A Block Cipher Involving a Key Bunch Matrix and an Additional Key Matrix, Supplemented with Modular Arithmetic Addition and supported by Key-based Substitution

Dr. V.U.K.Sastry
Professor (CSE Dept), Dean (R&D)
SreeNidhi Institute of Science & Technology, SNIST
Hyderabad, India

K. Shirisha
Computer Science & Engineering
SreeNidhi Institute of Science & Technology, SNIST
Hyderabad, India

Abstract— **In this paper, we have devoted our attention to the development of a block cipher, which involves a key bunch matrix, an additional matrix, and a key matrix utilized in the development of a pair of functions called Permute() and Substitute(). These two functions are used for the creation of confusion and diffusion for each round of the iteration process of the encryption algorithm. The avalanche effect shows the strength of the cipher, and the cryptanalysis ensures that this cipher cannot be broken by any cryptanalytic attack generally available in the literature of cryptography.**

Keywords-key bunch matrix; additional key matrix; multiplicative inverse; encryption; decryption; permute; substitute.

I. Introduction

Security of information, which has to be maintained in a secret manner, is the primary concern of all the block ciphers. In a recent development, we have studied several block ciphers [1][2][3], "in press" [4], "unpublished" [5][6], "in press" [7], "unpublished" [8], wherein we have included a key bunch matrix and made use of the iteration process as a fundamental tool. In [7] and [8], we have introduced a key-based permutation and a key-based substitution for strengthen the cipher. Especially in [8], we have introduced an additional key matrix, supplemented with xor operation for adding some more strength to the cipher.

In the present paper, our objective is to modify the block cipher, presented in [7], by including and an additional key matrix supplemented with modular arithmetic addition. Here, our interest is to see how the permutation, the substitution and the additional key matrix would act in strengthening the cipher.

Now, let us mention the plan of the paper. We put forth the development of the cipher in section 2. Here, we portray the flowcharts and present the algorithms required in the development of this cipher. Then, we discuss the basic concepts of the key based permutation and substitution. We give an illustration of the cipher and discuss the avalanche effect, in section 3. We analyze the cryptanalysis, in section 4. Finally, we talk about the computations carried out in this analysis, and arrive at the conclusions, in section 5.

II. Developemnt Of The Cipher

Consider a plaintext matrix P, given by

$$P = [\, p_{ij} \,],\ i=1 \text{ to } n,\ j=1 \text{ to } n. \tag{2.1}$$

Let us take the key bunch matrix E in the form

$$E = [\, e_{ij} \,],\ i=1 \text{ to } n,\ j=1 \text{ to } n. \tag{2.2}$$

Here, we take all e_{ij} as odd numbers, which lie in the interval [1-255]. On using the concept of the multiplicative inverse, we get the decryption key bunch matrix D, in the form

$$D= [\, d_{ij} \,],\ i=1 \text{ to } n,\ j=1 \text{ to } n, \tag{2.3}$$

wherein d_{ij} and e_{ij} are related by the relation

$$(e_{ij} \times d_{ij}) \bmod 256 = 1, \tag{2.4}$$

for all i and j.

Here, it is to be noted that d_{ij} will be obtained as odd numbers and lie in the interval [1-255].

The additional key matrix F, can be taken in the form

$$F=[\, f_{ij} \,],\ i=1 \text{ to } n,\ j=1 \text{ to } n, \tag{2.5}$$

where f_{ij} are integers lying in [0-255].

The basic equations governing the encryption and the decryption, in this analysis, are given by

$$C = [\, c_{ij} \,] = (([\, e_{ij} \times p_{ij} \,] \bmod 256) +F) \bmod 256,\quad i=1 \text{ to } n,\ j = 1 \text{ to } n, \tag{2.6}$$

and

$$P = [\, p_{ij} \,] = [\, d_{ij} \times (C-F)_{ij} \,] \bmod 256,\quad i=1 \text{ to } n,\ j = 1 \text{ to } n, \tag{2.7}$$

where C is the ciphertext.

