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

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

The corresponding equation describing decryption can be written in the form

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

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

Let us take a key bunch matrix E, given by

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

\[ D = \{ d_{ij} \}, \quad i=1 \text{ to } n, \quad j=1 \text{ to } n. \] (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. \[ p_{ij} = (e_{ij} \times p_{ij}) \mod 256 \]
7. \[ P = \{ p_{ij} \} \oplus F \]
8. \[ P = \text{Permute}(P) \]
9. \[ P = \text{Substitute}(P) \]
10. \[ C = P \]
11. \[ \text{Write}(P) \]

Algorithm for Decryption

1. Read C,E,K,F,n,r
2. \[ D = \text{Mult}(E) \]
3. For \( k = 1 \) to \( r \)
   \{ \[ C = \text{ISubstitute}(C) \]
   \[ C = \text{IPermute}(C) \]
   For \( i = 1 \) to \( n \)
   \{ \[ P_{ij} = (e_{ij} \times p_{ij}) \mod 256 \]
   \[ P = \{ p_{ij} \} \oplus F \]
   \[ P = \text{Permute}(P) \]
   \[ P = \text{Substitute}(P) \]
   \[ C = P \]
   \[ \text{Write}(C) \] \}

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

The functions \( \text{Permute()} \) and \( \text{Substitute()} \), 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.
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 submatrices, 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 submatrix. On applying the same procedure for the other submatrices also, we ultimately get $n/16$ submatrices. 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 process 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 the 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 $x_i$ 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

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

On using the EBCDIC code, we get

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

Let us take the key bunch matrix E in the form

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

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

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

(3.2)

(3.3)

(3.4)

(3.5)

www.ijacsa.thesai.org
The additional key matrix \( F \) is taken in the form
\[
F = \begin{bmatrix}
222 & 243 & 122 & 45 \\
56 & 22 & 100 & 99 \\
104 & 76 & 45 & 11 \\
9 & 22 & 25 & 67
\end{bmatrix}.
\] (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
\[
C = \begin{bmatrix}
222 & 243 & 122 & 45 \\
56 & 22 & 100 & 99 \\
104 & 76 & 45 & 11 \\
9 & 22 & 25 & 67
\end{bmatrix}.
\] (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.

\[
C = \begin{bmatrix}
1 & 198 & 243 & 34 \\
189 & 43 & 134 & 140 \\
89 & 195 & 102 & 168 \\
149 & 148 & 254 & 196
\end{bmatrix}.
\] (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
\[
C = \begin{bmatrix}
154 & 160 & 102 & 158 \\
173 & 29 & 134 & 243 \\
236 & 190 & 127 & 195 \\
209 & 188 & 48 & 241
\end{bmatrix}.
\] (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. CRYPTOANALYSIS

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

\[ 2^{7n^2} \times 2^{5n^2} \times 2^{128} = 2^{7n^2+5n^2+128} = 2^{15n^2+128} \]

\[ \approx (10)^{1.5n^2+128} = 10^{4.5n^2+38.4} \]

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

\[ \frac{10^{4.5n^2+38.4} \times 10^{-7}}{365 \times 24 \times 60 \times 60} = 3.12 \times 10^{45n^2+23.4} \text{years.} \]

In our present analysis, as n=4, the time for computation with all possible sets of keys in the key space is

\[ 3.12 \times 10^{95.4} \text{years.} \]

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

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

\[ P = \text{Permute}(P), \ (4.2) \]

\[ P = \text{Substitute}(P), \ (4.3) \]

\[ C = P \ (4.4) \]

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).

[Table of EK and FK values]

and

www.ijacsa.thesai.org
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.
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.
and

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  (5.5)
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

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).