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

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 developed a block cipher by extending the analysis of a Novel Block Cipher Involving a Key bunch Matrix and a Key-based Permutation and Substitution. Here we have include and additional key matrix, which is supplemented with xor operation. The cryptanalysis carried out in this investigation clearly indicates that this cipher cannot be broken by any attack.**

Keywords- Key; key bunch matrix; encryption; decryption; permutation; substitution; avalanche effect; cryptanalysis; xor operation

I. INTRODUCTION

In a recent investigation [1], we have developed a block cipher involving a key bunch matrix and including a pair of functions, called Permute() and Substitute(). In this analysis, we have seen that the permutation and the substitution, which depend effectively on a key, strengthen the cipher in a remarkable manner. This is all on account of the fact that the permutation and the substitution, induced into the plaintext at each and every stage in the iteration process, causes confusion and diffusion.

In the present investigation, our objective is to modify the afore-mentioned block cipher by introducing an additional key matrix supplemented with xor operation. The basic equation governing the encryption of this cipher can be written in the form

$$C = [\, c_{ij} \,] = ([\, e_{ij} \times p_{ij} \,] \bmod 256) \oplus F, \quad i=1 \text{ to } n,\ j = 1 \text{ to } n. \tag{1.1}$$

The corresponding equation describing decryption can be written in the form

$$P = [\, p_{ij} \,] = [\, d_{ij} \times (C \oplus F)_{ij} \,] \bmod 256, \quad i=1 \text{ to } n,\ j = 1 \text{ to } n. \tag{1.2}$$

Here, our interest is to examine, how the additional key matrix, F, would strengthen the cipher when supported by permuted and substitution.

Let us now present the plan of the paper. In section 2, we introduce the development of the cipher. Here, we depict the flowcharts and write the algorithms required in this investigation. Then, we mention the basic ideas of the key based permutation and substitution. In section 3, we mention an illustration of the cipher, and discuss the avalanche effect. We study the cryptanalysis, in section 4. Finally, we deal with the computations carried out in this analysis, and draw conclusions, in section 5.

II. DEVELOPMENT OF THE CIPHER

Consider a plaintext, which can be written in the form of a square matrix P, given by

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

Let us take a key bunch matrix E, given by

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

On using the concept of the multiplicative inverse [2], we get d_{ij} corresponding to each e_{ij} . Thus we have the decryption key bunch matrix D, given by

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

Here, it is to be noted that, all the e_{ij} and d_{ij} are odd numbers which lie in the interval [1-255].

The flowcharts concerned to the encryption and the decryption are drawn 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,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. $p_{ij} = (e_{ij} \times p_{ij}) \bmod 256$
   }
   }
6. P=[p_{ij}] $\oplus$ F
7. P=Permute(P)
8. P=Substitute(P)
   }
8. C=P
9. 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. $c_{ij} = [d_{ij} \times (c_{ij} \oplus f_{ij})] \bmod 256$
   }
   }
9. C=[c_{ij}]
   }
10. P=C
11. Write (P)

In this analysis, r denotes the number of rounds in the iteration process, and it is taken as 16.

The functions Permute() and Substitute(), which are utilized in encryption, depend upon a key. Let us choose the key, K, in the form

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

Keeping the serial numbers and the order of the elements in the key, in view, we construct a table of the form given in Table-1.