The flowcharts concerned to the procedure involved in this analysis are given in Figs. 1 and 2.

Here r denotes the number of rounds in the iteration process. The functions Permute() and Substitute() are used for achieving transformation of the plaintext, so that confusion and diffusion are created, in each round of the iteration process. The function Mult() is used to find the decryption key bunch matrix D from the given encryption key bunch matrix E. The functions IPermute() and ISubstitute() stand for the reverse process of the Permute() and Substitute(). The details of the permutation and substitution process are explained later.

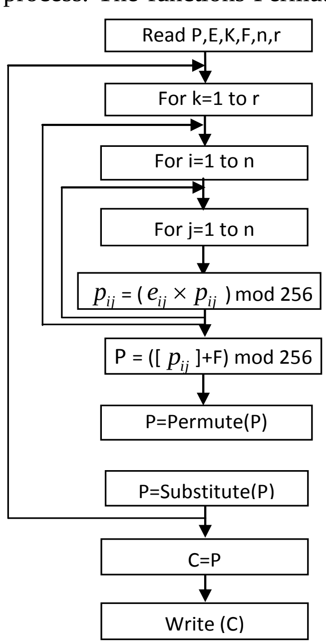

Figure 1 Flowchart for Encryption

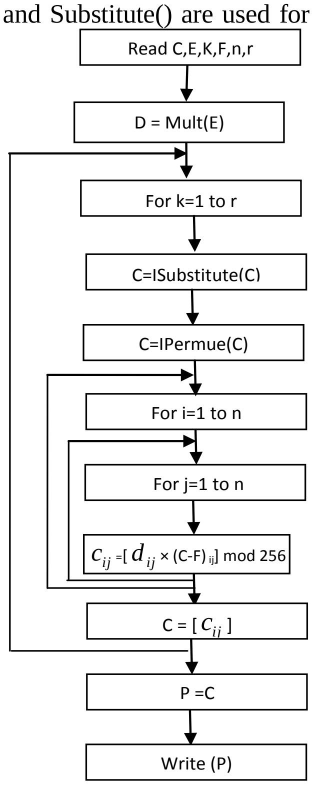

Figure 2 Flowchart for Decryption

The algorithms corresponding to the flowcharts are written as follows.

ALGORITHM FOR ENCRYPTION

1. Read P,E,K,F,n,r
2. For k = 1 to r do
   {
3. For i=1 to n do
   {
4. For j=1 to n do
   {
5. p_{ij} = (e_{ij} × p_{ij}) mod 256
   }
   }
6. P=([p_{ij}] + F) mod 256
7. P=Permute(P)
8. P=Substitute(P)
   }
9. C=P
10. Write(C)

ALGORITHM FOR DECRYPTION

1. Read C,E,K,F,n,r
2. D=Mult(E)
3. For k = 1 to r do
   {
4. C=ISubstitute(C)
5. C=IPermute(C)
6. For i =1 to n do
   {
7. For j=1 to n do
   {
8. c_{ij} =[d_{ij} ×(c_{ij} - f_{ij})] mod 256
   }
   }
9. C=[c_{ij}]
   }
10. P=C
11. Write (P)

In the development of the permutation and the substitution, we take a key matrix K in the form given below.

$$K = \begin{bmatrix} 156 & 14 & 33 & 96 \\ 253 & 107 & 110 & 127 \\ 164 & 10 & 5 & 123 \\ 174 & 202 & 150 & 94 \end{bmatrix} \qquad (2.8)$$

Figure 1. Flowchart for Encryption

The serial order, the elements in the key, the order of elements can be used and form a table of the form.

TABLE I. RELATION BETWEEN SERIAL NUMBERS AND NUMBERS IN ASCENDING ORDER

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
156	14	33	96	253	107	110	127	164	10	5	123	174	202	150	94
12	3	4	6	16	7	8	10	13	2	1	9	14	15	11	5

In the process of permutation, we convert the decimal numbers in the plaintext matrix into binary bits and swap the rows firstly and the columns nextly, one after another, and achieve the final form of the permuted matrix by representing the binary bits in terms of decimal numbers. In the case of the substitution process, we consider the EBCDIC code matrix consisting of the decimal numbers 0 to 255, in 16 rows 16 columns, and interchange the rows firstly and the columns nextly, and then achieve the substitution matrix. For a detailed discussion of the functions Permute() and Substitute(), we refer to [7].

