A Modified Feistel Cipher Involving XOR Operation 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 paper, we have developed a block cipher by modifying the Feistel cipher. In this, the plaintext is taken in the form of a pair of matrices. In one of the relations of encryption the plaintext is multiplied with the key matrix on both the sides. Consequently, we use the modular arithmetic inverse of the key matrix in the process of decryption. The cryptanalysis carried out in this investigation, clearly indicates that the cipher is a strong one, and it cannot be broken by any attack.**

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

I. INTRODUCTION

In a recent development, we have offered several modifications [1-4] to the classical Feistel cipher, in which the plaintext is a string containing 64 binary bits.

In all the afore mentioned investigations, we have modified the Feistel cipher by taking the plaintext in the form of a matrix of size mx(2m),where each element can be represented in the form of 8 binary bits. This matrix is divided into two halves, wherein each portion is a square matrix of size m. In the first modification [1], we have made use of the operations mod and XOR, and introduced the concepts mixing and permutation. In the second one [2], we have used modular arithmetic addition and mod operation, along with mixing and permutation. In the third one [3], we have introduced the operations mod and XOR together with a process called blending. In the fourth one [4], we have used mod operation, modular arithmetic addition and the process of shuffling. In each one of the ciphers, on carrying out cryptanalysis, we have concluded that the strength of the cipher, obtained with the help of the modification, is quite significant. The strength is increased, on account of the length of the plaintext and the operations carried out in these investigations.

In the present investigation, our interest is to develop a modification of the Feistel cipher, wherein we include the modular arithmetic inverse of a key matrix. This is expected to offer high strength to the cipher, as the encryption key induces a significant amount of confusion into the cipher, on account of the relationship between the plaintext and the cipher text offered by the key, as it does in the case of the Hill cipher.

In what follows we present the plan of the paper. In section 2, we discuss the development of the cipher and mention the flowcharts and the algorithms required in the development of the cipher. In section 3, we illustrate the cipher with an example. Here we discuss the avalanche effect which throws light on the strength of the cipher. We examine the cryptanalysis in section 4. Finally, we present computations and conclusions in section 5.

II. DEVELOPMENT OF THE CIPHER

Consider a plaintext P having $2m^2$ characters. On using EBCIDIC code, this can be written in the form of a matrix containing m rows and 2m columns, where m is a positive integer. This matrix is divided into a pair of square matrices P_0 and Q_0 , where each square matrix is of size m. Let us consider a key matrix K whose size is m x m.

The basic relations governing the encryption and the decryption of the cipher, under consideration, can be written in the form

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

and

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

where, P_i and Q_i are the plaintext matrices in the i^{th} iteration, K the key matrix, N is a positive integer, chosen appropriately, and K^{-1} is the modular arithmetic inverse of K. Here, n denotes the number of iterations that will be carried out in the development of the cipher.

The flow charts governing the encryption and the decryption are depicted in Figures 1 and 2 respectively.

