supplemented with XOR Operation

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

K. Anup Kumar
Associate Professor, Department of Computer Science and Engineering, SNIST,
Hyderabad, India

***Abstract*—In this investigation, we have developed a novel block cipher by modifying classical Feistel cipher. In this, we have used a key bunched wherein each key has a multiplicative inverse. The cryptanalysis carried out in this investigation clearly shows that this cipher cannot be broken by any attack.**

Keywords-encryption; decryption; cryptanalysis; avalanche effect; multiplicative inverse.

I. INTRODUCTION

The study of the Feistel cipher [1-2] laid the foundation for the development of cryptography in the seventies of the last century. In the classical Feistel cipher the block size is 64 bits, and it is divided into two halves wherein each half is containing 32 bits. The number of rounds in the iteration process is 16. The basic equations governing the Feistel cipher can be written in the form

$$P^i = Q^{i-1}, \quad (1.1)$$

$$Q^i = P^{i-1} \oplus F(Q^{i-1}, K^i), \quad (1.2)$$

and

$$Q^{i-1} = P^i, \quad (1.3)$$

$$P^{i-1} = Q^i \oplus F(P^i, K^i), \quad (1.4)$$

where P^i and Q^i are the blocks of the plaintext in the i^{th} round of the iteration process, F is a function chosen appropriately, and K^i is the key in the i^{th} round. In this analysis, the XOR operation and the permutation that is performed by interchanging two halves of the data in the iteration process play a vital role in deciding the strength of the cipher.

In the recent years, Sastry et al. [3-12] have offered several modifications to the Feistel cipher, and have studied various aspects of this cipher, including different types of permutations and substitutions. In all these investigations we have divided the plaintext into a pair of matrices of equal size, and the key is taken in the form of a matrix.

In the process of encryption, we take the key bunch as E, and represent it in the form of a matrix given by $E = [e_{jk}]$. The corresponding key bunch in the process of decryption is taken as $D = [d_{jk}]$. Here for a given value of the key e_{jk}, used in the encryption, we determine the corresponding key d_{jk}, by using the relation

$$(e_{jk} \times d_{jk}) \bmod 256 = 1, \quad (1.5)$$

where d_{kl} is the multiplicative inverse of e_{kl},

In order to satisfy (1.5), we chose e_{jk} as an odd integer, which lies in the interval [1-255], and thus we obtain d_{jk} also as an odd integer lying in the interval [1-255].

Here also we adopt an iterative procedure, and make use of the permutation process that consists of the interchange of the two halves of the plaintext , of course, represented in the form of a pair of matrices.

In the present analysis, our objective is to modify the Feistel cipher by including a bunch of keys. Here our interest is to see how the different keys, occurring in the key bunch, would influence the strength of the cipher.

In what follows, we present the plan of the paper. In section 2, we introduce the development of the cipher and present the flowcharts and the algorithms corresponding to the cipher, in section 3, we illustrate the cipher with an example and examine the avalanche effect. After that, we carry out the cryptanalysis in section 4. Finally we present numerical computation and draw conclusions.

II. DEVELOPMENT OF THE CIPHER

We consider a plaintext P containing $2m^2$ characters. On using the EBCIDIC code this is written in terms of numbers which are in the interval [0-255]. Now we write this in the form of a pair of square matrices P^0 and Q^0, wherein each matrix is of size m.

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

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

and

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

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

The corresponding equations of decryption are in the form,

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

and

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

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

here P_{jk}^{i} and Q_{jk}^{i} are the j^{th} row k^{th} column elements of the left and right portions of the plaintext matrix, respectively, in the i^{th} round of the iteration process.

On using the basic relations (2.1) - (2.4), governing the encryption and the decryption, the corresponding flowcharts for the encryption and the decryption can be written as shown below.

