A Block Cipher Involving a Key Matrix and a Key bunch Matrix, Supplemented with Mix

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

Abstract: In this paper, we have developed a block cipher, which includes a key matrix and a key bunch matrix. In this, we have used the basic concepts of Hill cipher and the concept of the multiplicative inverse. This analysis is supplemented with a function, called Mix(), for creating confusion. The cryptanalysis carried out in this investigation firmly indicates that this cipher is unbreakable by all possible attacks, available in the literature.

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

1. INTRODUCTION

The development of the Hill Cipher [1], which involves a key matrix and the modular arithmetic inverse of the key matrix, has been a pioneering area of research in cryptography. The basic equations governing the Hill cipher are

\[ C = (KP) \mod 26, \text{and} \]
\[ P = K^{-1}C \mod 26, \]

where \( K^{-1} \) is the modular arithmetic inverse [2] of the \( K \). The \( K \) and the \( K^{-1} \) are related by the equation

\[ (KK^{-1}) \mod 26 = I, \]

where \( I \) is the unit matrix. Here mod 26 is used as attention is confined to the English alphabet, which contains 26 characters.

In the literature of the cryptography, it is well-known that this cipher can be broken by the known plaintext attack [2]. However, the recent literature is replete with a number of investigations [3-11], wherein the Hill cipher is modified and strengthened by introducing iteration, permutation and substitution. In the recent development of the cryptography, we have designed several block ciphers by introducing a key bunch matrix [12-18] in the process of the encryption and carried out the decryption by obtaining the multiplicative inverse of each key in the key bunch matrix. This cipher is strengthened by including the functions, namely, Mix(), Permute() and Substitute(), which alter the plaintext in each round of the iteration process.

In the present paper, our objective is to develop a block cipher which includes the basic ideas of the Hill cipher and the basic concepts of the block cipher which we have developed in the recent past. The strength of the cipher is expected to enhance significantly as we have blended the basic ideas of both the ciphers. Here, our interest is to see how the diffusion and the confusion of the binary bits, in each round of the iteration process, are enhanced by the superposition of one process (in the development of the block cipher) over the other.

Let us mention the plan of the paper. Section 2 is devoted to the development of the cipher. In this, we have presented the flowcharts and the algorithms pertinent to this cipher. In section 3, we have dealt with an illustration of the cipher and discussed the avalanche effect, which gives an idea about the strength of the cipher. Then we have carried out the cryptanalysis, in section 4. Lastly, in section 5, we have mentioned about the computations carried out in this investigation, and have brought out the salient features of this cipher.

II. DEVELOPMENT OF THE CIPHER

Consider a plaintext \( P \), which can be written in the form of a square matrix of size \( n \), given by

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

(2.1)

As we have employed the EBCDIC code in writing this matrix, each element in this matrix lies in \([0-255]\).

Let \( K \) be a key matrix given by

\[ K = [k_{ij}], i=1 \text{ to } n, j=1 \text{ to } n. \]

(2.2)

Let us have an encryption key bunch matrix \( E \), given by
A Block Cipher Involving A Key Matrix...

E = \[
\begin{bmatrix}
  e_{ij} \\
  \end{bmatrix}
\] , i=1 to n, j=1 to n,

(2.3)

The basic equations governing this cipher, which include the concepts of the modular arithmetic inverse and the multiplicative inverse, can be written in the form

P = (KP) mod 256,

(2.4)

P = [ e_{ij} \times p_{ij} ] mod 256 , i=1 to n, j = 1 to n,

(2.5)

C = P,

(2.6)

and

C=[ c_{ij} ]=[ d_{ij} \times c_{ij} ]mod 256, i=1 to n, j=1 to n,

(2.7)

C = ( K^{-1}C) mod 256,

(2.8)

P = C.

(2.9)

Here, the equations (2.4) – (2.6) govern the encryption process, and (2.7) – (2.9) describe the decryption process. In the above equations, C denotes the ciphertext, and the \( e_{ij} \) and the \( d_{ij} \) are governed by the relation

\( ( e_{ij} \times d_{ij} ) \mod 256 = 1, \)

(2.10)

It is to be noted that both \( e_{ij} \) and \( d_{ij} \) are odd numbers lying in [1-255], and each \( d_{ij} \) can be determined for the corresponding chosen \( e_{ij} \).

The flowcharts depicting the cipher can be drawn as shown in Figs. 1 and 2.
The algorithms corresponding to the afore-mentioned flowcharts can be written in the form shown below.

### 2.1 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 = Mix(P)
   9. C=P
10. Write(C)

### 2.2 Algorithm for Decryption

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

In the above flowcharts and the algorithms, r denotes the number of rounds in the iteration process. Here, we have the function Mix() in the encryption process. The basic ideas underlying in this function can be explained as follows.