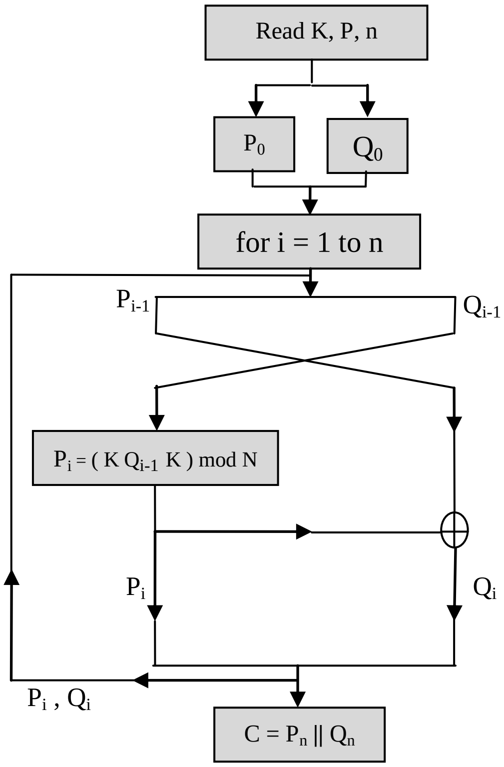

Fig 1. The process of Encryption

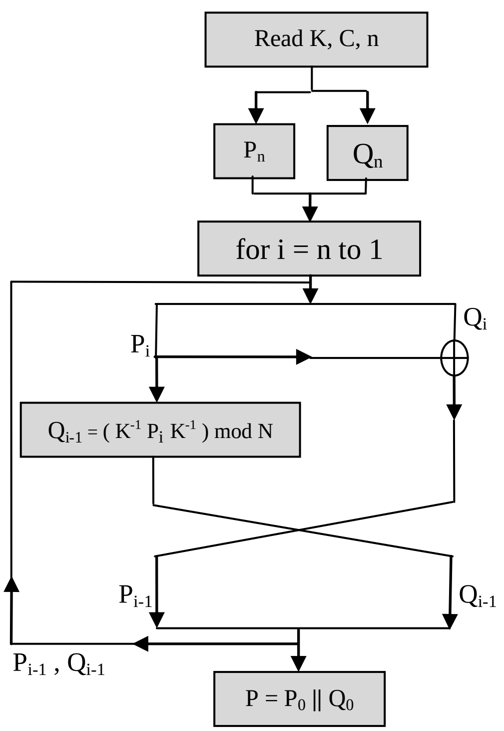

Fig 2. The process of Decryption

The algorithms corresponding to the flow charts can be written as

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

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

5. $C = \| P_n \ Q_n \|$ /* represents concatenation */
6. Write(C)

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

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

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

end

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

The modular arithmetic inverse of the key matrix K is obtained by adopting Gauss Jordan Elimination method [5] and the concept of the modular arithmetic.

III. ILLUSTRATION OF THE CIPPHER

Consider the plaintext given below:

Dear Ramachandra! When you were leaving this country for higher education I thought that you would come back to India in a span of 5 or 6 years. At that time, that is, when you were departing I was doing B.Tech 1st year. There in America, you joined in Ph.D program of course after doing M.S. I have completed my B.Tech and M.Tech, and I have been waiting for your arrival. I do not know when you are going to complete your Ph.D. Thank God, shall I come over there? I do wait for your reply. Yours, Janaki. (3.1)

Let us focus our attention on the first 128 characters of the above plain text. This is given by

Dear Ramachandra! When you were leaving this country for higher education I thought that you would come back to India in a span (3.2)

On using EBCIDIC code, (3.2) can be written in the form of a matrix having 8 rows and 16 columns. This is given by

$$P=\begin{bmatrix} 68 & 101 & 97 & 114 & 32 & 82 & 97 & 109 & 97 & 99 & 104 & 97 & 110 & 100 & 114 & 97 \\ 33 & 32 & 87 & 104 & 101 & 110 & 32 & 121 & 111 & 117 & 32 & 119 & 101 & 114 & 101 & 32 \\ 108 & 101 & 97 & 118 & 105 & 110 & 103 & 32 & 116 & 104 & 105 & 115 & 32 & 99 & 111 & 117 \\ 110 & 116 & 114 & 121 & 32 & 102 & 111 & 114 & 32 & 104 & 105 & 103 & 104 & 101 & 114 & 32 \\ 101 & 100 & 117 & 99 & 97 & 116 & 105 & 111 & 110 & 32 & 73 & 32 & 116 & 104 & 111 & 117 \\ 103 & 104 & 116 & 32 & 116 & 104 & 97 & 116 & 32 & 121 & 111 & 117 & 32 & 119 & 111 & 117 \\ 108 & 100 & 32 & 99 & 111 & 109 & 101 & 32 & 98 & 97 & 99 & 107 & 32 & 116 & 111 & 32 \\ 73 & 110 & 100 & 105 & 97 & 32 & 105 & 110 & 32 & 97 & 32 & 115 & 112 & 97 & 110 & 32 \end{bmatrix} \quad (3.3)$$