III. ILLUSTRATION OF THE CIPHER AND THE AVALANCHE EFFECT

Consider the plaintext given below.

Dear Brother! I have got posting in army as a Captain a few days back. Both father and mother are advising me not to go there. They say that they have committed a sin in sending you as an Army Doctor. You know all the problems which you are facing in that environment in Indian Army. Tell me what shall I do? Would you suggest me to join in the same profession in which you are? All the retired Army employees who are residing in our area are telling "Serving Mother India is really great". But most of their sons are working here only in our city. (3.1)

Let us focus our attention on the first 16 characters of the aforementioned plaintext. Thus we have

Dear Brother! I (3.2)

On using the EBCDIC code, the plaintext (3.2), can be written in the form P, given by

$$P = \begin{bmatrix} 196 & 133 & 129 & 153 \\ 64 & 194 & 153 & 150 \\ 163 & 136 & 133 & 153 \\ 79 & 64 & 201 & 64 \end{bmatrix}. \quad (3.3)$$

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

$$E = \begin{bmatrix} 9 & 81 & 201 & 137 \\ 235 & 93 & 15 & 107 \\ 33 & 79 & 191 & 255 \\ 57 & 197 & 179 & 3 \end{bmatrix}. \quad (3.4)$$

We take the additional key matrix F in the form

$$F = \begin{bmatrix} 78 & 43 & 224 & 209 \\ 45 & 53 & 80 & 100 \\ 14 & 6 & 236 & 1 \\ 69 & 42 & 53 & 250 \end{bmatrix}. \quad (3.5)$$

On using the concept of multiplicative inverse, mentioned in section 2, we get the decryption key bunch matrix D in the form

$$D = \begin{bmatrix} 57 & 177 & 121 & 185 \\ 195 & 245 & 239 & 67 \\ 225 & 175 & 63 & 255 \\ 9 & 13 & 123 & 171 \end{bmatrix}. \quad (3.6)$$

On using the P, the E, and the F, given by (3.3) – (3.5), and applying the encryption algorithm, given in section 2, w get the ciphertext C in the form

$$C = \begin{bmatrix} 133 & 110 & 122 & 68 \\ 33 & 174 & 239 & 98 \\ 221 & 102 & 191 & 248 \\ 100 & 184 & 169 & 21 \end{bmatrix}. \quad (3.7)$$

On using the C, the D, and the F, and applying the decryption algorithm, we get back the original plaintext P, given by (3.3).

Let us now examine the avalanche effect. On replacing the 2nd row 2nd column element 194 of the plaintext P, given by (3.3), by 195, we get the modified plaintext, wherein a change of one binary bit is there. On using this modified plaintext, the E and F, given by (3.4) and (3.5), and applying the encryption algorithm, we get the corresponding ciphertext.

$$C = \begin{bmatrix} 51 & 177 & 198 & 26 \\ 237 & 197 & 30 & 206 \\ 19 & 39 & 165 & 214 \\ 154 & 191 & 6 & 19 \end{bmatrix}. \quad (3.8)$$

On comparing (3.7) and (3.8), after representing them in their binary form, we notice that these two ciphertexts differ by 72 bits out of 128 bits.

In a similar manner, let us offer one binary bit change in the encryption key bunch matrix E. This is achieved by replacing 3rd row 1st column element 33 of E by 32. Then on using this E, the original P, given by (3.3), the F, given by (3.5), and using the encryption algorithm, we obtain the corresponding ciphertext in the form

$$C = \begin{bmatrix} 155 & 158 & 195 & 250 \\ 156 & 158 & 6 & 221 \\ 151 & 186 & 1 & 19 \\ 127 & 39 & 20 & 221 \end{bmatrix}. \quad (3.9)$$

On carrying out a comparative study of (3.7) and (3.9), after putting them in their binary form, we find that these two differ by 78 bits out of 128 bits. From the above discussion, we conclude that this cipher is exhibiting a strong avalanche effect, and the strength of the cipher is expected to be a remarkable one.

