The International Journal of Engineering
And Science (IJES)
||Volume|| 1 ||Issue|| 2 ||Pages|| 40-47 ||2012||
ISSN: **2319 – 1813** ISBN: **2319 – 1805**

A Block Cipher Involving A Key Matrix And A Key Bunch Matrix, Supplemented With Permutation

[1,]Dr. V.U.K.Sastry,[2,] K. Shirisha
[1,2,]Dept. of Computer Science & Engineering, SreeNidhi Institute of Science & Technology

Abstract

In this paper, we have devoted our attention to the development of a block cipher, which involves a key matrix and a key bunch matrix. Here, we have used a function called Permute() for causing permutation of the binary bits of the plaintext, in each round of the iteration process. Here, the diffusion arising on account of the keys and the confusion caused by the permutation, both play a prominent role in strengthening the cipher. The cryptanalysis carried out in this investigation strongly indicates the strength of the cipher.

Keywords - avalanche effect, cryptanalysis, decryption, encryption, key bunch matrix, key matrix, permutation

Date of Submission:20, November, 2012 ⟺ Date of Publication: 5,December 2012

1. Introduction

In a recent investigation [1], we have developed a block cipher, which includes a key matrix and a key bunch matrix. In this, the process of the encryption is supplemented with a function called Mix(), in which the binary bits of the plaintext are thoroughly mixed in each round of the iteration process. In this, we have made use of the modular arithmetic inverse of the key matrix, used in the Hill cipher [2], and the concept of the multiplicative inverse, which yields the decryption key bunch matrix, that is required in the decryption process. The strength of this cipher is found to be remarkable. The cryptanalysis shows very clearly, that this cipher cannot be broken by any general cryptanalytic attack.In the present paper, our objective is to develop another strong block cipher by using the basic ideas of the Hill cipher, and the basic ideas of the key bunch matrix [3-4]. Here we introduce a permutation process which shuffles the binary bits of a plaintext in each round of the iteration process. The details of the function Permute(), which describes the permutation process, are given later in section 2. Here, the strength of the cipher is expected to enhance, as the function Permute() is supporting the cipher.In what follows, we present the plan of the paper. In this, section 2 deals with the development of the cipher. Here, we have presented the flowcharts and the algorithms which indicate the development of the cipher. In section 3, we have put forth an illustration of the cipher and examined the avalanche effect, which stands as benchmark in respect of the strength of the cipher. Then we have discussed the cryptanalysis, in section 4. Finally, in section 5, we have considered the computations carried out in this investigation, and have drawn out the conclusions from this analysis.

2. Development Of The Cipher

Consider a plaintext. On using the EBCDIC code, we represent this in the form of a matrix, given by

$$P = [\, p_{ij} \,],\ I = 1 \text{ to } n,\ j=1 \text{ to } n. \qquad (2.1)$$

Let us choose a key matrix K and an encryption key bunch matrix E in the form

$$K = [\, k_{ij} \,],\ I = 1 \text{ to } n,\ j=1 \text{ to } n, \qquad (2.2)$$

and

$$E = [\, e_{ij} \,],\ i =1 \text{ to } n,\ j=1 \text{ to } n, \qquad (2.3)$$

Here, we assume that the determinant of K is not equal to zero and it is an odd number. In view of this fact the modular arithmetic inverse of K can be obtained by using the relation

$$(KK^{-1}) \bmod 256 = I \tag{2.4}$$

On assuming that e_{ij}, the elements of the matrix E, are odd numbers lying in [1-255], we get the decryption key bunch matrix D in the form

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

where e_{ij} and d_{ij} are governed by the relation

$$(\, e_{ij} \times d_{ij} \,) \bmod 256 = 1 \tag{2.6}$$

Here, it is to be noted that d_{ij} also turn out to be odd numbers in [1-255].