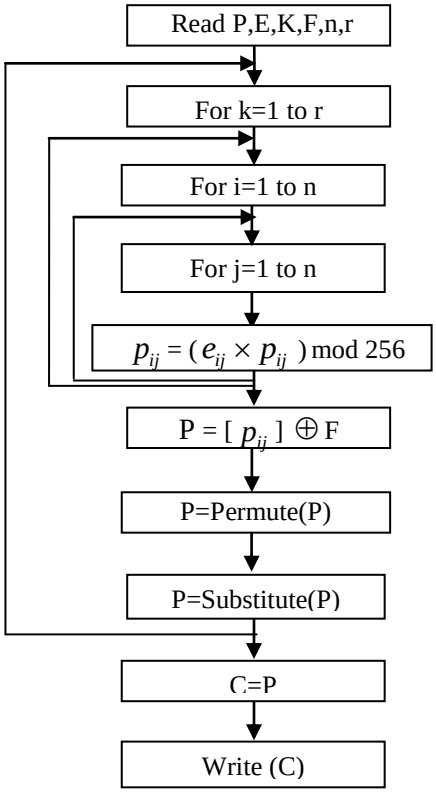

Fig.1 Flowchart for Encryption

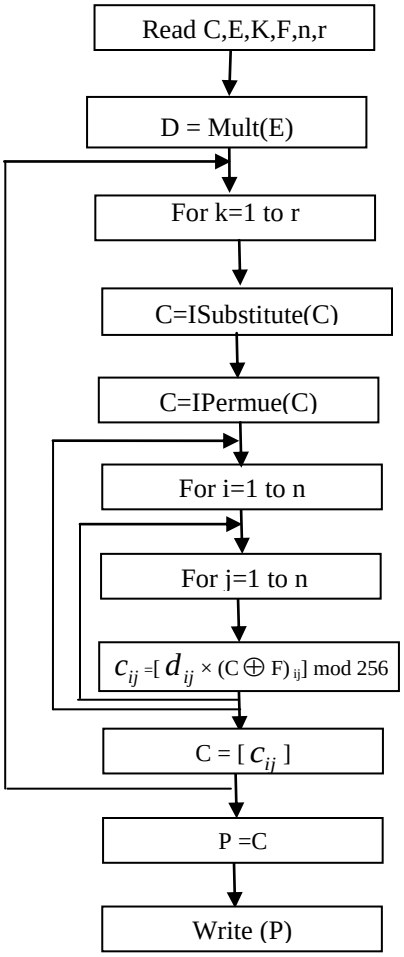

Fig.2 Flowchart for Decryption

TABLE-1. 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

The process of permutation can be explained as follows.

Let x_i, i=1 to 16, be a set of 16 numbers. As the table is suggesting (looking at the first row and the third row), we interchange x_1 with x_{12}, x_2 with x_3, x_4 with x_6, x_5 with x_{16}, x_7 with x_8, x_9 with x_{13}, and x_{14} with x_{15}. It may be noted here that we need not interchange any other numbers as they are already subjected to change in a way. Keeping this basic idea in view, let us now consider the plaintext matrix P = [p_{ij}], i=1 to n, j=1 to n, (after xoring with F) in any round of the iteration process. Considering the first two rows of this matrix and representing the elements p_{ij} in their binary form, and writing the binary bits in the vertical manner, we get a matrix of size 16xn. On dividing this matrix into sub-matrices, where each one of size 16x16, and performing the interchange of rows (firstly) and columns (subsequently), as is done in the case of numbers x_i , i=1 to 16, we get the corresponding permuted matrix, in the case of each sub-matrix. On applying the same procedure for the other sub-matrices also, we ultimately get n/16 sub-matrices. On representing the binary bits in terms of decimal numbers (converting 8 binary bits in a row as a decimal number), we get a 2xn matrix. On adopting the same procedure on the subsequent pairs of this matrix, we complete the permutation process. However, it is to be remembered that n must be divisible by 16. In case, if n<16, that is say, n=4, then a plaintext matrix of size 4x4 can be written as a matrix of size 8x16, by writing each decimal number as binary bits in a column. Then the procedure of swapping, applied for numbers, can be applied here, for rows firstly and for columns nextly.

However, in the case of rows, we restrict our interchanging process only to 8 rows. Then, on representing the binary bits in terms of decimal numbers (considering the bits in a row-wise manner) we get the permuted matrix. This completes t he process of permutation.

The process of substitution can be mentioned as follows. In the EBCDIC code, the characters can be represented in terms of a table of size 16x16, containing numbers 0 to 255, in a sequential manner. On swapping rows, firstly, and columns, nextly, as it is already done in the case of the numbers x_1 to x_{16}, we get a new table (see Table-2).