IV. CRYPTANALYSIS

In the development of all the block ciphers, the importance of cryptanalysis is commendable. The different cryptanalytic attacks that are dealt with very often in the literature are

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

Generally, the first two attacks are examined in an analytical manner, while the latter two attacks are inspected with all care, in an intuitive manner. It is to be noted here that no cipher can be accepted, unless it withstands the first two attacks [9], and no cipher can be relied upon unless a clear cut decision is arrived in the case of the latter two attacks.

Let us now consider the brute force attack. In this analysis, we have 3 important entities namely, the key bunch matrix E, the additional key matrix F, and the special key K, used in the Permute() and Substitute() functions. On account of these three, the size of the key space can be written in the form

$$2^{7n^2} \times 2^{8n^2} \times 2^{128} = 2^{7n^2+8n^2+128} = 2^{15n^2+128}$$
$$= \left(2^{10}\right)^{(1.5n^2+12.8)} \approx \left(10^{3}\right)^{(1.5n^2+12.8)} = 10^{4.5n^2+38.4}$$

On assuming that, we require 10^{-7} seconds for computation with one set of keys in the key space, the time required for execution with all such possible sets in the key space is

$$\frac{10^{4.5n^2+38.4} \times 10^{-7}}{365 \times 24 \times 60 \times 60} = 3.12 \times 10^{4.5n^2+23.4} \; years.$$

In this analysis, as we have taken n=4, the time for computation with all possible sets of keys in the key space is

$3.12 \times 10^{95.4}$ *years*.

As this is a very long span, this cipher cannot be broken by the brute force attack.

Now, let us examine the known plaintext attack. In the case of this attack, we know any number of plaintext and ciphertext pairs, which we require for our investigation. Focusing our attention on r=1, that is on the first round of the iteration process, in the encryption, we get the set of equations, given by

$$P=(([e_{ij} \times p_{ij}] \bmod 256)+F) \bmod 256, \ i=1 \text{ to } n, \ j=1 \text{ to } n, \quad (4.1)$$

$$P = \text{Permute}(P), \quad (4.2)$$

$$P = \text{Substitute}(P), \quad (4.3)$$

and

$$C = P \quad (4.4)$$

Here as C in (4.4) is known, we get P. However, as the substitution process and permutation process depend upon the key, one cannot have any idea regarding ISubstitute() and IPermute(). Thus it is simply impossible to determine P even at the next higher level that is in (4.3). In a spectacular manner, if one has a chance to know the key K (a rare situation), then one can determine P, occurring on the left hand side of (4.1), by using ISubstitute() and IPermute(). Then also, it is not at all possible to determine the e_{ij} (elements of the key bunch matrix), as this equation is totally involved on account of the presence of F and the mod operation. This shows that the cipher is strengthened by the presence of F.

From the above analysis, we conclude that this cipher cannot be broken by the known plaintext attack. As there are 16 rounds of iteration process, we can say very emphatically, that this cipher is unbreakable by the known plaintext attack.

On considering the set of equations in the encryption process, including mod, permute and substitute, we do not envisage any possible choice, either for the plaintext or for the ciphertext to make an attempt for breaking this cipher.

In the light of all these factors, we conclude that this cipher is a strong one and it can be applied for the secure transmission of any secret information.

V. COMPUTATIONS AND CONCLUSIONS

In this paper, we have developed a block cipher which involves an encryption key bunch matrix, an additional matrix and a key matrix utilized for the development of a pair of functions called Permute() and Substitute(). In this analysis the additional matrix is supplemented with modular arithmetic addition. The cryptanalysis carried out in this investigation firmly indicates that this cipher cannot be broken by any cryptanalytic attack.

The programs required for encryption and decryption are written in Java.

