A Modern Advanced Hill Cipher Involving XOR Operation and a Permitted Key

V.U.K. Sastry¹, Aruna Varanasi*² and S.Udaya Kumar³

¹Department of computer Science and Engineering, SNIST
Hyderabad, India, vuksastry@rediffmail.com
²Department of computer Science and Engineering, SNIST
Hyderabad, India, varanasi.aruna2002@gmail.com
³Department of computer Science and Engineering, SNIST
Hyderabad, India, uksusarla@rediffmail.com

Abstract: In this paper, we have developed a block cipher by extending the analysis of the advanced Hill cipher. In this, besides the usual involutory matrix, which contains the key, we have included another matrix, which is obtained by permuting the original involutory matrix. This analysis is strengthened by using the xor operation, modular arithmetic and a function called mix(), which mixes the binary bits of the plaintext and the involutory matrix, which includes the key. The avalanche effect and the cryptanalysis carried out in this investigation clearly indicate that the strength of the cipher is quite significant.

Keywords: symmetric block cipher, cryptanalysis, avalanche effect, ciphertext, key, permuted key, xor operation.

INTRODUCTION

In a recent investigation [1], we have developed a block cipher, called modern advanced Hill cipher, by modifying the advanced Hill cipher [2]. In this we have included a matrix A₀, which is obtained by permuting an involutory matrix A, which contains the key K. In this process, the basic relations governing the cipher are

\[ C = (AP + A₀) \mod N, \]  

and

\[ P = (A(C - A₀) \mod N, \]  

where P is a plaintext matrix, N a positive integer, chosen appropriately, and C is the corresponding ciphertext matrix. In this analysis, we have shown that the addition of A₀ plays a vital role in strengthening the cipher.

In the present paper our objective is to modify the modern advanced Hill cipher by replacing the addition operation with XOR operation. Our interest here is to show that the xor operation is quite comparable to the addition operation in strengthening the cipher.

The relations governing the block cipher under consideration are

\[ C = (AP \mod N \oplus A₀, \]  

and

\[ P = (A(C \oplus A₀)) \mod N. \]  

DEVELOPMENT OF THE CIPHER

In the development of the cipher, the plaintext P, the key K (basing upon which the involutory matrix A is found) and the ciphertext C are of the form

\[ P = [P_{ij}], \quad i=1 \text{ to } n, \quad j=1 \text{ to } n, \]  

\[ K = [K_{ij}], \quad i=1 \text{ to } n/2, \quad j=1 \text{ to } n/2, \]  

\[ C = [C_{ij}], \quad i=1 \text{ to } n, \quad j=1 \text{ to } n. \]  

Here \( n \) is an even positive integer and each element of P, K and C are decimal numbers, lying between 0 and 255, as we have made use of EBCDIC code.

On using the key K, the involutory matrix A can readily be obtained by applying the following relations:

\[ A = \begin{bmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{bmatrix}, \]  

\[ A_{11} = K, \]  

\[ A_{22} = -K, \]  

\[ A_{12} = [d(I-K)] \mod N, \]  

\[ A_{21} = [\lambda(I+K)] \mod N, \]  

\[(d\lambda) \mod N = 1, \]  

Let us now mention the plan of the paper. In section 2, we have introduced the development of the cipher and presented the algorithms for encryption and decryption. In section 3, we have illustrated the cipher and mentioned the avalanche effect. Section 4 is devoted to cryptanalysis. Finally in section 5, we have discussed the computations and drawn conclusions.
where N=256.

In order to have a detailed discussion for obtaining A, we refer to [3].

The A₀, which is obtained by permuting the terms in A can be written in the form

\[ A₀ = \begin{bmatrix} A_{22} & A_{21} \\ A_{12} & A_{11} \end{bmatrix} \] (2.10)

As we have already pointed out in section 1, the relations governing the encryption and the decryption are

\[ C = (AP) \mod N \]

\[ A₀ \] \[ P = (A(C \oplus A₀)) \mod N. \] (2.12)

The algorithms for encryption and decryption are given below.

