ISSN No. 0976-5697

Volume 2, No. 1, Jan-Feb 2011

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

A Modern Hill Cipher Involving XOR Operation and a Permuted Key

V. U. K. Sastry*, Aruna Varanasi and S. Udaya Kumar
Department of computer Science and Engineering,SNIST
Hyderabad, India,
vuksastry@rediffmail.com
varanasi.aruna2002@gmail.com
uksusarla@rediffmail.com

Abstract: In this paper, we have devoted our attention to the study of a symmetric block cipher by extending the analysis of the classical Hill cipher. In this development we have introduced iteration process. In each round of the iteration process we have included a function called mix() in order to achieve confusion and diffusion of the plaintext at every stage of the iteration. Here a key K_0, formed by permuting the original key K, is used in the formation of the cipher. This K_0 is linked with the other portion of the relation governing the cipher by introducing XOR operation. The avalanche effect and the cryptanalysis thoroughly indicate the strength of the cipher.

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

I. INTRODUCTION

In a recent investigation, sastry et al. have developed a modern block cipher[1] by including a permuted key and modular arithmetic addition into the Hill cipher[2]. In their analysis, the basic relations governing the cipher are

$$C = (KP + K_0) \bmod N, \qquad (1.1)$$

and

$$P = (K^{-1} (C - K_0)) \bmod N, \qquad (1.2)$$

where P is a plaintext matrix, C the corresponding ciphertext matrix, K the key matrix, N is any positive integer, K_0 another key matrix, obtained from K by permuting the elements of K in a chosen manner, and K^{-1} is the modular arithmetic inverse of K.

In this they have introduced iteration process and a function called mix(), for creating confusion and diffusion, and have shown that the draw back of the classical Hill cipher, namely the cipher can be broken by the known plaintext attack, can be overcome very easily on account of this modification.

In the present paper our objective is to develop a variant of the modern Hill cipher which is equally strong in all respects. Here the basic relations governing the cipher are given by

$$C = (KP) \bmod N \oplus K_0, \qquad (1.3)$$

and

$$P = (K^{-1}(C \oplus K_0)) \bmod N. \qquad (1.4)$$

Here also we use the iteration process, and the mix() function in each round of the iteration process.

In section 2, we deal with the development of the cipher and present a pair of algorithms for encryption and decryption. In section 3, we illustrate the cipher and discuss the avalanche effect. Section 4 is devoted to cryptanalysis. Finally in section 5 we mention the computations and draw conclusions.

II. DEVELOPMENT OF THE CIPHER

In the development of the cipher, the plaintext P, the key K and the ciphertext C are of the form

$$P = [P_{ij}], \quad i = 1 \text{ to } n, \; j = 1 \text{ to } n, \qquad (2.1)$$

$$K = [K_{ij}], \quad i = 1 \text{ to } n, \; j = 1 \text{ to } n, \qquad (2.2)$$

$$C = [C_{ij}], \quad i = 1 \text{ to } n, \; j = 1 \text{ to } n, \qquad (2.3)$$

where each element of P, K and C are decimal numbers lying between 0 and 255. This is all on account of the fact that we have used EBCDIC code.

The permuted key K_0 is taken in the form

$$K_0 = \begin{bmatrix} B_{11} & B_{12} \\ B_{21} & B_{22} \end{bmatrix}$$

where

$B_{11} = [K_{ij}]$, $i=(n/2+1)$ to n, $j=(n/2+1)$ to n,
$B_{12} = [K_{ij}]$, $i=(n/2+1)$ to n, $j=1$ to $n/2$,
$B_{21} = [K_{ij}]$, $i=1$ to $n/2$, $j=(n/2+1)$ to n,
$B_{22} = [K_{ij}]$, $i=1$ to $n/2$, $j=1$ to $n/2$.

The algorithms for encryption and decryption are written below.