Consider the plaintext \( P = [ p_{ij} ] \), \( i = 1 \) to \( n \), \( j = 1 \) to \( n \), in any round of the iteration process. On writing each element of this matrix in its binary form, we get a matrix of size \( n \times 8n \). Let us now divide this matrix into 2 halves, wherein the first half is containing right from \( (1)^{st} \) column to \( (4n)^{th} \) column, and second matrix is containing \( (4n+1)^{th} \) column to \( (8n)^{th} \) column. We place the elements of \( (4n+1)^{th} \) column after the \( 1^{st} \) column, the elements of the \( (4n+2)^{th} \) column after the \( 2^{nd} \) column, etc., till we exhaust all the columns. Then, we write the binary bits, in terms of decimal numbers, by taking the binary bits in a column-wise manner. Thus we get a new matrix of size \( n \times n \). This is the process in function Mix().

Imix() denotes the reverse process of Mix().

In the process of decryption, we have the functions Inv(), for obtaining the modular arithmetic inverse of a matrix, and the function Mult() for finding the decryption key bunch matrix \( D = [ d_{ij} ] \). For obtaining the modular arithmetic inverse of a matrix, say A, we employ the equations
A Block Cipher Involving A Key Matrix...

\[ AA^{-1} = I \]  
and  
\[ A^{-1} = \left[ \frac{A_{ji}}{\Delta} \right], \]  
(2.11)  
(2.12)

where \( A^{-1} \) is the arithmetic inverse of \( A \), and \( A_{ji} \) is the transpose of \( A_{ij} \), in which \( A_{ij} \) is the cofactor of element \( a_{ij} \) of the matrix \( A \).

From (2.11) and (2.12), we get

\[ I \times \left[ \frac{A_{ji}}{\Delta} \right] \mod N = I \]  
(2.13)

where \( N \) is a positive integer. On multiplying both the sides by a scalar quantity \( d \), we get

\[ \left( A \times \left[ dA_{ji} \right] \right) \mod N = \left( I \times \Delta \times d \right) \mod N \]  
(2.14)

If we obtain \( d \) such that \( \left( \Delta \times d \right) \mod N = 1 \), then (2.14) can be written in the form

\[ \left( A \times \left[ dA_{ji} \right] \right) \mod N = I \]  
(2.15)

This shows that the modular arithmetic inverse of \( A \), which may be denoted by \( B \), can be written in the form

\[ B = \left[ dA_{ji} \right] \mod N. \]  
(2.16)

In function Mult(), we make use of the relation (2.10) and obtain the decryption key bunch matrix \( D \).

### III. ILLUSTRATION OF THE CIPHER AND THE AVALANCHE EFFECT

Consider the plaintext given below.

Dear Brother! I have seen your letter. Do never join in this profession as death is very close to every soldier at every instance in this service. Go for higher education. Do think of discovering some interesting scientific facts or try to invent something with all your ability. I know you are very intelligent and you can make your mark in your future career and get name and fame to our country. Do remember serving mother and father in their old-age is much more important and valuable than serving this country, which is very vast having several castes, having several religions, having several languages, having several political parties and not having any unity among people. Do forget that job. Be happy in your life.  

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

**Dear Brother!**  

On using EBCDIC code, (3.2) can be written in the form of a matrix \( P \), given by

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

Let us take the key matrix \( K \) and the encryption key bunch matrix \( E \) in the form

\[ K = \begin{bmatrix} 210 & 71 & 87 & 152 \\ 255 & 161 & 164 & 181 \\ 218 & 64 & 59 & 177 \\ 228 & 255 & 204 & 148 \end{bmatrix} \]  
(3.4)

and

\[ E = \begin{bmatrix} 21 & 221 & 13 & 197 \\ 45 & 67 & 143 & 149 \\ 87 & 205 & 197 & 1 \\ 253 & 255 & 9 & 67 \end{bmatrix} \]  
(3.5)

On using \( E \) and the concept of the multiplicative inverse, we get the decryption key bunch matrix \( D \). Thus we have

\[ D = \begin{bmatrix} 61 & 117 & 197 & 13 \\ 165 & 107 & 111 & 189 \\ 103 & 5 & 13 & 1 \\ 85 & 255 & 57 & 107 \end{bmatrix} \]  
(3.6)
On making use of the plaintext P, the key matrix K, the encryption key bunch matrix E, and the algorithm for the encryption process, given in section 2, we get the cipher text C in the form

\[
C = \begin{bmatrix}
60 & 12 & 110 & 22 \\
153 & 113 & 179 & 69 \\
250 & 114 & 230 & 81 \\
171 & 40 & 159 & 212 \\
\end{bmatrix}.
\] (3.7)

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

Let us now study the avalanche effect. On replacing the 2nd row 2nd column element, 194 of the plaintext matrix P, by 226, we get a new plaintext matrix. On using this modified plaintext matrix, the K and the E, and applying the encryption algorithm, given in section 2, we get the corresponding ciphertext C in the form

\[
C = \begin{bmatrix}
181 & 60 & 132 & 11 \\
65 & 130 & 52 & 145 \\
80 & 82 & 49 & 138 \\
118 & 183 & 115 & 12 \\
\end{bmatrix}.
\] (3.8)

On comparing (3.7) and (3.8), after converting them into their binary form, we notice that these two ciphertexts differ by 70 bits out of 128 bits.