On using the Table-2, we perform substitution, by noting the correspondence between the number in the plaintext, the number in the EBCDIC table and hence the number in the substitution table. For clarity if this substitution process, we refer to [1].

The functions IPermute() and ISubstitute(), used in the decryption process, denote the reverse processes of the Permute() and the Substitute(). The function Mult() is used to find the decryption key bunch matrix D for the given E.

III. ILLUSTRATION OF THE CIPHER AND THE AVALANCHE EFFECT

Consider the plaintext given below.

Dear Madam! I have received your letter. Please do not run away from our country in that manner. I am coming within this month. I will not continue my Ph.D. programme. I may leave this research activity but I cannot leave you. It is indeed a surprise. Though there was no response from the selection committee for a span of one year, very recently I got selected in our country for IAS. I think I am lucky. Tell you father and mother about this news and tell them in a nice manner that you are running p8third month. I hope that all these issues will end up very soon and we will become one undoubtedly. Tell my father and mother that I am coming there. Yours loving husband

(3.1)

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

Dear Madam! I ha (3.2)

On using the EBCDIC code, we get

$$P = \begin{bmatrix} 196 & 133 & 129 & 153 \\ 64 & 212 & 129 & 132 \\ 129 & 148 & 79 & 64 \\ 201 & 64 & 136 & 129 \end{bmatrix}. \quad (3.3)$$

Let us take the key bunch matrix E in the form

$$E = \begin{bmatrix} 199 & 23 & 67 & 211 \\ 67 & 91 & 93 & 5 \\ 11 & 19 & 51 & 145 \\ 109 & 223 & 251 & 5 \end{bmatrix}. \quad (3.4)$$

On using the concept of the multiplicative inverse, we have the decryption key bunch matrix D in the form

$$D = \begin{bmatrix} 247 & 167 & 107 & 91 \\ 107 & 211 & 245 & 205 \\ 163 & 27 & 251 & 113 \\ 101 & 31 & 51 & 205 \end{bmatrix}. \quad (3.5)$$

187	178	177	181	191	179	183	182	188	185	186	176	184	190	189	180
43	34	33	37	47	35	39	38	44	41	42	32	40	46	45	36
27	18	17	21	31	19	23	22	28	25	26	16	24	30	29	20
91	82	81	85	95	83	87	86	92	89	90	80	88	94	93	84
51	242	241	245	255	243	247	246	252	249	250	240	248	254	253	244
59	50	49	53	63	51	55	54	60	57	58	48	56	62	61	52
123	114	113	117	127	115	119	118	124	121	122	112	120	126	125	116
107	98	97	101	111	99	103	102	108	105	106	96	104	110	109	100
203	194	193	197	207	195	199	198	204	201	202	192	200	206	205	196
155	146	145	149	159	147	151	150	156	153	154	144	152	158	157	148
171	162	161	165	175	163	167	166	172	169	170	160	168	174	173	164
11	2	1	5	15	3	7	6	12	9	10	0	8	14	13	4
139	130	129	133	143	131	135	134	140	137	138	128	136	142	141	132
235	226	225	229	239	227	231	230	236	233	234	224	232	238	237	228
219	210	209	213	223	211	215	214	220	217	218	208	216	222	221	212
75	66	65	69	79	67	71	70	76	73	74	64	72	78	77	68

TABLE-2 KEY BASED SUBSTITUTION

The additional key matrix F is taken in the form

$$F = \begin{bmatrix} 222 & 243 & 122 & 45 \\ 56 & 22 & 100 & 99 \\ 104 & 76 & 45 & 11 \\ 9 & 22 & 25 & 67 \end{bmatrix}. \quad (3.6)$$

Now, on making use of the plaintext P, the encryption key bunch matrix E and the additional key matrix F, and applying the encryption algorithm, given in section 2, we get the ciphertext matrix C in the form

$$C = \begin{bmatrix} 88 & 2 & 165 & 241 \\ 47 & 226 & 95 & 110 \\ 214 & 121 & 129 & 163 \\ 104 & 97 & 195 & 215 \end{bmatrix}. \quad (3.7)$$

On using this C, the F, and the decryption key bunch matrix D, given by (3.5), and the decryption algorithm, given in section 2, we get back the plaintext P, which is in the form (3.3).