The entire plain text given by (3.1) is divided into 3 blocks, wherein each block is written as a square matrix of size 16. As the last block is containing 37 characters, 219 zeroes are appended as additional characters so that it becomes a complete block.

To carry out the encryption of these plaintext blocks, here we take a key bunch matrix EK of size 16x16 and an additional matrix FK of the same size. They are taken in the form

$$EK = \begin{bmatrix}
19 & 173 & 1 & 247 & 187 & 205 & 221 & 157 & 129 & 15 & 249 & 125 & 69 & 127 & 193 & 245 \\
149 & 35 & 205 & 117 & 177 & 15 & 161 & 173 & 51 & 185 & 203 & 61 & 79 & 93 & 239 & 33 \\
211 & 213 & 207 & 29 & 91 & 237 & 159 & 9 & 49 & 29 & 69 & 35 & 113 & 49 & 179 & 119 \\
161 & 147 & 77 & 53 & 67 & 169 & 203 & 189 & 159 & 113 & 185 & 181 & 59 & 19 & 117 & 43 \\
65 & 221 & 195 & 171 & 145 & 253 & 65 & 115 & 229 & 173 & 147 & 63 & 181 & 147 & 11 & 109 \\
179 & 119 & 53 & 45 & 11 & 205 & 97 & 145 & 223 & 135 & 239 & 21 & 155 & 83 & 133 & 183 \\
7 & 45 & 71 & 177 & 57 & 203 & 145 & 189 & 221 & 191 & 197 & 109 & 227 & 131 & 1 & 75 \\
153 & 103 & 119 & 209 & 43 & 189 & 149 & 67 & 243 & 155 & 95 & 39 & 117 & 67 & 251 & 135 \\
181 & 157 & 185 & 11 & 153 & 127 & 55 & 241 & 73 & 205 & 255 & 227 & 229 & 149 & 9 & 21 \\
187 & 203 & 159 & 107 & 91 & 197 & 229 & 37 & 177 & 23 & 205 & 153 & 177 & 93 & 253 & 241 \\
239 & 115 & 233 & 187 & 227 & 71 & 85 & 249 & 175 & 77 & 29 & 245 & 69 & 179 & 189 & 249 \\
17 & 197 & 27 & 45 & 141 & 117 & 161 & 91 & 191 & 145 & 45 & 229 & 49 & 145 & 191 & 77 \\
107 & 105 & 245 & 75 & 99 & 185 & 97 & 211 & 151 & 239 & 229 & 105 & 233 & 155 & 179 & 213 \\
247 & 221 & 111 & 231 & 135 & 209 & 181 & 251 & 85 & 37 & 119 & 91 & 93 & 93 & 15 & 221 \\
157 & 89 & 199 & 121 & 193 & 23 & 47 & 115 & 159 & 127 & 203 & 167 & 3 & 239 & 249 & 47 \\
141 & 191 & 103 & 107 & 221 & 251 & 79 & 147 & 249 & 41 & 91 & 225 & 177 & 85 & 5 & 155
\end{bmatrix}$$