**Algorithm for Encryption**

1. Read n,P,K,r,d
2. \( A₁₁ = K \)
3. \( A = \text{involute}(A₁₁,d) \)
4. \( A₀ = \text{permute}(A) \)
5. for i = 1 to r
   \[ \{ \]
   \[ P = (A \cdot P) \mod 256 \oplus A₀ \]
   \[ P = \text{mix}(P) \]
   \[ C = P \]
   \[ \} \]
6. Write( C )

**Algorithm for Decryption**

1. Read n,C,K,r,d
2. \( A₁₁ = K \)
3. \( A = \text{involute}(A₁₁,d) \)
4. \( A₀ = \text{permute}(A) \)
5. for i= 1 to r
   \[ \{ \]
   \[ C = \text{Imix}(C) \]
   \[ C = (A(C \oplus A₀)) \mod 256 \]
   \[ \} \]
6. Write (P)

**Algorithm for inverse(K)**

1. Read A, n, N
   // A is an n x n matrix.  N is a positive integer with which modular arithmetic is carried out.  Here N= 256.
2. Find the determinant of A.  Let it be denoted by \( \Delta \), where \( \Delta \neq 0 \).
3. Find the inverse of A.  The inverse is given by \( [A_i\_{ij}]/\Delta \), i= 1 to n , j = 1 to n
   // \( [A_i\_{ij}] \) are the cofactors of \( a_{ij} \), where \( a_{ij} \) are the elements of A
   for i = 1 to N
   \[ \{ \]
   \[ // \Delta \text{ is relatively prime to N} \]
   \[ \text{if} ((i\Delta) \mod N == 1) \text{ break; } \]
   \[ \} \]
   \[ d = i; \]
   \[ B = [dA_i\_{ij}] \mod N. // B \text{ is the modular arithmetic inverse of A.} \]

In this analysis, we have taken r=16.  The function mix() can be written in the form \( P = \text{mix}(P) \).  For a detailed discussion of the functions mix() (that is how the binary bits are mixed) and involute() (used for obtaining the involutory matrix, A), we refer to [2].  The function Imix(), used in decryption, denotes the reverse process of mix().

**ILLUSTRATION OF THE CIPHER**

Consider the plaintext given below:

“As we came across, unfortunately, all selfish and greedy people, we are residing in wilderness in the forests. But we are having several scientists and engineers among us. We must be able to light our own lamp so that we drive away the gloom in our life, and fight a battle with the society.” (3.1)

Let us focus our attention on the first sixty four characters of the plaintext given by (3.1). Thus we have

(3.2)

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

<table>
<thead>
<tr>
<th>193</th>
<th>162</th>
<th>64</th>
<th>166</th>
<th>133</th>
<th>64</th>
<th>131</th>
<th>129</th>
</tr>
</thead>
<tbody>
<tr>
<td>148</td>
<td>133</td>
<td>64</td>
<td>129</td>
<td>131</td>
<td>153</td>
<td>150</td>
<td>162</td>
</tr>
<tr>
<td>162</td>
<td>107</td>
<td>64</td>
<td>164</td>
<td>149</td>
<td>134</td>
<td>150</td>
<td>153</td>
</tr>
<tr>
<td>163</td>
<td>164</td>
<td>149</td>
<td>129</td>
<td>163</td>
<td>133</td>
<td>147</td>
<td>168</td>
</tr>
<tr>
<td>107</td>
<td>64</td>
<td>129</td>
<td>147</td>
<td>147</td>
<td>64</td>
<td>162</td>
<td>133</td>
</tr>
<tr>
<td>147</td>
<td>134</td>
<td>137</td>
<td>162</td>
<td>136</td>
<td>64</td>
<td>129</td>
<td>149</td>
</tr>
<tr>
<td>132</td>
<td>64</td>
<td>135</td>
<td>153</td>
<td>133</td>
<td>133</td>
<td>132</td>
<td>168</td>
</tr>
<tr>
<td>64</td>
<td>151</td>
<td>133</td>
<td>150</td>
<td>151</td>
<td>147</td>
<td>133</td>
<td>107</td>
</tr>
</tbody>
</table>