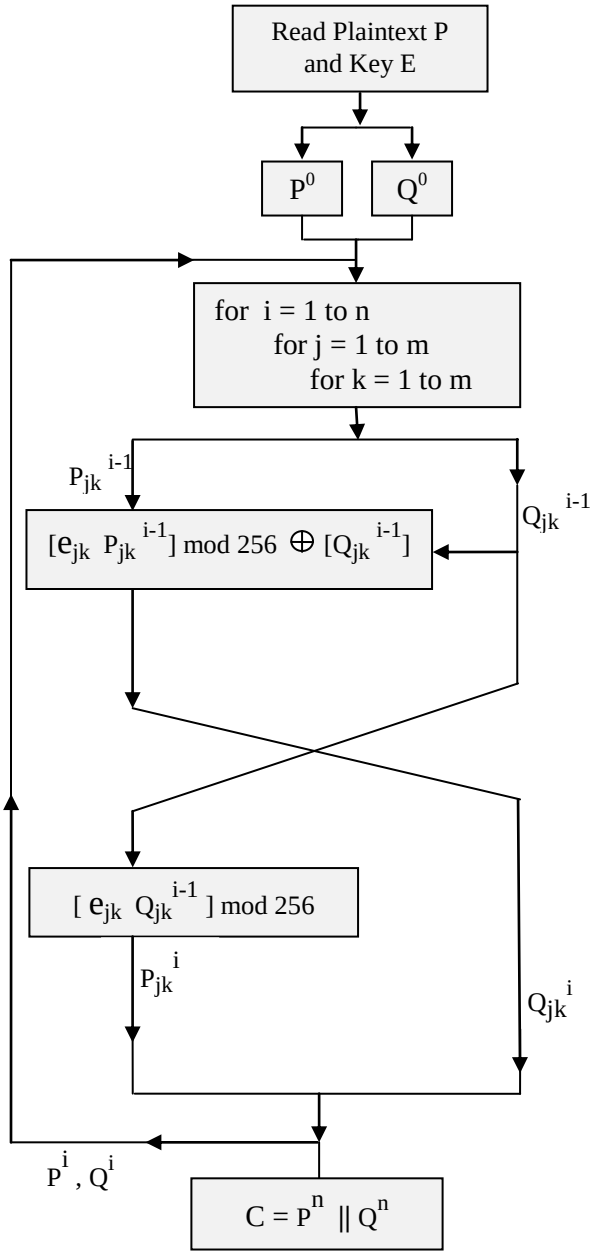

Figure 1. The Process of Encryption

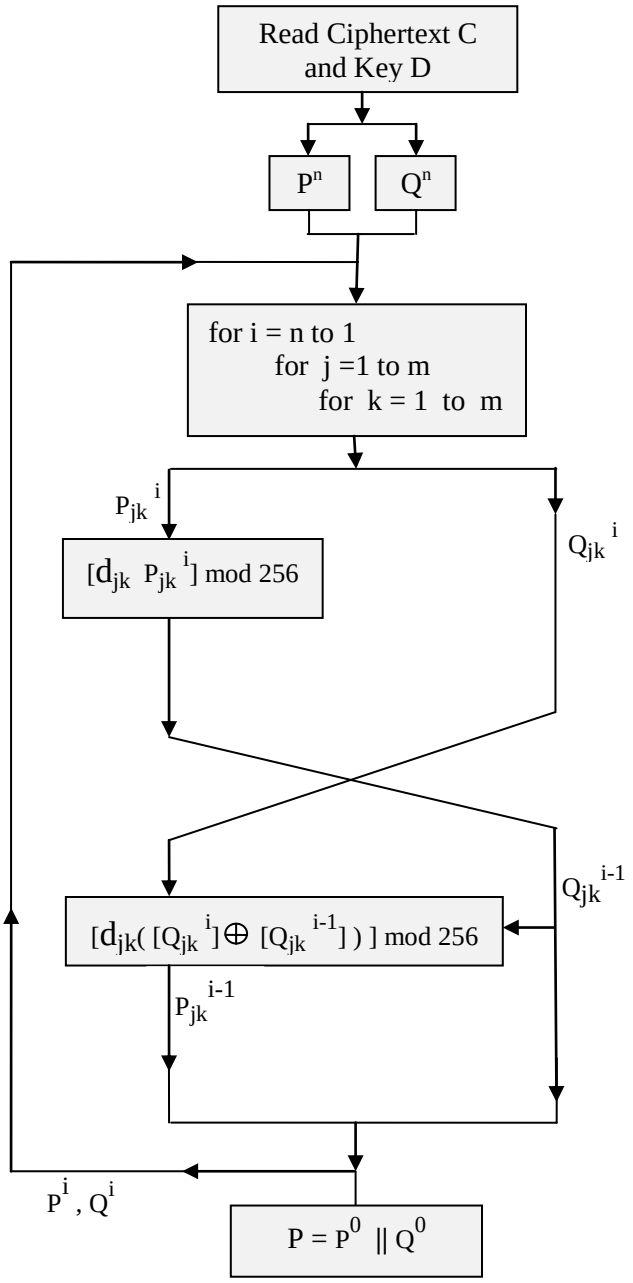

Figure 2. The process of Decryption

The algorithms for the encryption and the decryption are written as shown 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
$[P_{jk}^{i}] = [e_{jk} Q_{jk}^{i-1}] \bmod 256$,
$[Q_{jk}^{i}] = [e_{jk} P_{jk}^{i-1}] \bmod 256 \oplus [Q_{jk}^{i-1}]$,
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
$[Q_{jk}^{i-1}] = [d_{jk} P_{jk}^{i}] \bmod 256$,
$[P_{jk}^{i-1}] = [d_{jk} ([Q_{jk}^{i}] \oplus [Q_{jk}^{i-1}]] \bmod 256$
end
end
end
6. $P = P^0 \| Q^0$ /* || represents concatenation */
7. Write (P)

In what follows we illustrate the cipher with a suitable example.

III. Illustration Of The Cipher

Consider the plaintext given below.

Brother! When we were very poor, by looking at some corrupt politicians and employees who earned crores and crores, we use to think how to come up in life. Though you were a graduate having technical skills, you joined naxalites thinking that only unethical rich are totally responsible for the ruination of our country. After the death of our father, I joined as a police, our uncle started liquor business! He has earned crores and crores. Though I have become a police inspector, I am helpless. I am not able to control anything! I do not know when India will change! Write a letter. Do come back. (3.1)

Let us focus our attention on the first 32 characters of the plaintext (3.1). This is given by

Brother! When we were very poor, (3.2)

On using EBCIDIC code, we write (3.2) in the form of a pair of square matrices given by

$$P^0 = \begin{bmatrix} 066 & 114 & 111 & 116 \\ 032 & 087 & 104 & 101 \\ 032 & 119 & 101 & 114 \\ 114 & 121 & 032 & 112 \end{bmatrix} \quad (3.3)$$