and

$$FK = \begin{bmatrix}
58 & 125 & 140 & 75 & 9 & 209 & 148 & 230 & 62 & 52 & 94 & 184 & 76 & 195 & 213 & 28 \\
190 & 223 & 33 & 102 & 237 & 11 & 93 & 234 & 147 & 163 & 125 & 171 & 56 & 7 & 47 & 123 \\
141 & 52 & 198 & 148 & 83 & 159 & 15 & 128 & 0 & 169 & 193 & 116 & 114 & 232 & 167 & 32 \\
26 & 0 & 245 & 81 & 199 & 230 & 79 & 190 & 222 & 197 & 202 & 169 & 8 & 10 & 241 & 47 \\
189 & 148 & 30 & 85 & 174 & 52 & 195 & 76 & 33 & 100 & 35 & 141 & 109 & 73 & 205 & 244 \\
110 & 197 & 159 & 67 & 112 & 191 & 126 & 234 & 66 & 138 & 239 & 108 & 98 & 148 & 188 & 40 \\
1 & 146 & 84 & 215 & 77 & 151 & 44 & 141 & 238 & 148 & 120 & 182 & 208 & 20 & 182 & 5 \\
100 & 50 & 54 & 3 & 76 & 29 & 103 & 143 & 241 & 174 & 1 & 75 & 240 & 32 & 70 & 187 \\
92 & 10 & 136 & 150 & 207 & 134 & 188 & 135 & 231 & 109 & 108 & 134 & 103 & 115 & 153 & 188 \\
70 & 15 & 26 & 201 & 69 & 242 & 229 & 42 & 43 & 19 & 55 & 129 & 178 & 47 & 255 & 96 \\
85 & 8 & 25 & 80 & 129 & 120 & 182 & 205 & 135 & 249 & 68 & 12 & 131 & 41 & 98 & 95 \\
212 & 70 & 239 & 99 & 44 & 204 & 49 & 3 & 38 & 173 & 243 & 228 & 111 & 252 & 32 & 174 \\
233 & 62 & 187 & 61 & 221 & 230 & 87 & 203 & 71 & 39 & 16 & 160 & 139 & 105 & 232 & 41 \\
88 & 135 & 212 & 153 & 82 & 54 & 35 & 220 & 49 & 185 & 13 & 214 & 97 & 120 & 251 & 155 \\
197 & 205 & 217 & 159 & 69 & 217 & 54 & 143 & 232 & 27 & 19 & 252 & 202 & 238 & 96 & 166 \\
253 & 35 & 224 & 212 & 105 & 100 & 184 & 216 & 31 & 40 & 93 & 125 & 38 & 127 & 145 & 244
\end{bmatrix}$$

On using each block of the plain text, the key bunch matrix EK and the additional matrix FK, in the places of E and F respectively, and applying the encryption algorithm, given in section 2, we carry out the encryption of each block separately, and obtain the cipher text as follows in (5.1).

Now, for the secure transmission of EK and FK, we encrypt these two by using E and F, and applying the encryption algorithm. Thus, we have the ciphertexts corresponding to EK and FK as given below, in (5.2) and (5.3), respectively.

From this analysis the sender transmits all the 3 blocks of the cipher text, corresponding to the entire plain text, and the cipher text of EK and FK, given in (5.1), (5.2) and (5.3), In addition to this information, he provides the key bunch matrix E, the additional matrix F and the key matrix K in a secured manner. He also supplies the number of characters with which the last block of the entire plain text is appended.

From the cryptanalysis carried out in this investigation we have found that this cipher is a strong one and cannot be broken by any cryptanalytic approach.

Here it may be noted that this cipher can be applied for the encryption of a plain text of any size, and for the encryption of a gray level or color image.

REFERENCES

[1] Dr. V.U.K. Sastry, K.Shirisha, "A Novel Block Cipher Involving a Key Bunch Matrix", in International Journal of Computer Applications (0975 – 8887) Volume 55– No.16, Oct 2012, Foundation of Computer Science, NewYork, pp. 1-6.

[2] Dr. V.U.K. Sastry, K.Shirisha, "A Block Cipher Involving a Key Bunch Matrix and Including Another Key Matrix Supplemented with Xor Operation ", in International Journal of Computer Applications (0975 – 8887) Volume 55– No.16, Oct 2012, Foundation of Computer Science, NewYork, pp.7-10.

[3] Dr. V.U.K. Sastry, K.Shirisha, "A Block Cipher Involving a Key Bunch Matrix and Including another Key Matrix Supported With Modular Arithmetic Addition", in International Journal of Computer Applications (0975 – 8887) Volume 55– No.16, Oct 2012, Foundation of Computer Science, NewYork, pp. 11-14.

[4] Dr. V.U.K. Sastry, K.Shirisha, "A novel block cipher involving a key bunch matrix and a permutation", International Journal of Computers and Electronics Research (IJCER), in press.

[5] Dr. V.U.K. Sastry, K.Shirisha, "A block cipher involving a key bunch matrix, and a key matrix supported with xor operation, and supplemented with permutation", unpublished.