(3.3)

Let us choose the key K in the form

\[ K = \begin{bmatrix} 215 & 111 & 19 & 147 \\ 223 & 99 & 254 & 12 \\ 56 & 1 & 127 & 174 \\ 59 & 146 & 189 & 81 \end{bmatrix} \] (3.4)

Let us now construct the involutory matrix A by using the relations (2.4) to (2.9).  Here we take d= 99.  Thus we have
On using (2.10) and (3.5), we get

\[
A_0 = \begin{bmatrix}
150 & 239 & 213 & 252 & 227 & 178 & 205 & 47 \\
83 & 83 & 147 & 31 & 197 & 185 & 96 & 83 \\
39 & 255 & 79 & 1 & 187 & 143 & 244 \\
50 & 183 & 44 & 114 & 6 & 72 & 191 & 58 \\
100 & 120 & 118 & 203 & 198 & 213 & 120 & 11 \\
42 & 248 & 76 & 57 & 164 & 218 & 91 & 92 \\
157 & 73 & 228 & 60 & 176 & 182 & 231 & 43 \\
119 & 14 & 229 & 19 & 199 & 52 & 86 & 235
\end{bmatrix}
\]  

On using (3.3), (3.5), and (3.6), and the encryption algorithm, we get

\[
C = \begin{bmatrix}
71 & 245 & 119 & 211 & 223 & 154 & 227 & 50 \\
198 & 229 & 53 & 64 & 159 & 85 & 8 & 200 \\
226 & 137 & 17 & 175 & 240 & 181 & 40 & 96 \\
147 & 117 & 29 & 111 & 231 & 64 & 189 & 212 \\
139 & 112 & 81 & 62 & 214 & 226 & 102 & 128 \\
139 & 18 & 131 & 151 & 33 & 162 & 165 & 144 \\
67 & 9 & 166 & 158 & 228 & 174 & 210 & 192 \\
172 & 211 & 14 & 150 & 145 & 152 & 184 & 142
\end{bmatrix}
\]  

On comparing (3.7) and (3.8), in their binary form, we notice that the two ciphertexts differ by 260 bits (out of 512 bits). This indicates that the strength of the cipher is very good.

Let us now change the first row first column element of the key K, given by (3.3), from 215 to 214. This will lead to a change of one bit in their binary form. After obtaining the modified A and the A0 corresponding to the modified key, we apply the encryption algorithm (by taking the original plaintext), and obtain the corresponding ciphertext C. Thus we get

\[
A = \begin{bmatrix}
215 & 111 & 19 & 147 & 62 & 19 & 167 & 39 \\
223 & 99 & 254 & 12 & 195 & 26 & 198 & 92 \\
56 & 1 & 127 & 174 & 88 & 157 & 70 & 182 \\
59 & 146 & 189 & 81 & 47 & 138 & 233 & 16 \\
72 & 133 & 145 & 17 & 41 & 145 & 237 & 109 \\
85 & 76 & 106 & 132 & 33 & 157 & 2 & 244 \\
104 & 75 & 128 & 250 & 200 & 255 & 129 & 82 \\
73 & 198 & 95 & 6 & 197 & 110 & 67 & 175
\end{bmatrix}
\]

\[
A_0 = \begin{bmatrix}
82 & 31 & 150 & 136 & 158 & 252 & 27 & 182 \\
135 & 186 & 182 & 197 & 53 & 31 & 110 & 112 \\
92 & 66 & 111 & 124 & 242 & 247 & 182 & 110 & 189 \\
56 & 1 & 127 & 174 & 88 & 157 & 70 & 182 \\
147 & 117 & 29 & 111 & 231 & 64 & 189 & 212 \\
139 & 18 & 131 & 151 & 33 & 162 & 165 & 144 \\
67 & 9 & 166 & 158 & 228 & 174 & 210 & 192 \\
172 & 211 & 14 & 150 & 145 & 152 & 184 & 142
\end{bmatrix}
\]  

Now on comparing (3.7) and (3.9) in their binary form, we find that they differ by 269 bits (out of 512 bits). This also exhibits the strength of the cipher.