The basic equations governing the encryption and the decryption are given by

$$P = (KP) \bmod 256, \tag{2.7}$$

$$P = [\, e_{ij} \times p_{ij} \,] \bmod 256,\ i=1 \text{ to } n,\ j = 1 \text{ to } n, \tag{2.8}$$

$$P = \text{Permute}(P), \tag{2.9}$$

$$C = P, \tag{2.10}$$

and

$$C = \text{IPermute}(C), \tag{2.11}$$

$$C=[\, c_{ij} \,]=[\, d_{ij} \times c_{ij} \,] \bmod 256,\ i=1 \text{ to } n,\ j=1 \text{ to } n \tag{2.12}$$

$$C = (K^{-1}C\ ) \bmod 256, \tag{2.13}$$

$$P = C. \tag{2.14}$$

The details of the function Permute() and the function IPermute(), the reverse process of the Permute(), are given later. The flowcharts representing this process are given in Figs. 1 and 2.

The corresponding algorithms for the encryption and the decryption are as follows.

Algorithm for Encryption

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

Algorithm for Decryption

1. Read C,E,K,n,r
2. D=Mult(E)
3. K^{-1} = Inv(K)
4. For k = 1 to r do
   {
5. C=IPermute(C)
6. For i =1 to n do

{

7. For j=1 to n do

{

8. $c_{ij} = (d_{ij} \times c_{ij})$ mod 256

}

}

9. C = [c_{ij}]
10. C=(K^{-1}C) mod 256

}

11. P=C
12. Write (P)

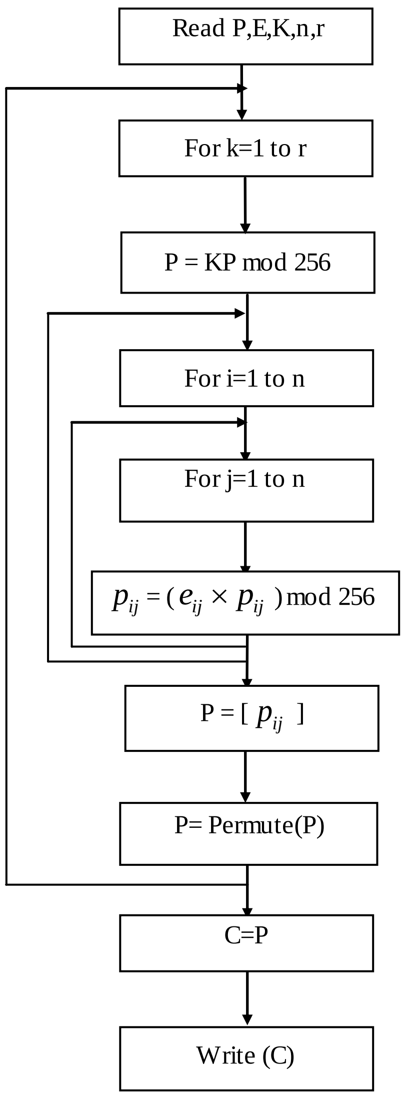

Fig.1 Flowchart for Encryption

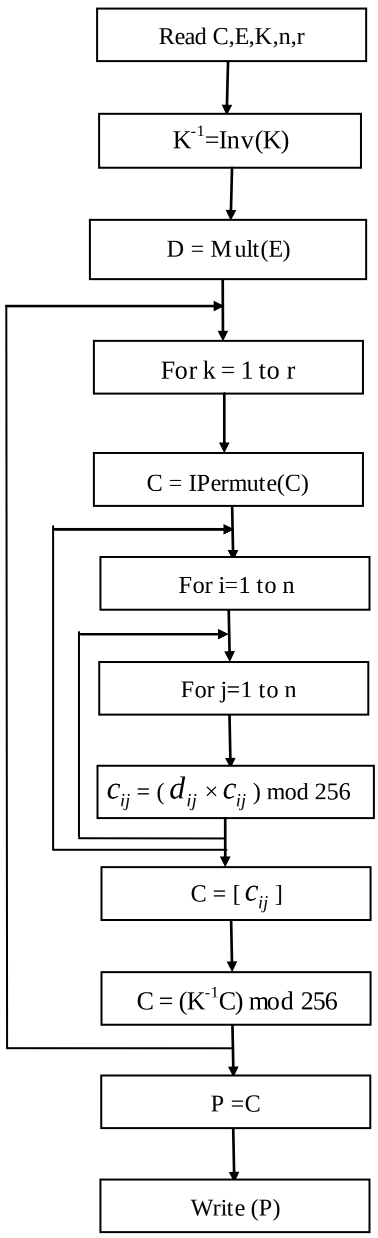

Fig.2. Flowchart for Decryption

In this analysis, r denotes the number of rounds carried out in the iteration process. Here we take r=16.