[6] Dr. V.U.K. Sastry, K.Shirisha, "A block cipher involving a key bunch matrix, and a key matrix supported with modular arithmetic addition, and supplemented with permutation", unpublished.

[7] Dr. V.U.K. Sastry, K.Shirisha, "A novel block cipher involving a key bunch matrix and a key-based permutation and substitution", International Journal of Advanced Computer Science and Applications (IJACSA), in press.

[8] Dr. V.U.K. Sastry, K.Shirisha, "A block cipher involving a key bunch matrix and an additional key matrix, supplemented with xor operation and supported by key-based permutation and substitution", unpublished.

[9] William Stallings: Cryptography and Network Security: Principle and Practices", Third Edition 2003, Chapter 2, pp. 29.

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 14 PhDs, and published more than 86 research papers in various International Journals. He received the Best Engineering College Faculty Award in Computer Science and Engineering for the year 2008 from the Indian Society for Technical Education (AP Chapter), Best Teacher Award by Lions Clubs International, Hyderabad Elite, in 2012, and Cognizant-Sreenidhi Best faculty award for the year 2012. His research interests are Network Security & Cryptography, Image Processing, Data Mining and Genetic Algorithms.

K. Shirisha is currently working as Associate Professor in the Department of Computer Science and Engineering (CSE), SreeNidhi Institute of Science & Technology (SNIST), Hyderabad, India, since February 2007. She is pursuing her Ph.D. Her research interests are Information Security and Data Mining. She published three research papers in International Journals. She stood University topper in the M.Tech.(CSE).

55	98	195	171	226	83	253	114	163	77	26	121	39	199	193	190
164	159	13	81	117	43	52	60	154	205	38	146	142	105	68	54
207	35	52	107	192	208	193	24	11	134	252	36	22	193	196	242
137	191	244	80	8	206	7	54	132	31	41	140	41	117	208	75
203	252	146	129	11	160	217	143	120	11	71	59	233	193	72	157
207	205	10	87	46	13	213	20	189	137	189	135	141	161	228	145
128	199	218	65	87	12	184	133	242	130	101	119	97	88	92	183
193	97	33	94	174	219	138	41	37	96	60	23	76	21	185	251
229	141	212	251	102	227	180	135	49	137	134	100	181	60	106	198
66	82	216	84	228	85	204	106	178	97	12	240	173	186	55	241
123	221	164	106	78	109	157	41	7	23	32	69	251	59	236	231
33	203	137	21	213	28	83	187	20	74	53	108	190	234	125	5
24	10	66	74	123	3	105	179	41	164	100	79	23	21	31	128
251	239	115	49	124	75	19	28	41	72	105	187	36	70	205	92
49	29	162	253	39	251	109	65	118	18	254	252	159	94	120	123
195	238	106	186	180	251	183	37	245	173	112	16	5	231	2	236
187	166	0	84	24	113	0	176	211	250	131	95	63	67	84	164
134	204	147	101	67	157	191	24	236	80	159	245	130	60	185	171
228	33	237	209	121	30	14	243	202	80	147	109	247	83	39	170
118	64	144	24	233	138	109	121	90	68	110	4	242	220	207	239
216	45	26	38	1	226	4	25	174	6	239	164	185	103	71	121
47	207	34	153	29	125	155	186	228	219	192	226	45	120	154	50
98	128	235	220	8	40	163	154	164	67	103	115	129	148	90	85
67	181	251	59	120	53	97	7	37	210	192	15	33	252	84	152
109	128	185	230	65	141	198	227	119	64	247	106	151	163	5	8
150	166	129	130	17	54	1	38	180	69	36	15	102	78	106	134
14	200	51	243	192	162	200	43	64	52	90	16	1	70	193	34
126	78	156	252	57	84	199	200	29	104	46	101	151	0	96	111
225	152	219	108	60	187	22	161	75	205	76	206	117	216	3	199
57	200	162	99	52	22	205	88	75	61	141	183	72	235	174	7
172	232	228	31	240	105	180	85	207	189	252	134	77	144	148	141
248	27	132	35	154	195	161	209	176	169	136	78	229	160	180	79
244	161	218	39	227	184	49	171	105	36	203	137	166	210	242	135
135	58	61	235	246	199	126	224	136	164	228	42	229	34	204	252
161	231	179	113	141	146	197	197	243	230	188	69	60	148	23	42
14	109	166	239	54	23	117	182	67	7	52	83	113	219	42	163
137	74	198	183	247	73	133	93	205	23	19	61	1	63	61	155
59	66	89	105	102	217	107	74	169	72	72	98	140	196	253	2
34	178	246	157	240	116	218	205	49	207	44	185	190	252	50	180
29	34	126	43	89	96	100	149	233	132	102	192	48	51	25	154
190	34	18	109	217	108	90	205	64	145	113	70	54	138	191	29
160	157	192	74	218	189	99	89	68	125	239	199	24	216	22	21
255	198	147	22	53	89	164	99	93	146	233	217	219	121	212	61
231	38	174	103	125	63	175	178	147	30	9	175	197	167	200	177
197	85	90	248	190	225	96	74	45	19	35	194	157	158	198	31
233	108	66	0	56	114	65	50	87	15	205	89	91	80	241	146
85	132	187	63	151	245	175	211	114	121	31	155	199	186	229	116
183	64	216	127	196	21	229	173	252	71	135	143	85	245	162	78