Now let us study the avalanche effect. On replacing the 4th row 4th column element, 129 in the plaintext (3.3) by 193, we have a one binary bit change in the plaintext. On using this modified plaintext, the E, the F, and the encryption algorithm, we get the new ciphertext in the form, given by (3.8).

On comparing (3.8) and (3.7), after converting them into their binary form, we notice that there is a change of 72 bits out of 128 bits. This shows that the cipher is a strong one.

$$C = \begin{bmatrix} 1 & 198 & 243 & 34 \\ 189 & 43 & 134 & 140 \\ 89 & 195 & 102 & 168 \\ 149 & 148 & 254 & 196 \end{bmatrix}. \quad (3.8)$$

Now, let us have one binary bit change in the key bunch matrix E. To this end, we replace the 3rd row 2nd column element 19 in E by 18. On using this modified E, the original P, given by (3.3), and the F, given by (3.6), and applying the encryption algorithm, we get the corresponding ciphertext C, in the form

$$C = \begin{bmatrix} 154 & 160 & 102 & 158 \\ 173 & 29 & 134 & 243 \\ 236 & 190 & 127 & 195 \\ 209 & 188 & 48 & 241 \end{bmatrix}. \quad (3.9)$$

Now, let us convert (3.7) and (3.9) into their binary form and compare them. From this, we find that these two ciphertexts differ by 74 bits out of 128 bits. This also shows that the cipher is having appreciable strength.

Now, on making use of the plaintext P, the encryption key bunch matrix E and the additional key matrix F, and applying the encryption algorithm, given in section 2, we get the ciphertext matrix C in the form

On using this C, the F, and the decryption key bunch matrix D, given by (3.5), and the decryption algorithm, given in section 2, we get back the plaintext P, which is in the form (3.3).

Now let us study the avalanche effect. On replacing the 4th row 4th column element, 129 in the plaintext (3.3) by 193, we have a one binary bit change in the plaintext. On using this modified plaintext, the E, the F, and the encryption algorithm, we get the new ciphertext in the form

Now, let us convert (3.7) and (3.9) into their binary form and compare them. From this, we find that these two ciphertexts differ by 74 bits out of 128 bits. This also shows that the cipher is having appreciable strength.

IV. CRYPTANALYSIS

The study of cryptanalysis plays a prominent role in the development of every cipher. The different types of attacks that are available in the literature of cryptography are

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

Generally, every algorithm is designed [2] such that it withstands the first two attacks. The cipher is also examined in a thorough manner, by using all possible intuitive ideas, in the case of the latter two attacks.

In this analysis, we have the key bunch matrix E, whose size is nxn. Besides this, we have the additional key matrix F, whose size is also nxn. In addition to these two, we have the key matrix K which is used in the development of permutation and substitution processes. In view of all these three, the size of the key space is

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

On assuming that, we require 10^{-7} seconds for computation with one set of-n keys in the key space, then the time required for all such possible set s 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 our present analysis, as 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 time is very large, it is simply impossible to break this cipher by the brute force attack.

Let us now examine the known plaintext attack. In order to carry out this approach, we have plaintext and ciphertext pairs, as many as we want, at our disposal. If we focus our attention on only one round of the iteration process, that is if r=1, then the basic equations governing the encryption process are given by

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

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

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

and

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

In this attack, the ciphertext C in (4.4), is known to us. On using this one, we can know the P, occurring in the left side of (4.3). As key is unknown, we do not know ISubstitute(). Hence P occurring on the right hand side of (4.3) cannot be determined. Hence this cipher cannot be broken by the known plaintext attack. Luckily, if key K is known (a very stray case), then we can obtain P, occurring on the left hand side of (4.1). Then, though p_{ij} is known to us, we cannot determine the e_{ij}, by any means, as the equation (4.1) is containing several unknowns related to F, and is including mod and xor operations. Thus this cipher cannot be broken by the known plaintext attack, even when r=1, and the key matrix K, used in the permutation process is known to the attacker.