The process of permutation, embedded in the function Permute(), is explained below. Let P=[p_{ij}], i=1 to n, j=1 to n, be the plaintext matrix in any round of the iteration process. On writing each element in terms of binary bits, in a row-wise manner, we get a matrix of size $n \times 8n$. Then we offer a right circular rotation to the first row and a downward circular rotation to the first column. On assuming that, n is divisible by 8, the afore-mentioned matrix can be viewed as ($n^2/8$) sub-matrices, where each sub-matrix is a square matrix of size 8. Now, we focus our attention on each sub-matrix, and partition this into four sub-matrices, wherein each one is a square matrix of size 4, by dividing horizontally and vertically. Then, on permuting the 4x4 sub-matrices by swapping them along the diagonals, they occupy new positions. Now, we convert the binary bits of the afore-mentioned matrix into decimal numbers, by taking the binary bits in a column-wise manner, and writing the decimal numbers in a row-wise manner. We get the ultimate permuted form. The function IPermute() is having the reverse process of the function Permute(). The function Inv() yields the modular arithmetic inverse of the key matrix K. The function Mult() is used to obtain the decryption key bunch matrix D for the given encryption key bunch matrix E. For a detailed discussion of these function , we may refer to [1].

3. Illustration Of The Cipher And The Avalanche Effect

Consider the plaintext given below.

Respected Madam! If we stop tobacco production immediately at one stroke, several lakhs of farmers and coolies, who are dependant on this production, will loose their livelihood. This may even to lead their death. Tobacco is not only used for cigarettes and gutka, but it is also utilized in pharmacy companies and research centers for the production of medicines. The State Government is getting an amount of twenty thousand crores profit (as tax) on the tobacco production. If prohibition of tobacco is implemented, there is a danger that many farmers might fall on the road without any agricultural activity, which fetches money to them. Thus, reducing tobacco production on a world-wide basis must be planned. The World Health Organization is contemplating this issue in a serious manner. They want to conduct a conference. In this conference, the opinion of the farmers, who are producing tobacco, must also be taken into account. In order to send some tobacco farmers from the village level to this sort of conferences, we must get pressure on the administration. After having such a sort of attempt, we will let you know what is to be done by the Centre, in what way we have to proceed in this direction. Thanking You.

(3.1)

We focus our attention on the first 16 characters. Thus we have

Respected Madam! (3.2)

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

$$P = \begin{bmatrix} 217 & 133 & 162 & 151 \\ 133 & 131 & 163 & 133 \\ 132 & 64 & 212 & 129 \\ 132 & 129 & 148 & 79 \end{bmatrix} \tag{3.3}$$

Let us take a key matrix K and the key bunch matrix E in the form

$$K = \begin{bmatrix} 102 & 181 & 101 & 12 \\ 24 & 13 & 15 & 199 \\ 29 & 146 & 60 & 121 \\ 39 & 126 & 205 & 90 \end{bmatrix} \tag{3.4}$$

and

$$E = \begin{bmatrix} 47 & 23 & 19 & 235 \\ 67 & 99 & 109 & 49 \\ 221 & 195 & 205 & 39 \\ 187 & 155 & 235 & 41 \end{bmatrix} \tag{3.5}$$

On using the concept of the multiplicative inverse, mentioned in section 2, we get

$$D = \begin{bmatrix} 207 & 167 & 27 & 195 \\ 107 & 75 & 101 & 209 \\ 117 & 235 & 5 & 151 \\ 115 & 147 & 195 & 25 \end{bmatrix} \tag{3.6}$$

Now, on using the P, the K, and the E, given by (3.3)-(3.5), and applying the encryption algorithm, we get the ciphertext C in the form

$$C = \begin{bmatrix} 89 & 23 & 80 & 147 \\ 214 & 83 & 22 & 150 \\ 143 & 152 & 216 & 138 \\ 94 & 16 & 160 & 56 \end{bmatrix} \qquad (3.7)$$