Algorithm for Encryption

```
1. Read n,P,K,r
2. K0= permute(K)
3. for i = 1 to r
   {
   P = (K P)mod 256 ⊕ K0
   P= mix(P)
   }
   C = P
4. Write( C )
```

Algorithm for Decryption

```
1. Read n,C,K,r
2. K^-1 = Inverse(K)
   K0 = Permute(K)
3. for i= 1 to r
      {
```

C = Imix(C)
C= (K^{-1} (C $\oplus$ K_0))mod 256

}
P = C
4. 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 Δ, where Δ ≠ 0.
3. Find the inverse of A. The inverse is given by $[A_{ji}]/\Delta$, i= 1 to n , j = 1 to n
// $[A_{ij}]$ are the cofactors of a_{ij}, where a_{ij} are the elements of A
for i = 1 to N
{
// Δ is relatively prime to N
if((iΔ) mod N == 1) break;
}
d= i;
4. B = $[dA_{ji}]$ mod N. // B is the modular arithmetic inverse of A.

In this analysis r=16. For a detailed discussion of the functions mix() and Imix() we refer to [1].

III. ILLUSTRATION OF THE CIPHER

Consider the plaintext given below:

No doctor wants to see a poor patient except when there is a support of the Government. All doctors want to examine the rich patients as they can shell down lacs and lacs. God also does not want to see the face of the poor!
(3.1)

Let us take the first sixteen characters of the plaintext (3.1) into consideration. This is given by
No doctor wants . (3.2)

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

$$P = \begin{bmatrix} 213 & 150 & 64 & 132 \\ 150 & 131 & 163 & 150 \\ 153 & 64 & 166 & 129 \\ 149 & 163 & 162 & 64 \end{bmatrix} \qquad (3.3)$$

Let us choose the key, K in the form

$$K = \begin{bmatrix} 123 & 25 & 9 & 67 \\ 134 & 17 & 20 & 11 \\ 48 & 199 & 209 & 75 \\ 39 & 55 & 85 & 92 \end{bmatrix} \qquad (3.4)$$

On using the definition of K_0, mentioned in section 2, we get

$$K_0 = \begin{bmatrix} 209 & 75 & 48 & 199 \\ 85 & 92 & 39 & 55 \\ 9 & 67 & 123 & 25 \\ 20 & 11 & 134 & 17 \end{bmatrix} \qquad (3.5)$$

On using (3.3) to (3.5) and the encryption algorithm, we obtain

$$C = \begin{bmatrix} 162 & 124 & 30 & 73 \\ 122 & 169 & 43 & 214 \\ 230 & 97 & 207 & 241 \\ 157 & 230 & 200 & 49 \end{bmatrix} \qquad (3.6)$$

On adopting the decryption algorithm, with the required inputs, we get back the original plaintext given by (3.3).

Let us now examine the avalanche effect, which shows the strength of the cipher.

In order to carry out this one, we replace the fifteenth character‘s’ by ‘t’ in the plaintext (3.2). The EBCDIC codes of ‘s’ and ‘t’ are 162 and 163. These two differ by one bit in their binary form. Thus, on using the modified plaintext we get the ciphertext C in the form

$$C = \begin{bmatrix} 37 & 8 & 43 & 176 \\ 228 & 151 & 80 & 34 \\ 100 & 210 & 68 & 171 \\ 158 & 226 & 41 & 66 \end{bmatrix} \qquad (3.7)$$

On converting (3.6) and (3.7) into their binary form, we notice that the two ciphertexts differ by 66 bits (out of 128 bits). This shows that the cipher is a strong one.

Let us now consider a one bit change in the key K. This can be achieved by replacing the second row fourth column element of (3.4) “11” by “10”. On executing the encryption algorithm with the modified key, the corresponding permuted key $K_{0,}$ and the original plaintext intact, we get

$$\overline{C} = \begin{bmatrix} 65 & 31 & 188 & 242 \\ 137 & 236 & 214 & 115 \\ 255 & 157 & 147 & 100 \\ 31 & 253 & 128 & 211 \end{bmatrix} \qquad (3.8)$$

Now on comparing the binary forms of (3.6) and (3.8), we find that they differ by 67 bits (out of 128 bits). This also shows that the cipher is a potential one.