In view of the equations, involved in the encryption process, we do not find any possibility to choose either a plaintext or a ciphertext for breaking this cipher.

In the light of the above facts, we conclude that this cipher is a very strong one.

V. Computations and Conclusions

In this investigation, we have developed a block cipher involving a key bunch matrix and an additional key matrix, and involving key-based permutation and substitution. The strength of the cipher is highly remarkable due to permutation and substitution, and it is further supplemented with the additional key matrix.

The programs for encryption and decryption are written in Java.

In order to carry out the encryption of the entire plaintext, given by (3.1), we use a large size encryption key bunch matrix EK of size 16x16. Along with this, we have taken an additional key matrix FK, which is also of the same size 16x16. The EK and FK are given below in (5.1) and (5.2).

$$EK = \begin{bmatrix}
125 & 171 & 129 & 101 & 141 & 225 & 251 & 47 & 69 & 123 & 121 & 65 & 177 & 5 & 131 & 243 \\
213 & 29 & 227 & 127 & 61 & 107 & 195 & 145 & 83 & 89 & 221 & 167 & 151 & 79 & 125 & 167 \\
3 & 41 & 213 & 161 & 35 & 131 & 203 & 125 & 125 & 41 & 177 & 231 & 15 & 21 & 93 & 111 \\
209 & 83 & 65 & 203 & 183 & 163 & 165 & 59 & 123 & 15 & 113 & 157 & 249 & 243 & 171 & 113 \\
195 & 45 & 63 & 23 & 191 & 197 & 25 & 129 & 177 & 151 & 221 & 217 & 21 & 173 & 31 & 185 \\
103 & 17 & 47 & 3 & 223 & 223 & 167 & 13 & 43 & 241 & 173 & 117 & 31 & 113 & 227 & 93 \\
37 & 219 & 195 & 175 & 199 & 83 & 79 & 217 & 233 & 217 & 169 & 253 & 127 & 75 & 163 & 243 \\
215 & 111 & 79 & 159 & 193 & 5 & 231 & 117 & 55 & 55 & 63 & 119 & 249 & 205 & 193 & 13 \\
231 & 243 & 199 & 115 & 201 & 67 & 173 & 195 & 19 & 191 & 17 & 145 & 219 & 155 & 39 & 241 \\
251 & 223 & 231 & 95 & 105 & 201 & 119 & 51 & 181 & 229 & 181 & 167 & 247 & 153 & 225 & 149 \\
37 & 183 & 253 & 177 & 117 & 33 & 17 & 231 & 163 & 83 & 195 & 157 & 223 & 13 & 95 & 95 \\
183 & 241 & 95 & 53 & 247 & 117 & 169 & 23 & 27 & 107 & 85 & 167 & 215 & 171 & 203 & 139 \\
49 & 221 & 127 & 69 & 127 & 245 & 73 & 3 & 113 & 125 & 237 & 45 & 55 & 115 & 241 & 221 \\
213 & 85 & 21 & 15 & 21 & 205 & 85 & 203 & 105 & 235 & 155 & 5 & 105 & 153 & 109 & 135 \\
223 & 133 & 239 & 181 & 127 & 157 & 77 & 243 & 17 & 129 & 133 & 161 & 11 & 65 & 93 & 169 \\
91 & 59 & 171 & 201 & 53 & 91 & 31 & 169 & 203 & 113 & 181 & 125 & 151 & 165 & 245 & 51
\end{bmatrix} \quad (5.1)$$