On using the C, the D, and the K, given by (3.7), (3.6) and (3.4), and employing the decryption algorithm, we get back the original plaintext P, given by (3.3).This shows that the algorithm is perfect.Let us now study the avalanche effect. On replacing the 3rd row 1st column element 132 of the plaintext P, given by (3.3), by 164, we get a one binary bit change in the plaintext. On using this modified plaintext, the K, the E, and the encryption algorithm, we obtain the corresponding ciphertext C in the form

$$C = \begin{bmatrix} 114 & 232 & 131 & 22 \\ 255 & 157 & 65 & 45 \\ 71 & 66 & 24 & 128 \\ 195 & 76 & 125 & 149 \end{bmatrix} \qquad (3.8)$$

On comparing (3.7) and (3.8), after putting them in their binary form, we find that these two ciphertexts differ by 71 bits out of 128 bits.Let us now consider a one binary bit change in the key matrix K. To achieve this one, we change the 4th row 3rd column element from 205 to 204. On using this modified K, the plaintext P, the encryption key bunch matrix E, and the encryption algorithm, given in section 2, we get the corresponding ciphertext C in the form

$$C = \begin{bmatrix} 217 & 133 & 162 & 151 \\ 133 & 131 & 163 & 133 \\ 132 & 64 & 212 & 129 \\ 132 & 129 & 148 & 79 \end{bmatrix} \qquad (3.9)$$

On converting (3.9) into its binary form, and comparing the resulting matrix with the ciphertext matrix C, given in (3.7), after putting it in its binary form, we find that these two ciphertexts differ by 71 bits out of 128 bits.

From the above discussion, we conclude that the cipher is a potential one.

4. CRYPTANALYSIS

In information security, the study of cryptanalysis occupies a very important position. This ensures the strength of a cipher. The different types of cryptanalysis attacks available in the literature of the cryptography are

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

The analytical study of the first two attacks, ascertains the strength of a cipher. A cipher is generally designed [5] so that it sustains the first two attacks. However, one has to check the strength of the cipher in respect of the latter two attacks also. However, these two attacks are studied on the basis of intuitive ideas.Let us analyze the brute force attack. Here, we are having the key matrix K of size nxn and the encryption key bunch matrix E, which is also of the same size and containing the odd numbers lying in [1-255]. Thus, the size of the key space is

$$2^{8n^2} \times 2^{7n^2} = 2^{15n^2} = \left(2^{10}\right)^{1.5n^2} \approx \left(10^3\right)^{1.5n^2} = 10^{4.5n^2} \qquad (4.1)$$

On assuming that, the time required for the computation of the cipher with one key matrix and one key bunch matrix in the key space is 10^{-7} seconds, then the time needed for the execution of the cipher with all possible keys in the key space is

$$\frac{10^{4.5n^2} \times 10^{-7}}{365 \times 24 \times 60 \times 60} = 3.12 \times 10^{4.5n^2-15} \ \textit{years}. \qquad (4.2)$$

As we have taken n=4, the above time assumes the form 3.12 x 10^{57} years. As the time span required here is typically large, it is simply impossible to break the cipher by the brute force attack.Let us now consider the known plaintext attack. In this case, we know as many pairs of plaintext and ciphertext, as we require for carrying out the analysis. If we confine our analysis only to one round of the iteration process (r=1), then the basic equations governing the cipher are

P = (KP) mod 256, (4.3)

$$P = [\, e_{ij} \times p_{ij} \,] \bmod 256,\ i=1 \text{ to } n,\ j = 1 \text{ to } n, \tag{4.4}$$

$$P = \text{Permute}(P), \tag{4.5}$$

and

$$C = P. \tag{4.6}$$

Here, the C on the left hand side of the equation (4.6) is known to us. Thus we can have the P occurring on the left hand side of (4.5). On using this P and IPermute(), we can obtain the P on the right hand side of (4.5), which is the same as the P on the left hand side of (4.4). Though P on the right hand side of (4.3) is known to us, we cannot proceed further and hence this cipher cannot be broken by the known plaintext attack, even when r=1. In this analysis, as we have taken r=16, we can emphatically say that we cannot break this cipher by the known plaintext attack.In view of the complexity of the equations, governing the encryption process of this cipher, on account of the presence of the mod operation and the permutation, it is not at all possible either to choose a plaintext or to choose a ciphertext for breaking this cipher, even by adopting all intuitive ideas.
In the light of the above discussion, we conclude that this cipher is a strong one.

