ISSN No. 0976-5697
Volume 1, No. 4, Nov-Dec 2010
International Journal of Advanced Research in Computer Science
RESEARCH PAPER
Available Online at www.ijarcs.info

Advanced Hill Cipher Handling the Entire Plaintext as a Single Block

V.U.K.Sastry*
Department of computer Science and Engineering,SNIST
Hyderabad, India,
vuksastry@rediffmail.com

Aruna Varanasi
[2]Department of computer Science and Engineering,SNIST
Hyderabad, India,
varanasi.aruna2002@gmail.com

S.Udaya Kumar
[3]Department of computer Science and Engineering,SNIST
Hyderabad, India,
uksusarla@rediffmail.com

Abstract: In this paper we have devoted our attention to the study of large block cipher by employing the basic concepts of the advanced Hill cipher. In this the computation of the inverse of a matrix is very simple as we have confined our attention to an involutory matrix, i.e., a matrix whose inverse is the same as the original matrix. The avalanche effect and the cryptanalysis carried out in this investigation, to check the strength of the cipher, prominently indicate that the cipher is a potential one, and it can be applied to a plaintext of any length

Keywords: key, involutory matrix, cryptanalysis, avalanche effect, Ciphertext, block cipher

I. INTRODUCTION

The study of the advanced Hill cipher [1] and its application in image cryptography [2] has attracted the attention of researchers in the recent years. In a recent investigation, we [3] have developed a block cipher wherein the advanced Hill cipher is modified by introducing iteration and a permutation. In this we have taken the plaintext as a column vector containing n components and the key as a square matrix of size n/2xn/2. The development of the involutary matrix (a matrix is equal to its inverse) has enabled us to develop the cipher in a convenient manner. From the view point of the avalanche effect and the cryptanalysis, we have seen that this cipher is a very strong one. In this analysis it has been found that the permutation involved in the iteration process played a vital role in strengthening the cipher.

In the present paper our objective is to develop a block cipher which includes all the plaintext under consideration as a single block. This is, in a way, an extension of the preceding analysis presented in [3]. In this analysis also we use iteration process and permutation (in each round of the iteration process) in the development of the cipher.

In this investigation we have made use of the involutary matrix A, given by the relations

$$A = \begin{bmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{bmatrix} \qquad (1.1)$$

where

$A_{11}=K$ (1.2)

$A_{22} \bmod N = - A_{11} \bmod N,$ (1.3)

$A_{12}=[d(I- A_{11})] \bmod N,$ (1.4)

$A_{21}=[\lambda(I+ A_{11})] \bmod N,$ (1.5)

in which K is the key matrix, N a positive integer taken appropriately, 'd' a chosen positive integer lying between 0 and N, and λ is a positive integer obtained from the relation

$(d\lambda) \bmod N =1.$ (1.6)

For a detailed discussion of the involutory matrix, governed by the above relations (1.2)-(1.6), and the permutation used in the development of the cipher, one may refer to the earlier paper [3].

In section 2 we have discussed the development of the cipher. Section 3 deals with the illustration of the cipher and presents the avalanche effect. Section 4 is devoted to the

Cryptanalysis of the cipher. Finally, section 5 contains the conclusions.

II. DEVELOPMENT OF THE CIPHER

Let us consider the entire plaintext P and represent it in the form

$P= [P_{ij}]$, i=1 to n, j=1 to m.

Here n and m are chosen appropriately depending upon the size of the plaintext.

Let K be the key matrix given by

K=[Kij], i = 1 to n/2, j = 1 to n/2.

Let C be the ciphertext given by

C= [Cij], i=1 to n, j = 1 to m.

In the Advanced Hill cipher [3], the basic relations governing the encryption are

P= (A P) mod 256,

and

P=Permute(P).