Though the avalanche effect is indicating the strength of the cipher, let us now consider the cryptanalysis which establishes very firmly the strength of the cipher.

**CRYPTANALYSIS**

The cryptanalytic attacks which are generally considered 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.

The key matrix K, given by (3.3), contains 16 decimal numbers. In this analysis, we have taken an integer d in the construction of the involutory matrix, A. As this also is to be treated as an additional key, the total length of the key can be considered as 17 decimal numbers, which is equal to 136 binary bits. Thus the size of the key space is

\[
2^{136} = (2^{10})^{13.6} = 10^{40.8} \cdot 10^{13.6}
\]

If we assume that the time required for computation with each one of the keys is 10^{-7} seconds, then the time required for carrying out the computation with all keys in the key space is

\[
10^{40.8} \times 10^{-7} = 3.171 \times 10^{25.8} \text{ years}
\]

As this is very large, we conclude that this cipher cannot be broken by the brute force attack.

Let us now examine the known plaintext attack. In this we know pairs of the plaintext and the ciphertext as many as we require. In the development of this cipher we have an iterative process and mix function. Denoting the mix function as M, for clarity and convenience, the relation between the ciphertext and the original plaintext, obtained at the end of the iteration process (for r=16), can be written in the form

\[
C=M((AM((……...M(A M(AP \mod 256 \oplus A_0)) \mod 256 \oplus A_0) \ldots\ldots) \mod 256 \oplus A_0) \mod 256 \oplus A_0)
\]  

(4.1)

On focusing our attention on the equation (4.1), we notice several interesting factors. After multiplying A and P we have carried out mod 256. Then the elements of A_0 are xored with the result of (AP) mod 256. After this, the resulting value is converted into binary bits and then the mix process is carried out. In the light of all these operations, the binary bits of the key (included in A) and the plaintext P are totally mixed and they have undergone diffusion. As this process continues in
each round, we do not have any scope for the determination of the key or a function of the key so that we can break the cipher. Thus the cipher cannot be broken by the known plaintext attack.

Generally every encryption algorithm is designed to withstand against the first two attacks. The latter two cryptanalytic attacks depend totally on intuition and imagination. Here we do not find any such scope for breaking the cipher.

COMPUTATIONS AND CONCLUSIONS

In this paper, we have developed a block cipher, called modern advanced Hill cipher, in which we have included a matrix $A_0$ (obtained by permuting the involuntary matrix $A$, which includes the key $K$) and the xor operation. In this cipher the computations are carried out by writing programs for encryption and decryption in Java.

The plaintext (3.1) is divided into five blocks by taking 64 characters at a time. Each block is written in the form of a square matrix of size 8. The last block is supplemented with twenty nine characters, so that it becomes a complete one. The ciphertext corresponding to the complete plaintext (3.1) is obtained in the form

\begin{verbatim}

text
\end{verbatim}

The avalanche effect and the cryptanalysis, considered in sections 3 and 4, clearly indicate that the cipher is a strong one and it cannot be broken by any cryptanalytic attack. This generalization of the advanced Hill cipher is markedly an interesting one.

REFERENCES


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 12 PhDs, and published more than 40 research papers in various international journals. His research interests are Network Security & Cryptography, Image Processing, Data Mining and Genetic Algorithms.

Aruna Varanasi is presently working as Associate Professor in the Department of Computer Science and Engineering (CSE), Sreenidhi Institute of Science and Technology (SNIST), Hyderabad, India. She was awarded “Suman Sharma” by Institute of Engineers (India), Calcutta for securing highest marks among women in India in AMIE course.