5. COMPUTATIONS AND CONCLUSIONS

In the present investigation, we have devoted our attention to the development of a block cipher, which includes a key matrix and a key bunch matrix, in the process of the encryption. Correspondingly, we have made use of the modular arithmetic inverse of the key matrix and the decryption key bunch matrix in the process of the decryption. The cryptanalysis carried out in this investigation, clearly shows that this cipher is a strong one, and it cannot be broken by any cryptanalytic attack.The programs required in this analysis are developed in Java.The plaintext, given by (3.1), containing 1225 characters, is divided into 77 blocks, wherein each block is containing 16 characters. In the last block, we have added 7 zeroes as characters so that it becomes a complete block.On using the entire plaintext (3.1), the key matrix K, the encryption key bunch matrix E, and the algorithm for the encryption, given in section 2, we get the corresponding ciphertext. Thus we have the same in (5.1)

In this cipher, as the key matrix K and the encryption key bunch matrix E are used for multiplying the plaintext, in each round of the iteration process, and permutation is used for shuffling the plaintext in a thorough manner, we have created diffusion and confusion in a significant manner so that the cipher becomes exceedingly strong. The cryptanalysis carried out in this investigation exhibits the strength of the cipher in a remarkable manner.

It may be noted here that his cipher can be extended for a key K and encryption key bunch matrix E of very large size, say 16x16, and then this analysis can be applied very conveniently for encryption of images.

REFERENCES

Journal Papers:

[1] Dr. V.U.K. Sastry, K.Shirisha, " A Block Cipher Involving a Key Matrix and a Key bunch Matrix, Supplemented with Mix", sent for publication.

[2] Lester Hill, (1929), "Cryptography in an algebraic alphabet", (V.36 (6), pp. 306-312.), American Mathematical Monthly.

[3] 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.

[4] 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.

Books:

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

89	23	80	147	214	83	22	150	143	152	216	138	94	16	160	56
50	49	218	120	142	101	112	136	141	161	217	150	104	216	37	142
96	110	229	33	240	93	130	94	160	125	69	80	29	126	166	127
247	73	49	225	0	91	67	103	150	164	198	64	198	40	238	202
103	83	192	31	63	229	126	153	132	47	122	89	187	23	118	79
26	219	52	194	87	166	213	56	88	218	174	54	158	15	108	36
134	255	188	190	253	134	75	121	147	205	172	163	167	247	9	13
132	243	142	226	94	82	202	38	68	40	224	153	88	120	175	178
4	119	197	225	92	7	189	54	49	6	118	0	245	216	142	242
0	19	192	142	43	30	36	48	171	115	83	178	220	120	126	31
244	38	96	120	114	147	25	51	195	116	58	162	76	213	28	96
146	30	223	2	225	192	213	127	99	39	74	221	103	0	7	63
195	80	42	79	111	234	86	229	254	64	8	53	128	201	73	79
198	243	169	133	26	250	214	9	193	146	163	224	142	87	107	238
155	5	35	240	231	229	246	2	197	165	13	247	162	80	6	142
17	217	82	85	93	112	142	168	170	25	222	24	107	62	210	150
32	107	26	235	150	135	179	231	195	171	3	41	55	66	130	112
115	2	238	28	12	105	178	86	64	218	165	76	232	170	151	20
151	18	105	157	252	38	57	233	236	160	147	179	183	249	253	18
213	190	45	37	195	71	2	20	74	136	163	45	112	119	188	162
240	145	231	131	185	158	123	170	225	99	30	16	88	94	13	146
101	49	54	144	209	211	186	83	19	62	86	239	144	193	236	19
1	157	183	12	83	101	74	171	78	61	154	180	49	238	3	101
139	190	64	2	213	68	113	144	193	22	92	17	209	100	201	69
252	168	178	114	12	71	131	73	185	132	190	44	255	248	78	22
250	191	105	170	75	68	122	233	86	212	252	231	197	118	86	124
118	121	232	243	96	201	133	16	129	7	133	138	130	144	129	19
193	38	192	73	29	139	54	159	247	215	36	241	200	107	223	100
84	255	206	140	183	234	27	57	169	149	152	103	223	98	246	242
206	7	109	194	114	162	102	101	77	120	7	212	225	37	249	99
163	56	114	248	69	236	233	232	229	55	186	61	94	211	17	250
186	185	40	119	147	31	163	202	128	51	115	102	160	232	157	232
118	123	150	235	113	120	190	32	237	77	183	15	253	15	1	232
60	90	126	59	89	153	197	84	65	229	174	102	125	244	90	104
11	34	77	198	244	175	102	62	131	166	156	191	80	222	156	94
46	174	40	253	147	51	192	242	47	116	235	61	92	58	243	10
58	116	163	133	168	119	24	171	130	224	213	149	82	38	189	44
128	234	167	133	251	11	55	44	159	19	20	185	221	201	137	159
46	24	102	6	57	176	107	1	241	233	110	109	52	124	187	23
6	55	68	53	75	221	116	249	130	139	12	57	138	201	255	213
90	62	159	212	176	175	17	15	248	79	176	247	137	46	54	210
118	127	108	63	180	118	60	167	54	172	115	67	103	33	178	29
247	218	240	177	42	153	78	108	236	92	109	165	157	88	218	120
189	220	131	201	150	191	239	24	31	22	219	43	30	54	158	29
16	82	21	39	187	199	41	198	84	220	162	119	247	86	246	67
32	88	225	189	200	110	83	5	231	9	172	97	27	213	74	31
130	134	151	191	121	160	47	38	160	161	32	70	156	193	93	247
29	164	0	22	104	131	34	155	101	25	216	232	171	229	208	251