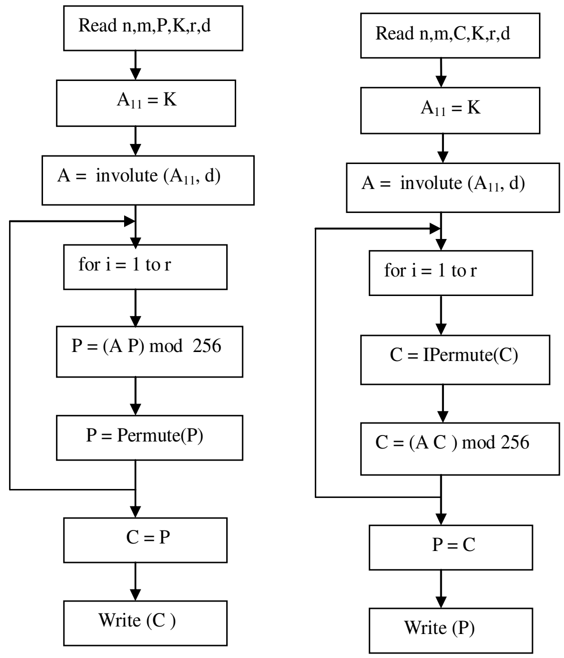
The corresponding steps in decryption are

C = IPermute(C),

and

C = (A C) mod 256.

In what follows, we present the flow charts and the algorithms depicting the procedures for encryption and decryption.



(a) Process of Encryption (b) Process of Decryption

Figure 1. Schematic diagram of the Cipher

Algorithm for Encryption

1. Read n,m,P,K,r,d
2. A_{11}= K
3. A= involute(A_{11},d)
4. for i = 1 to r
   {
   P = (A P) mod 256
   P= Permute(P)
   }
   C = P
5. Write(C)

Algorithm for Decryption

1. Read n,m,C,K,r,d
2. A_{11}= K
3. A= involute(A_{11},d)
4. for i= 1 to r
   {
   C = IPermute(C)
   C = (A C) mod 256
   }
5. P = C
6. Write (P)

involute(A_{11}, d)

{
1. A_{22} = - A_{11} mod 256
2. for i = 1 to 255
{
   if(id mod 256=1)
   {
   λ =i;
   break;
   }
}
3. A_{12}=[d(I- A_{11})] mod 256
4. A_{21}=[λ(I+ A_{11})] mod 256
5. Obtain A by using relation

$$A = \begin{bmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{bmatrix}$$

}

The function involute() yields the involutory matrix A, which is required for encryption and decryption.

Now let us see how the permutation can be carried out with the help of the Permute() function in the encryption algorithm. Let M be an nxm matrix obtained as a result of (AP) mod N. Let it be given by

$$\begin{bmatrix} M_{11} & M_{12} & \cdots & M_{1m} \\ M_{21} & M_{22} & \cdot & M_{2m} \\ \cdot & & \cdot & \cdot \\ \cdot & & \cdot & \cdot \\ \cdot & & \cdot & \cdot \\ M_{n1} & M_{n2} & \cdots & M_{nm} \end{bmatrix}$$

On converting each element of M into its binary form we get

$$\begin{bmatrix} M_{111} & M_{112} & \cdots & M_{118} & M_{121} & M_{122} & \cdots & M_{128} & \cdots & M_{1m1} & M_{1m2} & \cdots & M_{1m8} \\ M_{211} & M_{212} & \cdots & M_{218} & M_{221} & M_{222} & \cdots & M_{228} & \cdots & M_{2m1} & M_{2m2} & \cdots & M_{2m8} \\ \cdot & & & & & & & & & & & & \cdot \\ \cdot & & & & & & & & & & & & \cdot \\ \cdot & & & & & & & & & & & & \cdot \\ M_{n11} & M_{n12} & \cdots & M_{n18} & M_{n21} & M_{n22} & \cdots & M_{n28} & \cdots & M_{nm1} & M_{nm2} & \cdots & M_{nm8} \end{bmatrix}$$

This matrix is of size nx8m.

As it was mentioned in [3], the above matrix is divided into two halves, wherein the upper half is containing the rows 1 to n/2, and the lower half is containing the remaining rows, that is, (n/2+1) to n. Starting with the last element of the upper half, that is, with $M_{n/2m8}$,and going in the backward direction, along that particular row, and similarly along the other rows one after the other, until we reach $M_{111,}$ we place all the elements obtained in the above fashion in a new matrix in a column wise manner, one below the other, starting with the first row first column element.

Thus we get n rows and 4m columns. Then starting with the first element of the lower half, that is, with $M_{(n/2+1)11,}$ we go in a row wise manner till we reach the last element $M_{nm8.}$ On placing these elements, in the afore mentioned manner, we get the remaining 4m columns of the new matrix . Thus we have the permuted matrix of size nx8m. Now on converting each eight binary bits (taking along the row) of the permuted matrix into their decimal equivalent, we get a matrix of size nxm. The size of this matrix is the same as that of the original matrix.