and

$$FK = \begin{bmatrix} 91 & 46 & 145 & 165 & 147 & 49 & 59 & 169 & 175 & 168 & 103 & 104 & 148 & 178 & 111 & 70 \\ 10 & 203 & 14 & 102 & 66 & 123 & 116 & 111 & 21 & 15 & 196 & 54 & 130 & 244 & 239 & 244 \\ 196 & 118 & 21 & 164 & 34 & 129 & 100 & 230 & 170 & 7 & 247 & 118 & 79 & 59 & 79 & 221 \\ 38 & 189 & 221 & 142 & 11 & 39 & 142 & 255 & 168 & 49 & 78 & 150 & 157 & 183 & 101 & 161 \\ 145 & 139 & 227 & 131 & 17 & 224 & 116 & 99 & 108 & 144 & 176 & 161 & 50 & 35 & 105 & 20 \\ 150 & 211 & 123 & 240 & 174 & 55 & 101 & 210 & 141 & 87 & 83 & 246 & 46 & 70 & 53 & 46 \\ 108 & 46 & 80 & 112 & 172 & 232 & 228 & 69 & 97 & 232 & 166 & 102 & 70 & 63 & 94 & 18 \\ 18 & 214 & 79 & 151 & 79 & 250 & 10 & 116 & 81 & 115 & 228 & 77 & 121 & 12 & 153 & 167 \\ 131 & 133 & 132 & 246 & 53 & 94 & 132 & 39 & 151 & 183 & 207 & 36 & 194 & 222 & 227 & 70 \\ 141 & 193 & 91 & 210 & 120 & 146 & 152 & 224 & 202 & 110 & 34 & 0 & 73 & 176 & 4 & 0 \\ 198 & 2 & 215 & 20 & 141 & 203 & 183 & 92 & 214 & 217 & 37 & 140 & 141 & 161 & 211 & 248 \\ 25 & 70 & 49 & 234 & 95 & 31 & 25 & 99 & 200 & 248 & 251 & 243 & 15 & 149 & 206 & 78 \\ 116 & 135 & 103 & 157 & 37 & 64 & 242 & 116 & 246 & 219 & 17 & 71 & 249 & 157 & 127 & 34 \\ 17 & 148 & 51 & 32 & 121 & 45 & 163 & 192 & 14 & 166 & 62 & 211 & 64 & 156 & 40 & 50 \\ 220 & 210 & 244 & 208 & 41 & 113 & 132 & 254 & 115 & 174 & 22 & 231 & 196 & 188 & 67 & 126 \\ 121 & 96 & 4 & 234 & 70 & 102 & 186 & 145 & 133 & 69 & 222 & 158 & 239 & 30 & 75 & 146 \end{bmatrix} \quad (5.2)$$

The entire plaintext, given by (3.1), is divided into 3 blocks, wherein each block is of size 16x16. In the 3rd block, we have appended 95 zeroes as characters, so that we make it a complete block. On using EK, FK, in the place of E and F, in the encryption algorithm, we carry out the encryption process 3 times, so that the complete plaintext is converted into the corresponding ciphertext. This ciphertext is given by (5.3).

The EK and FK are encrypted by using the E, the F, and applying the encryption algorithm. The resulting ciphertexts of the keys EK and FK are as follows, in (5.4) and (5.5).

These are transmitted to the receiver by the sender. In addition to these, the key bunch matrix E, the additional key matrix F, the key K used in the processes permutation and substitution are sent by the sender to the receiver, in a secure manner. The number of additional characters appended in the last block is also informed to the receiver.