IV. 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

As the key matrix K contains 16 decimal numbers, wherein each number can be represented in terms of eight binary bits, the length of the key is 128 bits. As it is established very clearly in [1] the ciphertext only attack is ruled out.

Let us now consider the known plaintext attack, wherein the pairs of the plaintext and the ciphertext (as many as we require) are known. If we focus our attention on different stages of the iteration process, the relations between C and P are given by

$$C = M((KP) \bmod 256 \oplus K_0) \quad \text{for } r=1, \tag{4.1}$$

$$C = M((K\, M((KP) \bmod 256 \oplus K_0)) \bmod 256 \oplus K_0) \quad \text{for } r=2, \tag{4.2}$$

.

.

.

$$C=M((KM((\ldots\ldots M((K\, M((KP) \bmod 256 \oplus K_0)) \bmod 256 \oplus K_0) \ldots\ldots) \bmod 256 \oplus K_0)) \bmod 256 \oplus K_0) \quad \text{for } r=16. \tag{4.3}$$

In writing the above relations the function mix() is replaced by M() for elegance.

The relation (4.1), corresponding to r=1, can be written in the form

$$\text{Imix}(C) = (KP)\text{mod}256 \oplus K_0 . \tag{4.4}$$

When r=1 i.e., when we have only one round of the iteration, from (4.4) we notice that this cipher cannot be broken on account of the presence of K_0. This is the significant departure between the classical Hill cipher and the present cipher. When r=16, the relation between C and P given by (4.3) is a complicated one, and the key K, the plaintext P and the K_0, after undergoing several operations, and thoroughly mixed. In view of this fact, the key K or a function of K cannot be determined by any means, and hence the cipher remains unbreakable in the case of the known plaintext attack.

Apparently, no scope is found for breaking the cipher in the last two cases of the cryptanalytic attack.

From the above discussion, we conclude that the cipher is a strong one.

V. COMPUTATIONS AND CONCLUSIONS

In this paper, we have developed a modern Hill cipher, which includes a permuted Key K_0 (dependent on K) and 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 fourteen blocks by taking sixteen characters at a time. The last block is supplemented with one blank character, so that it becomes a full one. The ciphertext corresponding to the complete plaintext (3.1) is obtained in the form presented below.

162	124	30	73	122	169	43	214	230	97	207	241	157	230	200	49
214	12	90	252	112	233	244	56	188	33	207	110	170	18	117	175
69	211	118	79	20	212	233	4	59	31	44	25	201	116	179	193
167	111	158	217	133	192	152	14	159	67	130	248	71	213	98	211
30	135	182	12	196	126	87	213	56	38	84	163	52	124	166	130
45	103	191	43	200	41	126	29	174	62	88	88	50	21	168	42
178	217	181	71	21	222	244	83	18	191	103	0	253	22	92	185
231	182	137	18	45	88	115	28	147	90	246	160	52	187	191	220
227	139	177	237	138	82	104	205	90	149	174	33	195	26	6	87
155	248	182	31	101	233	2	66	213	249	236	212	47	157	152	240
179	15	28	252	40	8	18	164	214	172	22	37	247	58	193	182
2	56	224	160	81	220	204	139	176	229	148	244	17	2	70	148
138	217	79	249	253	64	191	246	141	112	140	170	75	41	128	154
254	73	189	13	159	108	216	12	210	180	70	63	71	89	89	143

The avalanche effect and cryptanalysis considered in sections 3 and 4 clearly display that the cipher is a strong one and it cannot be broken by any attack.

VI. REFERENCES

[1] V.U.K.Sastry, Aruna Varanasi, and S.Udaya Kumar, " A modern Hill cipher Involving a Permuted Key and Modular Arithmetic Addition Operation", International Journal of Advanced Research in Computer science (paper sent for publication).

[2] William Stallings, Cryptography and Network Security, Principles and Practice, Third edition, Pearson, 2003.