Here it is to be noted that the function IPermute(), used in the decryption, is the reverse process to Permute().

In carrying out the encryption and the decryption, we have taken the number of rounds as r =16.

III. ILLUSTRATION OF THE CIPHER

Consider the plaintext given below

All the police officers are our own friends. They got an opportunity to get into police service, while we have joined in the band of Maoists. We can do well if we go on providing necessary financial assistance to our friends. Let us survive amicably. (3.1)

Let us take the key matrix K in the form

$$K = \begin{bmatrix} 128 & 12 & 45 & 34 \\ 189 & 200 & 9 & 99 \\ 245 & 135 & 59 & 33 \\ 72 & 122 & 27 & 109 \end{bmatrix} \tag{3.2}$$

On using the procedure, mentioned in the introduction, for the construction of the involutory matrix A, we get

$$A = \begin{bmatrix} 128 & 12 & 45 & 34 & 51 & 156 & 137 & 58 \\ 189 & 200 & 9 & 99 & 217 & 219 & 181 & 199 \\ 245 & 135 & 59 & 33 & 177 & 155 & 114 & 237 \\ 72 & 122 & 27 & 109 & 168 & 178 & 31 & 124 \\ 251 & 196 & 159 & 86 & 128 & 244 & 211 & 222 \\ 207 & 147 & 83 & 145 & 67 & 56 & 247 & 157 \\ 183 & 221 & 212 & 219 & 11 & 121 & 197 & 223 \\ 152 & 158 & 249 & 218 & 184 & 134 & 229 & 147 \end{bmatrix} \tag{3.3}$$

whose size is 8x8.

Now on using the EBCDIC code we can write the entire plaintext (3.1) in the form of a matrix given by

$$P = \begin{bmatrix} 193 & 151 & 134 & 129 & 150 & 149 & 168 & 64 & 149 & 135 & 64 & 162 & 64 & 133 & 150 & 64 & 132 & 137 & 64 & 166 & 166 & 64 & 149 & 162 & 129 & 162 & 133 & 64 & 75 & 64 & 64 & 168 \\ 147 & 150 & 134 & 153 & 166 & 132 & 64 & 150 & 137 & 133 & 151 & 133 & 166 & 64 & 137 & 163 & 64 & 162 & 131 & 133 & 133 & 151 & 135 & 129 & 149 & 162 & 64 & 134 & 64 & 162 & 129 & 75 \\ 147 & 147 & 137 & 133 & 149 & 162 & 135 & 151 & 163 & 163 & 150 & 153 & 136 & 136 & 149 & 136 & 150 & 163 & 129 & 147 & 64 & 153 & 64 & 153 & 131 & 137 & 163 & 153 & 211 & 164 & 148 & 64 \\ 64 & 137 & 131 & 64 & 64 & 75 & 150 & 151 & 168 & 64 & 147 & 165 & 137 & 129 & 133 & 133 & 134 & 162 & 149 & 147 & 135 & 150 & 149 & 168 & 137 & 162 & 150 & 137 & 133 & 153 & 137 & 64 \\ 163 & 131 & 133 & 150 & 134 & 64 & 163 & 150 & 64 & 137 & 137 & 137 & 147 & 165 & 132 & 64 & 64 & 75 & 64 & 64 & 150 & 165 & 133 & 64 & 129 & 163 & 64 & 133 & 163 & 165 & 131 & 64 \\ 136 & 133 & 153 & 164 & 153 & 227 & 64 & 153 & 163 & 149 & 131 & 131 & 133 & 133 & 64 & 130 & 212 & 64 & 132 & 137 & 64 & 137 & 131 & 134 & 147 & 129 & 150 & 149 & 64 & 137 & 129 & 64 \\ 133 & 64 & 162 & 153 & 137 & 136 & 129 & 163 & 150 & 163 & 133 & 133 & 64 & 64 & 137 & 129 & 129 & 230 & 150 & 134 & 150 & 132 & 133 & 137 & 64 & 149 & 164 & 132 & 164 & 165 & 130 & 64 \\ 64 & 150 & 64 & 64 & 133 & 133 & 149 & 164 & 64 & 150 & 64 & 107 & 166 & 145 & 149 & 149 & 150 & 133 & 64 & 64 & 149 & 137 & 162 & 149 & 129 & 131 & 153 & 162 & 162 & 133 & 147 & 64 \end{bmatrix} \tag{3.4}$$

This contains eight rows and thirty two columns. The plaintext is written in the matrix P in a column wise manner.