(5.1)

116	112	40	123	211	102	93	179	40	154	235	69	34	147	243	36
146	180	23	213	21	186	167	12	57	85	65	84	121	78	180	31
224	176	75	84	49	185	144	147	170	205	61	200	217	72	100	207
105	110	246	250	158	251	111	164	49	10	62	52	231	245	237	106
90	72	239	74	160	4	183	54	28	243	51	135	161	194	153	80
251	35	250	13	222	66	16	246	78	20	98	115	121	242	111	239
13	94	140	164	189	182	31	5	42	244	230	117	228	231	67	239
101	190	72	68	226	46	188	215	238	127	152	114	121	99	19	10
155	224	45	11	206	8	98	81	126	233	95	3	166	44	133	97
161	116	250	217	241	169	79	197	219	216	182	98	160	100	24	127
131	51	198	162	250	246	201	116	118	76	160	124	72	132	38	50
144	170	99	186	250	165	87	62	147	19	114	104	131	14	204	188
191	160	18	37	247	233	129	220	199	40	71	96	171	108	253	92
129	101	41	89	89	4	247	147	144	12	4	122	210	78	249	103
42	10	255	126	157	148	99	255	173	214	52	200	113	215	190	231
181	131	98	6	241	203	213	96	64	95	99	135	253	228	136	213

(5.2)

and

58	125	140	75	9	209	148	230	62	52	94	184	76	195	213	28
190	223	33	102	237	11	93	234	147	163	125	171	56	7	47	123
141	52	198	148	83	159	15	128	0	169	193	116	114	232	167	32
26	0	245	81	199	230	79	190	222	197	202	169	8	10	241	47
189	148	30	85	174	52	195	76	33	100	35	141	109	73	205	244
110	197	159	67	112	191	126	234	66	138	239	108	98	148	188	40
1	146	84	215	77	151	44	141	238	148	120	182	208	20	182	5
100	50	54	3	76	29	103	143	241	174	1	75	240	32	70	187
92	10	136	150	207	134	188	135	231	109	108	134	103	115	153	188
70	15	26	201	69	242	229	42	43	19	55	129	178	47	255	96
85	8	25	80	129	120	182	205	135	249	68	12	131	41	98	95
212	70	239	99	44	204	49	3	38	173	243	228	111	252	32	174
233	62	187	61	221	230	87	203	71	39	16	160	139	105	232	41
88	135	212	153	82	54	35	220	49	185	13	214	97	120	251	155
197	205	217	159	69	217	54	143	232	27	19	252	202	238	96	166
253	35	224	212	105	100	184	216	31	40	93	125	38	127	145	244

(5.3)