38	148	35	233	157	94	147	31	252	129	27	155	11	231	166	169
227	99	59	188	89	55	67	212	75	208	216	147	227	18	217	166
109	69	91	40	101	193	98	1	60	135	125	188	51	73	45	59
24	125	41	75	17	36	157	134	53	226	20	204	25	248	99	200
6	170	236	237	98	229	205	189	41	162	91	140	73	182	9	78
212	221	116	182	225	53	203	180	252	188	235	233	247	88	149	86
66	213	88	95	157	43	93	182	30	177	134	138	98	231	199	79
241	156	13	75	4	115	91	86	228	10	138	18	244	149	8	0
81	145	34	125	247	160	62	115	40	239	253	1	17	37	113	74
116	83	51	136	116	57	107	126	236	164	167	104	18	200	83	18
0	126	111	20	47	152	172	104	81	138	65	210	181	145	206	78
53	44	149	99	233	58	76	209	40	33	42	224	179	221	160	90
223	201	57	138	120	212	159	105	173	176	164	233	198	118	108	126
134	55	93	84	231	232	250	150	28	201	170	51	8	112	254	139
28	37	30	175	46	13	75	10	139	102	118	118	39	97	121	241
44	104	224	190	16	209	148	231	150	83	22	252	166	156	19	203

94	156	21	226	84	41	36	223	26	192	97	94	125	189	59	237
231	99	144	43	241	159	157	217	34	186	20	244	191	43	85	152
5	155	0	98	149	218	53	3	172	204	84	118	108	12	55	76
151	99	60	175	243	251	17	35	228	141	243	153	49	174	240	181
94	139	65	240	120	95	148	93	108	245	248	240	102	58	108	8
40	96	157	14	62	24	190	164	167	227	8	251	109	45	97	187
43	2	132	243	32	40	78	173	103	176	38	58	163	124	185	233
242	73	171	62	202	177	208	202	3	213	221	121	115	38	96	154
89	203	141	46	252	18	149	99	165	125	22	239	46	36	52	54
121	175	143	164	45	196	2	163	2	80	208	112	229	196	97	56
253	217	107	97	162	180	229	220	142	161	225	229	109	239	177	19
98	92	205	89	31	151	4	68	116	9	171	217	100	53	247	110
225	136	232	70	124	192	22	140	188	211	109	134	97	203	41	238
51	123	20	89	179	222	63	93	70	92	203	170	185	35	52	90
167	116	159	7	174	158	159	82	118	160	73	39	110	31	75	179
26	247	244	28	163	166	11	144	203	86	180	33	200	138	201	181

12	181	81	91	149	203	173	223	77	216	176	223	5	211	181	161	
39	123	8	93	233	6	230	76	127	189	226	144	34	83	134	221	
251	138	37	98	24	37	227	199	123	24	134	133	140	186	132	8	
114	170	231	225	178	141	116	190	89	63	243	59	200	61	84	247	
49	192	79	209	105	47	144	254	206	42	178	254	228	204	220	49	
9	167	2	213	179	134	249	23	193	100	28	205	62	69	119	91	(5.3)
109	6	127	88	45	2	147	226	135	49	240	209	246	206	224	125	
71	185	146	5	72	206	99	67	233	152	192	253	13	154	215	36	
67	22	233	65	248	236	180	223	114	45	4	195	106	215	123	135	
0	31	236	22	169	81	206	62	34	170	194	54	77	233	160	141	
153	196	90	225	27	31	225	226	94	179	143	130	195	44	64	82	
255	30	13	203	62	194	21	17	106	201	56	2	71	210	24	231	
17	119	167	107	156	63	62	233	182	46	160	38	58	50	165	173	
78	175	80	75	113	233	225	172	42	176	15	42	1	132	238	95	
144	42	54	3	190	173	131	50	50	200	229	128	161	103	47	37	
85	203	59	113	31	245	244	190	62	39	37	176	196	123	66	129M	

The cryptanalysis carried out in this investigation strongly indicate that this cipher is a potential one and it can be applied for the transmission of text of any size and gray level/color images.