On applying the procedure for encryption, mentioned in section 2, we get the Ciphertext C in the form

$$C = \begin{bmatrix} 204 & 92 & 195 & 104 & 206 & 240 & 192 & 76 & 252 & 129 & 87 & 243 & 50 & 240 & 228 & 174 & 209 & 155 & 251 & 33 & 126 & 116 & 27 & 193 & 165 & 126 & 8 & 143 & 114 & 159 & 158 & 182 \\ 101 & 176 & 229 & 15 & 231 & 211 & 80 & 126 & 199 & 19 & 77 & 171 & 215 & 38 & 76 & 106 & 132 & 154 & 186 & 54 & 143 & 170 & 215 & 247 & 18 & 185 & 216 & 107 & 183 & 69 & 250 & 251 \\ 56 & 72 & 173 & 69 & 86 & 196 & 161 & 241 & 52 & 25 & 183 & 61 & 63 & 27 & 196 & 59 & 199 & 226 & 114 & 242 & 214 & 19 & 240 & 238 & 153 & 182 & 223 & 134 & 50 & 201 & 12 & 95 \\ 87 & 90 & 221 & 64 & 8 & 254 & 13 & 214 & 117 & 102 & 113 & 113 & 115 & 154 & 157 & 81 & 160 & 2 & 64 & 185 & 83 & 210 & 70 & 67 & 194 & 242 & 151 & 130 & 131 & 26 & 250 & 34 \\ 191 & 14 & 12 & 201 & 170 & 73 & 140 & 216 & 132 & 23 & 164 & 78 & 143 & 59 & 1 & 104 & 116 & 14 & 240 & 164 & 147 & 35 & 240 & 154 & 242 & 210 & 130 & 105 & 244 & 3 & 31 & 151 \\ 64 & 37 & 188 & 203 & 187 & 85 & 27 & 88 & 160 & 215 & 169 & 120 & 167 & 194 & 176 & 221 & 208 & 126 & 44 & 134 & 54 & 1 & 101 & 87 & 98 & 141 & 240 & 146 & 203 & 58 & 202 & 251 \\ 141 & 142 & 163 & 6 & 169 & 129 & 183 & 117 & 103 & 139 & 131 & 181 & 128 & 227 & 173 & 36 & 195 & 12 & 14 & 184 & 19 & 15 & 248 & 54 & 27 & 158 & 247 & 46 & 166 & 56 & 221 & 105 \\ 212 & 213 & 113 & 210 & 142 & 74 & 240 & 15 & 249 & 210 & 27 & 44 & 110 & 214 & 218 & 167 & 253 & 178 & 94 & 207 & 5 & 221 & 138 & 216 & 124 & 112 & 135 & 83 & 162 & 140 & 226 & 42 \end{bmatrix} \tag{3.5}$$

where C is of size 8x32.

On using the ciphertext given by (3.5), and the involutory matrix A given by (3.3) we apply the decryption algorithm and obtain the plaintext. This is found to be the same as the original one given by (3.4).

Now let us study the avalanche effect. To this end we have changed the two hundred and thirty second character 's' in the plaintext, given by (3.1), to 't'. Thus we have brought in a change of one binary bit as the EBCDIC codes of 's' and 't' are 162 and 163 respectively. On using the new plaintext and the encryption algorithm, we get the corresponding ciphertext C in the form