(contd.)

218	162	193	168	75	247	81	76	113	24	192	254	198	18	96	181	
56	253	161	253	73	17	15	48	38	72	229	158	78	120	102	7	
39	100	131	199	94	169	225	78	129	223	244	163	82	47	230	204	
33	238	109	224	23	194	17	248	90	222	244	88	101	0	14	28	
239	25	43	25	128	210	40	61	154	112	243	250	124	150	165	138	
43	189	107	168	99	104	116	89	216	232	53	194	32	161	8	203	
95	15	103	131	29	104	170	221	53	54	1	114	50	55	105	39	
239	164	129	122	14	246	17	115	100	175	37	150	123	165	107	255	
45	135	127	221	196	126	86	25	110	194	128	96	103	130	152	231	
203	76	183	184	233	69	15	135	216	19	20	106	248	95	160	28	
55	159	224	42	157	234	122	61	137	127	121	153	158	132	83	207	
217	37	204	221	200	114	219	180	51	49	167	107	152	155	183	110	
21	87	16	248	5	223	159	65	45	187	57	13	234	67	191	91	
195	221	110	233	197	219	112	106	228	24	94	25	132	190	234	129	
89	81	159	23	91	230	119	116	237	175	89	230	26	81	188	133	
210	41	170	247	89	114	65	28	159	108	221	11	199	158	35	196	
228	69	53	85	98	223	105	243	128	141	8	106	131	169	10	172	
179	173	151	104	26	233	205	120	88	156	67	37	107	156	43	185	
41	117	119	63	33	193	191	194	194	221	54	245	161	170	88	207	(5.1)
3	77	149	30	5	120	231	211	21	136	222	242	181	58	135	167	
76	187	175	185	117	210	217	137	164	172	0	89	79	235	184	181	
5	203	34	99	173	127	235	112	0	73	98	66	58	7	175	77	
73	99	144	56	142	238	202	191	58	60	95	39	148	106	212	12	
35	107	216	51	198	128	151	106	163	111	172	48	69	125	15	140	
138	228	168	159	114	142	86	115	213	204	33	117	98	181	157	244	
35	131	130	203	76	225	41	155	93	202	108	10	134	246	210	46	
66	135	74	131	156	81	42	53	239	56	99	113	37	183	41	158	
83	67	170	237	98	29	151	139	53	104	27	70	104	42	57	191	
52	122	175	168	96	235	136	206	42	21	147	190	64	189	162	81	

Biographies and Photographs

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 Data Mining and Information Security.