2	95	7	118	130	53	132	123	10	29	82	113	143	155	35	59	
70	109	146	221	38	152	190	52	18	202	30	202	95	137	241	108	
7	166	2	21	200	105	36	1	63	251	128	219	29	149	6	185	
222	220	147	41	44	159	82	136	151	205	190	65	210	146	172	107	
30	241	25	80	94	28	65	18	241	112	50	238	98	5	204	255	
42	149	71	197	104	106	49	71	180	154	87	213	137	97	152	210	
5	148	246	66	203	164	188	168	232	105	222	143	61	40	255	81	
89	177	154	111	224	201	213	213	14	88	184	245	226	74	58	179	(5.4)
148	70	31	251	7	1	126	100	11	249	244	73	240	58	212	23	
174	150	143	158	163	155	137	239	139	96	130	82	244	105	87	23	
1	63	184	102	93	113	70	156	185	241	173	157	58	15	216	17	
202	1	47	213	55	48	231	37	13	38	35	19	157	40	21	68	
61	71	255	44	109	131	140	98	182	14	95	176	239	38	129	113	
111	235	208	238	192	46	187	5	63	75	131	23	114	114	204	75	
49	230	221	242	247	131	6	142	45	198	167	221	227	106	129	8	
85	3	99	170	211	133	6	225	234	109	187	240	237	200	53	139	

and

$$\begin{bmatrix}
91 & 46 & 145 & 165 & 147 & 49 & 59 & 169 & 175 & 168 & 103 & 104 & 148 & 178 & 111 & 70 \\
10 & 203 & 14 & 102 & 66 & 123 & 116 & 111 & 21 & 15 & 196 & 54 & 130 & 244 & 239 & 244 \\
196 & 118 & 21 & 164 & 34 & 129 & 100 & 230 & 170 & 7 & 247 & 118 & 79 & 59 & 79 & 221 \\
38 & 189 & 221 & 142 & 11 & 39 & 142 & 255 & 168 & 49 & 78 & 150 & 157 & 183 & 101 & 161 \\
145 & 139 & 227 & 131 & 17 & 224 & 116 & 99 & 108 & 144 & 176 & 161 & 50 & 35 & 105 & 20 \\
150 & 211 & 123 & 240 & 174 & 55 & 101 & 210 & 141 & 87 & 83 & 246 & 46 & 70 & 53 & 46 \\
108 & 46 & 80 & 112 & 172 & 232 & 228 & 69 & 97 & 232 & 166 & 102 & 70 & 63 & 94 & 18 \\
18 & 214 & 79 & 151 & 79 & 250 & 10 & 116 & 81 & 115 & 228 & 77 & 121 & 12 & 153 & 167 \\
131 & 133 & 132 & 246 & 53 & 94 & 132 & 39 & 151 & 183 & 207 & 36 & 194 & 222 & 227 & 70 \\
141 & 193 & 91 & 210 & 120 & 146 & 152 & 224 & 202 & 110 & 34 & 0 & 73 & 176 & 4 & 0 \\
198 & 2 & 215 & 20 & 141 & 203 & 183 & 92 & 214 & 217 & 37 & 140 & 141 & 161 & 211 & 248 \\
25 & 70 & 49 & 234 & 95 & 31 & 25 & 99 & 200 & 248 & 251 & 243 & 15 & 149 & 206 & 78 \\
116 & 135 & 103 & 157 & 37 & 64 & 242 & 116 & 246 & 219 & 17 & 71 & 249 & 157 & 127 & 34 \\
17 & 148 & 51 & 32 & 121 & 45 & 163 & 192 & 14 & 166 & 62 & 211 & 64 & 156 & 40 & 50 \\
220 & 210 & 244 & 208 & 41 & 113 & 132 & 254 & 115 & 174 & 22 & 231 & 196 & 188 & 67 & 126 \\
121 & 96 & 4 & 234 & 70 & 102 & 186 & 145 & 133 & 69 & 222 & 158 & 239 & 30 & 75 & 146
\end{bmatrix} \quad (5.5)$$

REFERENCES

[1] Dr.V.U.K.Sastry, K.Shirisha, "A Novel Block Cipher Involving a Key Bunch Matrix and a Key-based Permutation and Substitution", in International Journal of Advanced Computer Science and Applications(IJACSA), Vol. 3, No. 12, Jan 2012, pp.16-122.

[2] 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 87 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 9 research papers in International Journals. She stood University topper in the M.Tech.(CSE).