$$C=\begin{bmatrix}
135 & 101 & 203 & 13 & 133 & 97 & 250 & 58 & 64 & 7 & 188 & 209 & 192 & 75 & 0 & 231 & 240 & 48 & 83 & 70 & 17 & 235 & 77 & 44 & 168 & 155 & 245 & 132 & 229 & 247 & 212 & 204 \\
248 & 137 & 0 & 230 & 12 & 142 & 8 & 127 & 233 & 23 & 46 & 31 & 66 & 89 & 206 & 38 & 156 & 180 & 139 & 77 & 22 & 230 & 96 & 198 & 20 & 25 & 12 & 34 & 152 & 223 & 98 & 27 \\
135 & 198 & 60 & 43 & 251 & 235 & 16 & 206 & 158 & 71 & 52 & 143 & 34 & 76 & 245 & 38 & 242 & 100 & 112 & 244 & 167 & 88 & 109 & 1 & 122 & 164 & 81 & 255 & 101 & 108 & 102 & 182 \\
11 & 48 & 219 & 186 & 184 & 160 & 90 & 107 & 182 & 193 & 93 & 50 & 79 & 64 & 124 & 171 & 177 & 16 & 24 & 252 & 173 & 35 & 167 & 171 & 207 & 31 & 122 & 39 & 112 & 2 & 19 & 57 \\
39 & 48 & 203 & 245 & 77 & 212 & 241 & 176 & 105 & 125 & 189 & 59 & 188 & 71 & 190 & 97 & 224 & 178 & 128 & 251 & 25 & 135 & 8 & 34 & 39 & 162 & 0 & 71 & 131 & 88 & 249 & 10 \\
83 & 215 & 174 & 165 & 41 & 78 & 233 & 181 & 2 & 19 & 245 & 109 & 181 & 118 & 4 & 217 & 143 & 251 & 155 & 32 & 140 & 142 & 41 & 162 & 130 & 112 & 54 & 204 & 39 & 136 & 12 & 240 \\
136 & 84 & 95 & 219 & 31 & 47 & 150 & 115 & 212 & 122 & 67 & 233 & 242 & 252 & 124 & 87 & 121 & 76 & 67 & 245 & 193 & 22 & 122 & 164 & 79 & 0 & 33 & 34 & 160 & 119 & 106 & 64 \\
128 & 176 & 184 & 168 & 49 & 86 & 250 & 232 & 39 & 122 & 17 & 172 & 30 & 232 & 228 & 224 & 32 & 224 & 27 & 67 & 219 & 60 & 92 & 143 & 211 & 85 & 221 & 92 & 160 & 49 & 162 & 153
\end{bmatrix} \quad (3.6)$$

On comparing the ciphertexts (3.5) and (3.6), after converting them in to their binary form, we notice that the two ciphertexts differ by 1045 bits (out of 2048 bits). This is an excellent result, which shows that the cipher is a strong one.

Further, let us now change the key by replacing K_{31} from 245 to 244. Correspondingly the involutory matrix assumes the form

$$A=\begin{bmatrix}
128 & 12 & 45 & 34 & 51 & 156 & 137 & 58 \\
189 & 200 & 9 & 99 & 217 & 219 & 181 & 199 \\
244 & 135 & 59 & 33 & 100 & 155 & 114 & 237 \\
72 & 122 & 27 & 109 & 168 & 178 & 31 & 124 \\
251 & 196 & 159 & 86 & 128 & 244 & 211 & 222 \\
207 & 147 & 83 & 145 & 67 & 56 & 247 & 157 \\
60 & 221 & 212 & 219 & 12 & 121 & 197 & 223 \\
152 & 158 & 249 & 218 & 184 & 134 & 229 & 147
\end{bmatrix} \qquad (3.7)$$

On carrying out the encryption process with the original plaintext (3.4) and the modified involutory matrix given by (3.7), we get the ciphertext C in the form