Now (3.3) can be written in the form of a pair of square matrices given by

$$P_0=\begin{bmatrix} 68 & 101 & 97 & 114 & 32 & 82 & 97 & 109 \\ 33 & 32 & 87 & 104 & 101 & 110 & 32 & 121 \\ 108 & 101 & 97 & 118 & 105 & 110 & 103 & 32 \\ 110 & 116 & 114 & 121 & 32 & 102 & 111 & 114 \\ 101 & 100 & 117 & 99 & 97 & 116 & 105 & 111 \\ 103 & 104 & 116 & 32 & 116 & 104 & 97 & 116 \\ 108 & 100 & 32 & 99 & 111 & 109 & 101 & 32 \\ 73 & 110 & 100 & 105 & 97 & 32 & 105 & 110 \end{bmatrix} \quad (3.4)$$

and

$$Q_0=\begin{bmatrix} 97 & 99 & 104 & 97 & 110 & 100 & 114 & 97 \\ 111 & 117 & 32 & 119 & 101 & 114 & 101 & 32 \\ 116 & 104 & 105 & 115 & 32 & 99 & 111 & 117 \\ 32 & 104 & 105 & 103 & 104 & 101 & 114 & 32 \\ 110 & 32 & 73 & 32 & 116 & 104 & 111 & 117 \\ 32 & 121 & 111 & 117 & 32 & 119 & 111 & 117 \\ 98 & 97 & 99 & 107 & 32 & 116 & 111 & 32 \\ 32 & 97 & 32 & 115 & 112 & 97 & 110 & 32 \end{bmatrix} \quad (3.5)$$

Let us take the key matrix K in the form

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

On using the encryption algorithm mentioned in section 2, we get

$$C=\begin{bmatrix} 47 & 36 & 206 & 218 & 60 & 59 & 123 & 231 & 136 & 21 & 102 & 153 & 8 & 73 & 110 & 244 \\ 73 & 133 & 152 & 198 & 214 & 246 & 181 & 216 & 219 & 86 & 197 & 165 & 70 & 115 & 201 & 31 \\ 95 & 27 & 149 & 155 & 233 & 115 & 150 & 255 & 233 & 44 & 85 & 154 & 100 & 29 & 189 & 243 \\ 196 & 5 & 152 & 137 & 225 & 237 & 35 & 158 & 142 & 228 & 195 & 135 & 76 & 243 & 1 & 238 \\ 233 & 223 & 102 & 67 & 156 & 183 & 123 & 146 & 131 & 183 & 190 & 72 & 128 & 179 & 0 & 5 \\ 205 & 185 & 126 & 90 & 88 & 195 & 182 & 149 & 176 & 26 & 183 & 212 & 219 & 50 & 69 & 189 \\ 106 & 233 & 188 & 190 & 71 & 35 & 180 & 237 & 243 & 247 & 198 & 73 & 199 & 225 & 125 & 217 \\ 4 & 218 & 198 & 221 & 31 & 99 & 91 & 29 & 251 & 152 & 197 & 93 & 37 & 36 & 141 & 183 \end{bmatrix} \quad (3.7)$$

On adopting the decryption algorithm, we get back the original plaintext matrix given by (3.3)

Now we examine the avalanche effect. In order to achieve this one, firstly, let us have a change of one bit in the plaintext.

To this end, we change the first row, first column element of the plaintext from 68 to 69. On using the modified plaintext and the encryption algorithm, we get the cipher text in the form

$$C=\begin{bmatrix} 182 & 108 & 50 & 76 & 228 & 143 & 108 & 194 & 82 & 71 & 102 & 45 & 35 & 114 & 42 & 205 \\ 136 & 59 & 104 & 240 & 46 & 91 & 111 & 139 & 182 & 196 & 145 & 144 & 118 & 247 & 206 & 246 \\ 183 & 231 & 51 & 76 & 131 & 162 & 190 & 193 & 13 & 118 & 54 & 243 & 150 & 255 & 160 & 118 \\ 222 & 183 & 253 & 242 & 134 & 155 & 217 & 219 & 57 & 228 & 143 & 175 & 234 & 217 & 190 & 149 \\ 11 & 49 & 141 & 164 & 151 & 169 & 3 & 76 & 128 & 195 & 188 & 119 & 38 & 28 & 44 & 6 \\ 207 & 17 & 23 & 230 & 197 & 93 & 29 & 205 & 190 & 30 & 219 & 124 & 244 & 202 & 186 & 103 \\ 159 & 174 & 73 & 254 & 88 & 164 & 214 & 32 & 30 & 239 & 150 & 239 & 105 & 115 & 59 & 236 \\ 242 & 254 & 30 & 225 & 123 & 169 & 182 & 107 & 236 & 237 & 147 & 244 & 150 & 46 & 23 & 45 \end{bmatrix} \quad (3.8)$$

On comparing (3.7) and (3.8) in their binary form, we notice that they differ by 516 bits (out of 1024 bits).