and

$$Q^0 = \begin{bmatrix} 104 & 101 & 114 & 033 \\ 110 & 032 & 119 & 101 \\ 101 & 032 & 118 & 101 \\ 111 & 111 & 114 & 044 \end{bmatrix} \quad (3.4)$$

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

$$E = \begin{bmatrix} 071 & 053 & 011 & 061 \\ 117 & 069 & 057 & 051 \\ 121 & 139 & 101 & 043 \\ 099 & 095 & 111 & 035 \end{bmatrix} \quad (3.5)$$

and

$$D = \begin{bmatrix} 119 & 029 & 163 & 021 \\ 221 & 141 & 009 & 251 \\ 201 & 035 & 109 & 131 \\ 075 & 159 & 143 & 139 \end{bmatrix} \quad (3.6)$$

On using the algorithm for encryption, given in section 2, we get the ciphertext C in the form

$$C = \begin{bmatrix} 088 & 166 & 064 & 218 & 222 & 060 & 064 & 088 \\ 140 & 078 & 014 & 104 & 028 & 204 & 176 & 036 \\ 088 & 094 & 002 & 182 & 244 & 188 & 202 & 108 \\ 240 & 120 & 038 & 118 & 208 & 224 & 146 & 196 \end{bmatrix} \quad (3.7)$$

On using the keys in D, and applying the decryption algorithm on (3.6), we get back the original plaintext P given by (3.2)

Let us now study the avalanche effect. On changing the first row , second column element of P_0 from 114 to 115, we get a change of one binary bit in the plaintext.

On applying the encryption algorithm on this modified plaintext, using the same key bunch matrix E, we get the ciphertext C in the form

$$C = \begin{bmatrix} 104 & 144 & 028 & 204 & 176 & 122 & 222 & 228 \\ 172 & 244 & 236 & 162 & 210 & 024 & 158 & 030 \\ 214 & 206 & 016 & 004 & 144 & 096 & 120 & 014 \\ 218 & 218 & 226 & 242 & 076 & 036 & 176 & 086 \end{bmatrix} \quad (3.8)$$

On converting (3.6) and (3.8) into their binary form and comparing them, we notice that these two ciphertext differ by 133 bits out of 256 bits. This shows that the strength of the cipher is quite up to the mark.