Let us now consider a one binary bit change in the key bunch matrix E. To this end, we replace the 1st row 4th column element, 197 by 196. On using this modified E, the original plaintext P, the key K and employing the encryption algorithm, we obtain the corresponding ciphertext in the form

\[
C = \begin{bmatrix}
115 & 240 & 218 & 86 \\
35 & 229 & 228 & 210 \\
53 & 46 & 218 & 112 \\
55 & 67 & 128 & 35 \\
\end{bmatrix}.
\] (3.9)

After converting (3.9) into its binary form, and comparing the resulting matrix with the binary form of (3.7), we find that these two differ by 71 bits out of 128 bits.

From the afore-mentioned results, we conclude that the avalanche effect is quite up to the mark and the strength of the cipher is expected to be very good.

IV. CRYPTANALYSIS

In the literature of cryptography, the strength of a cipher is a very important issue and this is decided by considering all possible attacks. The attacks that are considered are

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

Generally analytical proofs are offered for the first two attacks, and intuitive inspections are made for the latter two attacks. No cipher will be accepted unless it withstands the first two attacks. In this cipher, the key matrix and the key bunch matrix are square matrices of size n. Here it is to be noted that the key bunch matrix contain odd numbers which are lying in [1-255]. In the light of these factors, the size of the key space is

\[
2^{5n^2} \times 2^{7n^2} = 2^{15n^2} \approx \left(10^3\right)^{\frac{5n^2}{3}} = 10^{4.5n^2}.
\] (4.1)

If the time required for the execution of this cipher with one key matrix and one key bunch matrix is \(10^{-7}\) seconds, then the time for the computation of this cipher with all possible keys in the key space is

\[
\frac{10^{4.5n^2} \times 10^{-7}}{365 \times 24 \times 60 \times 60} = 3.12 \times 10^{4.5n^2 - 15} \text{ years}.
\] (4.2)

Here, in this analysis, as we have taken \(n=4\), the time required for the whole computation is \(3.12 \times 10^{57}\) years. As this number is very large, we conclude that we cannot break this cipher, by the brute force attack. Let us now consider the known plaintext attack. In order to carry out this attack, we are provided with any number of plaintext and ciphertext pairs that we may require, in this process. If we confine our attention to only one round of the iteration process, that is taking \(r=1\), the basic equations governing the cipher are

\[
P = (KP) \mod 256,
\] (4.3)

\[
P = \left[e_{ij} \times p_{ij}\right] \mod 256, \text{ } i=1 \text{ to } n, \text{ } j = 1 \text{ to } n,
\] (4.4)
P= Mix(P),

(4.5)

and

C = P.

(4.6)

Here, as C is known to us, we can determine P, occurring on the left hand side of (4.5). On using Imix(), we get the P on the right hand side of (4.5), and hence the P occurring on the left hand side of (4.4).

Though the initial plaintext P occurring in the right hand side of (4.3) is known to us, we cannot proceed anymore and break the cipher in any way. As this is the case with r=1, we cannot break this cipher by the known plaintext attack, as we have taken r=16, in this analysis.

On inspecting the basic equations of this cipher, with all possible intuitions, we find that it is simply impossible to break the cipher either by choosing a plaintext or a ciphertext, in a selective manner.

In the light of the afore-mentioned discussions, we conclude that this cipher is unbreakable by all possible attacks, and is having enormous strength.

V. COMPUTATIONS AND CONCLUSIONS

In this investigation, we have developed a block cipher which includes a key matrix and a key bunch matrix. This cipher is supported by a function, called Mix(), wherein the binary bits are thoroughly mixed in each round of the iteration process.

The programs for the algorithms for the encryption and the decryption are written in Java.

The entire plaintext, given by (3.1), is consisting of 725 characters. Hence this is divided into 46 blocks, wherein each block is containing 16 characters. In the last block, we have included eleven 0s as additional characters, to make it a complete block. On using the K, the E, and the plaintext in each block, one after another, and employing the encryption algorithm, we have obtained the ciphertext corresponding to each block. Thus we have got the ciphertext corresponding to the entire plaintext. This is given by (5.1). In this analysis, we have noticed very clearly, that the cipher is strengthened very much, on account of the multiplication with a key, firstly, and with the multiplication with the key bunch matrix, subsequently. It may be noted here that this cipher can be extended with a key matrix of large size, and a key bunch matrix of the corresponding size, and then this analysis can be utilized in image processing of gray level images and color images.

REFERENCES

[16] Dr. V.U.K. Sastry, K.Shirisha, “A Block Cipher Involving a Key Bunch Matrix and an Additional Key Matrix, Supplemented with Modular Arithmetic Addition and supported by Key-based Substitution”, accepted in International Journal of Advanced Computer Science and Application(IJACSA), Nov 2012.
A Block Cipher Involving A Key Matrix...