Now let us consider a change of one bit in the key. In order to have this one, we change the first row, first column element of the key form 53 to 52.

On using this key and the encryption algorithm, given in section 2, we get the cipher text in the form

$$C=\begin{bmatrix} 70 & 219 & 194 & 242 & 76 & 237 & 163 & 193 & 37 & 187 & 209 & 38 & 42 & 205 & 50 & 14 \\ 222 & 249 & 226 & 2 & 204 & 99 & 107 & 123 & 90 & 236 & 109 & 171 & 98 & 210 & 163 & 57 \\ 228 & 143 & 175 & 141 & 202 & 205 & 244 & 185 & 203 & 127 & 244 & 150 & 42 & 205 & 50 & 14 \\ 222 & 249 & 226 & 2 & 204 & 68 & 240 & 246 & 145 & 207 & 71 & 114 & 97 & 195 & 166 & 121 \\ 128 & 247 & 116 & 239 & 179 & 33 & 206 & 91 & 189 & 201 & 65 & 219 & 223 & 36 & 64 & 89 \\ 128 & 2 & 230 & 220 & 191 & 45 & 44 & 97 & 219 & 74 & 216 & 13 & 91 & 234 & 109 & 153 \\ 34 & 222 & 181 & 116 & 222 & 95 & 35 & 145 & 218 & 118 & 249 & 251 & 227 & 36 & 227 & 240 \\ 190 & 236 & 130 & 109 & 99 & 110 & 143 & 177 & 173 & 142 & 253 & 204 & 98 & 174 & 146 & 146 \end{bmatrix} \quad (3.9)$$

On converting (3.7) and (3.9) into their binary form, we notice that they differ by 508 bits (out of 1024 bits).

From the above analysis we conclude that the cipher is expected to be a strong one.

IV. CRYPTANALYSIS

In the study of cryptology, cryptanalysis plays a prominent role in deciding the strength of a cipher. The well-known methods available for cryptanalysis are

a) *Cipher text only attack (Brute Force Attack)*
b) *Known plaintext attack*
c) *Chosen plaintext attack*
d) *Chosen cipher text attack*

Generally, an encryption algorithm is designed to withstand the brute force attack and the known plaintext attack [6].

Now let us focus our attention on the cipher text only attack. In this analysis, the key matrix is of size m x m. Thus, it has m^2 decimal numbers wherein each number can be represented in the form of 8 binary bits. Thus the size of the key space is

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

If we assume that the time required for the computation of the encryption algorithm with one value of the key, in the key space is

10^{-7} seconds,

then the time required for the computation with all the keys in the key space

$$= \frac{10^{2.4m^2} \times 10^{-7}}{365 \times 24 \times 60 \times 60} \text{ Years}$$

$$= 10^{2.4m^2} \times 3.12 \times 10^{-15}$$

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

In this analysis, as we have taken m=8, the time required for the entire computation is

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

This is enormously large. Thus, this cipher cannot be broken by the cipher text only attack (Brute Force Attack).

Now let us study the known plaintext attack. In this case, we know, as many plaintext cipher text pairs as we require. In the light of this fact, we have as many P_0 and Q_0, and the corresponding P_n and Q_n available at our disposal. Now our objective is to determine the key matrix K, if possible, to break the cipher.

From the equations (2.1) and (2.2) we get

$P_1 = (K\, Q_0\, K) \bmod N$,

$Q_1 = P_0 \oplus (K\, Q_0\, K) \bmod N$,

$P_2 = (K (P_0 \oplus (K\, Q_0\, K) \bmod N) K) \bmod N$

$Q_2 = ((K\, Q_0\, K) \bmod N) \oplus (K ((P \oplus (K\, Q_0\, K) \bmod N) K) \bmod N)$

$P_3 = (K ((K\, Q_0\, K) \bmod N) \oplus (K ((P_0 \oplus (K\, Q_0\, K) \bmod N) K) \bmod N) \bmod N)$