Now let us consider one bit change in the key bunch matrix E. On replacing first row , second column element of E from 53 to 52, we have a one bit change in the key matrix. On using the original plaintext (3.2) and the modified key bunch matrix, and the algorithm for encryption, given in section 2, we get the ciphertext C in the form

$$C = \begin{bmatrix} 246 & 150 & 038 & 080 & 058 & 246 & 202 & 246 \\ 190 & 170 & 220 & 124 & 038 & 238 & 178 & 202 \\ 230 & 040 & 236 & 250 & 004 & 036 & 154 & 022 \\ 224 & 122 & 166 & 216 & 146 & 218 & 182 & 238 \end{bmatrix} \quad (3.9)$$

On comparing (3.6) and (3.9), in their binary form, we find that two ciphertext matrices differ by 127 bits out of 256 bits. This also shows that the block cipher under consideration is a potential one.

IV. CRYPTANALYSIS

The different types of cryptanalytic attacks that are well known in the literature of cryptography [13] are

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

Generally all the algorithms are designed to withstand the brute force attack and the known plaintext attack. Further, an algorithm is examined, intuitively, whether it withstands the later two attacks or not.

In this analysis, the key bunch is a square matrix containing m2 elements. In view of this fact, 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 encryption with each key in the key space as 10-7 seconds, then the time required for all the keys in the key space is approximately equal to

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

In this analysis, we have taken m=4. Thus the time required is $3.12 \times 10^{23.4}$ years.

As this time is very large, we cannot break the cipher by the brute force attack.

Let us now consider the known plaintext attack. If we confine our attention only to one round of the iteration process, that is when n=1, from the encryption algorithm given in section 2, we get

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

and

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

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

Further we have,

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

In the known plaintext attack, the attacker knows the plaintext and the corresponding ciphertext. Thus he knows P_{jk}^{1} and Q_{jk}^{1} occurring in (4.3) and, P_{jk}^{0} and Q_{jk}^{0} occurring in (4.1) and (4.2). in the light of this fact on obtaining the multiplicative inverse of Q_{jk}^{0} (selecting Q_{jk}^{0} as odd numbers) occurring in (4.1), the attacker can determine e_{jk} very conveniently. Thus the cipher can be broken when n=1.

Let us known consider the case when n=2. In this case, the equations governing the encryption are of the form

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

and

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

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

and

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

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

Further we have,

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

As C is known, the attacker knows P_{jk}^{2} and Q_{jk}^{2}. The attacker also knows P_{jk}^{0} and Q_{jk}^{0} occurring in (4.4) and (4.5) as this is the known plaintext attack. Thus the attacker cannot determine the keys e_{jk} occurring in (4.4) as P_{jk}^{1} cannot be determined by any means.

In the light of aforementioned fact, this cipher having sixteen rounds (n=16) cannot be broken by the known plaintext attack.

On inspecting the above equations arising in this analysis, we find that it is simply impossible to choose plaintext or

ciphertext, intuitively, and break the cipher in any way. Thus we conclude that this cipher is a strong one.

V. Computations And Conclusions

In this investigation, we have developed a block cipher by selecting a bunch of keys wherein each key has its multiplicative inverse.

The programs for the encryption and the decryption are written in C language.

Let us now consider the entire plaintext given by (3.1). This can be divided into 19 blocks wherein each block is having 32 characters. As the last block is containing 24 characters, we append 8 blank characters. On using the key bunch E, given by (3.5), and carrying out the encryption process given in section 2, we get the ciphertext (excluding the portion which is already given by (3.6)), we get