$$C=\begin{bmatrix}
164 & 2 & 243 & 213 & 1 & 235 & 162 & 148 & 59 & 23 & 50 & 212 & 131 & 158 & 128 & 217 & 126 & 77 & 105 & 68 & 78 & 222 & 60 & 224 & 171 & 146 & 150 & 139 & 129 & 136 & 237 & 3 \\
118 & 173 & 242 & 110 & 206 & 141 & 196 & 100 & 168 & 231 & 12 & 61 & 69 & 219 & 134 & 189 & 190 & 250 & 241 & 141 & 243 & 145 & 166 & 19 & 100 & 208 & 134 & 163 & 235 & 145 & 125 & 138 \\
172 & 23 & 118 & 194 & 253 & 73 & 86 & 145 & 64 & 122 & 127 & 6 & 164 & 1 & 32 & 157 & 16 & 141 & 52 & 16 & 124 & 224 & 199 & 156 & 171 & 81 & 169 & 220 & 89 & 131 & 83 & 27 \\
222 & 1 & 106 & 93 & 87 & 54 & 192 & 139 & 141 & 172 & 22 & 93 & 125 & 98 & 138 & 246 & 106 & 234 & 124 & 127 & 97 & 248 & 55 & 175 & 226 & 22 & 205 & 254 & 206 & 159 & 80 & 249 \\
134 & 34 & 10 & 60 & 99 & 230 & 147 & 193 & 141 & 132 & 127 & 71 & 32 & 122 & 122 & 76 & 223 & 83 & 189 & 23 & 33 & 95 & 128 & 95 & 205 & 190 & 151 & 167 & 12 & 88 & 66 & 196 \\
63 & 219 & 111 & 86 & 156 & 74 & 1 & 58 & 65 & 122 & 151 & 242 & 159 & 205 & 159 & 109 & 28 & 122 & 29 & 119 & 129 & 18 & 172 & 38 & 24 & 107 & 93 & 207 & 9 & 229 & 239 & 86 \\
207 & 175 & 18 & 107 & 5 & 13 & 4 & 217 & 92 & 135 & 233 & 203 & 193 & 222 & 248 & 232 & 177 & 170 & 27 & 47 & 154 & 21 & 187 & 114 & 63 & 136 & 77 & 118 & 94 & 35 & 79 & 190 \\
89 & 42 & 80 & 32 & 71 & 116 & 204 & 237 & 167 & 113 & 228 & 2 & 197 & 156 & 115 & 107 & 4 & 151 & 135 & 95 & 77 & 127 & 167 & 167 & 57 & 145 & 93 & 139 & 176 & 105 & 68 & 9
\end{bmatrix} \quad (3.8)$$

On comparing (3.5) and (3.8), after converting them in to their binary form, we find that they differ by 1069 bits (out of 2048 bits). This difference also is quite significant, and shows very effectively that the cipher is undoubtedly a strong one.

IV. CRYPTANALYSIS

The well known different approaches in cryptanalysis are

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

Let us now consider the brute force attack. Here the key K is of size n/2xn/2, and hence the key space is of size 2^{2n^2}. As 'd' also can be treated as a key, the size of the key space gets modified to the form 2^{2n^2+8}. In the present analysis we have taken n=8. If the time required for the computation of this cipher with a single value of the key is 10^{-7}seconds, it can be shown that the time for the brute force attack is $8.11\text{x}10^{25.4}$ years. For the detailed account of this analysis one may refer to [3].

Let us now examine the possibility of known plaintext attack. To this end let us take the plaintext P in the form of a square matrix of size nxn, this is done by choosing m=n. Here we assume that the entire plaintext is of this special form. Let us assume that the corresponding ciphertext is known to us. Of course, in this attack we can assume that we have as many such pairs as we require. However, as the P multiplied with A is operated with mod N (= 256 in this example), and further, as the result is permuted in each round of the iteration process, the binary bits of K and P are scattered. Hence the inverse of P cannot be found out and the K (or) function of K cannot be determined, by any means. Thus, the cipher cannot be broken in this approach.

In the last two cases, as we do not visualize any special choice of the plaintext or the ciphertext which enables us to determine the key or a function of the key, we do not have any scope to break the cipher.

V. CONCLUSIONS

In this paper, taking the entire plaintext into consideration as a single block, we have developed a block cipher for a very large block. In this we have made use of the concept of the advanced Hill cipher. The programs for encryption and decryption are written in java language.

In this analysis we have seen that the permutation carried out in each round of the iteration process has strengthened the cipher significantly. It is interesting to note that the avalanche effect corresponding to one bit change, either in the plaintext or in the key, is conspicuous. The cryptanalysis clearly shows that the cipher cannot be broken by any conventional cryptanalytic attacks.

We conclude that this cipher can be applied very well for the security of any plaintext.

VI. REFERENCES

[1] Bibhudendra Acharya.Girija Sankar Rath, Sarat Kumar Patra, Saroj Kumar Panigrahy. 2007. Novel methods of Generating Self-Invertible Matrix for Hill Cipher Algorithm, Internation Journal of Security, Vol.1, Issue 1, 2007, pp.14-21.

[2] Bibhudendra Acharya. Saroj Kumar Panigrahy, Sarat Kumar Patra, and Ganapathi Panda, " Image Encryption Using Advanced Hill Cipher Algorithm", International Journal of Recent Trends in Engineering, Vol.1, No.1, May2009.

[3] V.U.K.Sastry, Aruna Varanasi, and S.Udaya Kumar, " Advanced Hill Cipher Involving Permutation and Iteration",sent to International Journal of Advanced Research in Computer science for publication.