$Q_3 = (K ((K\, Q_0\, K) \bmod N) \oplus (K ((P_0 \oplus (K\, Q_0\, K) \bmod N) K) \bmod N)$

From the above equations we notice that, P_n and Q_n can be written in terms of P_0 , Q_0 , K and mod N. These equations are structurally of the form

$$P_n = F (P_0, Q_0, K, \bmod N), \quad (4.1)$$
$$Q_n = G (P_0, Q_0, K, \bmod N), \quad (4.2)$$

where F and G are two functions which depend upon, P_0, Q_0, K and mod N. on inspecting above equations in the analysis, we find that the equations (4.1) and (4.2) are nonlinear in K.

Though the matrices P_0 and Q_0, corresponding to the plaintext P, and the matrices P_n and Q_n corresponding to the ciphertext C are known to us, as the equations (4.1) and (4.2) are nonlinear in K, and including mod N at various instances, it is simply impossible to solve these equations and determine K. Thus, this cipher cannot be broken by the known plaintext attack.

As the relations (4.1) and (4.2) connecting P_0 , Q_0 and P_n and Q_n are formidable (being nonlinear and involving mod N), it is not possible to choose a plaintext or a cipher text and then determine the key K. Thus we cannot break the cipher in case 3 and case 4.

In the light of the above facts, the cryptanalysis clearly indicates that the cipher is a strong one.

V. COMPUTATIONS AND CONCLUSIONS

In this analysis the programs for encryption and decryption are written in C language.

The entire plaintext given by (3.1) is divided into 4 blocks. In the last block we have appended 5 blank characters to make it a complete block, for carrying our encryption.

The cipher text corresponding to the entire plaintext is obtained as given below

126	209	11	27	146	208	146	91	221	105	30	05	238	91	61	160
185	109	190	46	219	18	70	65	219	223	59	218	223	156	205	50
14	138	251	04	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	03	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
31	180	66	198	228	180	120	36	150	247	90	66	247	45	158	208
92	182	223	23	109	137	35	32	237	239	157	237	111	206	102	153
07	69	125	130	26	236	109	231	45	255	64	237	189	111	251	229
13	55	179	182	115	201	31	95	213	179	125	42	22	99	27	73
47	82	06	153	01	135	120	238	76	56	88	13	158	34	47	205
138	186	59	155	124	61	182	249	233	149	116	207	63	92	147	252
177	73	172	64	61	223	45	222	210	230	119	217	229	252	61	194
247	83	108	215	217	219	39	69	194	229	184	172	216	131	189	37
189	162	22	55	37	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	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	107	236	237	147	162	225	114	220	86	108	65	222	146

197	141	201	104	240	47	114	217	237	09	37	189	214	145	251	68
23	45	183	197	219	98	72	200	59	123	231	123	91	243	153	166
65	209	95	96	134	187	27	121	203	127	208	59	111	91	254	249
67	77	236	237	156	242	71	215	245	108	223	74	133	152	198	210
75	212	129	166	64	97	222	59	147	14	22	03	103	136	139	243
98	174	142	230	223	15	109	190	122	101	93	51	207	215	36	255
44	82	107	16	15	119	203	119	180	185	157	246	121	127	15	112
189	212	219	53	246	118	201	209	112	185	110	43	54	32	239	73

(5.1)

From the cryptanalysis carried out in this paper, we conclude that this cipher is a strong one and it cannot be broken by any attack.

It may be noted here that this cipher has gained enormous strength due to the multiplication of the plaintext matrix with the key matrix and the process of iteration, which is changing significantly the plaintext, before it becomes the cipher text.

REFERENCES

[1] 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, No.1, pp. 23-31, 2012.

[2] 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, No.1, pp. 32-39, 2012.

[3] V.U.K Sastry and K. Anup Kumar, "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", International Journal of Computer Science and Information Technologies ISSN: 0975-9646. Vol. 3, No.1, pp. 3133-3141, 2012.

[4] 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, No.1, pp. 3119-3128, 2012.

[5] William H.press,Brain P. Flannery, Saul A. Teukolsky, William T. Vetterling, Numerical Recipes in C: The Art of Scientific Computing, second Edition, 1992, Cambridge university Press, pp. 36-39.

[6] 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.