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	070	214	198	228	102	250	092	228	190	250	074
020	102	150	206	016	014	104	028	214	098	018	194	110	094	150	150
048	236	170	216	012	158	142	228	194	134	076	242	072	098	172	210
032	236	224	134	056	110	246	036	254	044	244	054	204	144	110	120
206	222	082	230	238	166	204	236	236	174	178	016	014	118	078	250
062	072	126	066	188	246	218	232	002	200	150	036	242	054	038	116
042	232	144	052	048	140	114	098	174	134	114	110	130	102	036	142
012	068	004	236	232	114	082	086	138	098	072	140	182	192	218	230
112	246	122	220	156	188	006	106	088	200	218	070	156	182	050	156
022	072	248	034	232	172	090	036	172	092	122	210	118	238	056	222
230	044	254	210	094	076	098	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	002	204	098	106
122	090	236	108	170	098	210	162	056	228	142	174	140	202	204	244
184	202	126	244	150	042	204	050	014	222	152	198	214	246	252	240
000	090	236	108	170	098	210	162	056	228	142	174	140	202	204	244
226	172	210	248	226	000	236	034	018	204	098	120	108	202	242	210
198	028	180	090	000	178	208	220	152	112	232	158	104	044	084	154
100	028	188	016	230	044	204	144	110	120	206	222	082	230	238	166
204	236	236	174	178	016	014	118	078	250	062	072	126	066	188	246
218	232	002	200	150	036	242	054	038	116	042	232	144	052	048	140
114	0 98	174	134	114	110	130	102	036	142	012	068	004	236	232	114
082	098	044	176	118	248	156	060	158	182	038	110	000	218	150	050
118	208	230	108	140	230	004	146	062	072	122	210	118	238	056	032
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	098	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	002	204	098	106	122	090	236	108	170	098	210	162	056	228	142
174	140	202	204	244	184	202	126	244	150	042	204	050	014	222	152
198	214	246	252	240	000	090	236	108	170	098	210	162	056	228	244
240	184	088	190	156	084	154	094	060	064	060	164	118	092	074	158

From the above analysis we conclude that the novel Feistel cipher, wherein we have made use of a bunch of keys is a strong one as the cryptanalysis shows that it cannot be broken by any attack. This is all on account of the iteration process and the multiplication by the bunch of keys.

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] V.U.K. Sastry and 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", International Journal of Computer Technology and Applications, ISSN 2229-6093,Vol 3 (1), pp, 23-31 , 2012.

[4] V.U.K. Sastry and 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", International Journal of Computer Technology and Applications, ISSN 2229-6093,Vol 3 (1), pp, 32-39 , 2012.

[5] V.U.K. Sastry and 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", International Journal of Computer Science and Information Technologies ISSN 0975 – 9646. Vol. 3 (1) , 2012, pp, 3133 – 3141,2012.

[6] V.U.K. Sastry and K. Anup Kumar, "A Modified Feistel Cipher involving a pair of key matrices, Supplemented with Modular Arithmetic Addition and Shuffling of the plaintext in each round of the iteration process", International Journal of Computer Science and Information Technologies ISSN 0975 – 9646. Vol. 3 (1) , 2012, pp, 3119 – 3128,2012.

[7] V.U.K Sastry and K. Anup Kumar, "A Modified Feistel Cipher Involving XOR Operation and Modular Arithmetic Inverse of a Key Matrix" International Journal of Advanced Computer Science and Applications ISSN : 2156-5570(Online), pp.35-39 , Vol.3 No.7. 2012, U.S.A

[8] V.U.K Sastry and K. Anup Kumar, "A Modified Feistel Cipher Involving Modular Arithmetic Addition and Modular Arithmetic Inverse of a Key Matrix" International Journal of Advanced Computer Science and Applications ISSN : 2156-5570(Online),pp. 40-43, Vol.3 No.7, 2012, U.S.A.

[9] V.U.K Sastry and K. Anup Kumar, "A Modified Feistel Cipher Involving Substitution, Shifting of rows, Mixing of columns, XOR operation with a Key and Shuffling" International Journal of Advanced Computer Science and Applications ISSN : 2156-5570(Online), pp. 23-29, Vol.3 No.8, 2012, U.S.A.

[10] V.U.K Sastry and K. Anup Kumar, "A Modified Feistel Cipher Involving Key Based Substitution, Shifting of rows, Key Based Mixing of columns, Modular Arithmetic Addition and Shuffling "International Journal of Engineering Research and Applications (IJERA) ISSN : 2248-9622 (Online), Vol. 2 , No. 5, pp 237-245, 2012.

[11] V.U.K Sastry and K. Anup Kumar, "A Block Cipher Obtained by Blending Modified Feistel Cipher and Advanced Hill Cipher Involving a Single Key Matrix International Journal of Engineering Research and Applications (IJERA) ISSN : 2248-9622 (Online), Vol. 2 , No. 5, pp 951-958, 2012.

[12] V.U.K Sastry and K. Anup Kumar, "A Block Cipher Obtained by Blending Modified Feistel Cipher and Advanced Hill Cipher Involving a Pair of Key Matrices International Journal of Engineering Research and Applications (IJERA) ISSN : 2248-9622 (Online), Vol. 2 , No. 5, pp 959-964, 2012.

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