Volume 2, No. 4, April 2011
Journal of Global Research in Computer Science
ISSN-2229-371X
RESEARCH PAPER
Available Online at www.jgrcs.info

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

V.U.K.Sastry[1], Aruna Varanasi[*2] and S.Udaya Kumar[3]

[1]Department of computer Science and Engineering,SNIST
Hyderabad, India,
vuksastry@rediffmail.com
[*2]Department of computer Science and Engineering,SNIST
Hyderabad, India,
varanasi.aruna2002@gmail.com
[3]Department 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 A_0, which is obtained by permuting an involutory matrix A, which contains the key K. In this process, the basic relations governing the cipher are

$$C = (AP + A_0) \bmod N, \quad (1.1)$$

and

$$P = (A (C - A_0)) \bmod N, \quad (1.2)$$

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 A_0 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

$$C = (AP) \bmod N \oplus A_0, \quad (1.3)$$

and

$$P = (A(C \oplus A_0)) \bmod N. \quad (1.4)$$

In this analysis also we have introduced the iteration process, and the mix() function in each round of the iteration. The departure between the previous paper and the present one is the addition (+) in the previous paper is replaced by the xor in the present one. These two operations are expected to be of equal importance.

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.

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

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

$$K = [K_{ij}], \quad i = 1 \text{ to } n/2, \ j = 1 \text{ to } n/2, \quad (2.2)$$

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

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:

$$A = \begin{bmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{bmatrix} \quad (2.4)$$

$$A_{11} = K, \quad (2.5)$$

$$A_{22} = -K, \quad (2.6)$$

$$A_{12} = [d(I - K)] \bmod N, \quad (2.7)$$

$$A_{21} = [\lambda(I + K)] \bmod N, \quad (2.8)$$

$$(d\lambda) \bmod N = 1, \quad (2.9)$$

© JGRCS 2010, All Rights Reserved

where N=256.

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

The A_0, which is obtained by permuting the terms in A can be written in the form

$$A_0 = \begin{bmatrix} A_{22} & A_{21} \\ A_{12} & A_{11} \end{bmatrix}. \qquad (2.10)$$

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

$$C = (AP) \bmod N \oplus A_0, \qquad (2.11)$$

and

$$P = (A(C \oplus A_0)) \bmod N. \qquad (2.12)$$

The algorithms for encryption and decryption are given below.

Algorithm for Encryption

1. Read n,P,K,r,d
2. A_{11}=K
3. A= involute(A_{11},d)
4. A_0= permute(A)
5. for i = 1 to r
   {
   P = (A P)mod 256 ⊕ A_0
   P= mix(P)
   }
   C = P
6. Write(C)

Algorithm for Decryption

1. Read n,C,K,r,d
2. A_{11}=K
3. A= involute(A_{11},d)
4. A_0= permute(A)
5. for i= 1 to r
   {
   C = Imix(C)
   C= (A (C ⊕ A_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;
   B = $[dA_{ji}]$ mod N. // B 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= 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

"As we came across, unfortunately, all selfish and greedy people," (3.2)

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

$$P = \begin{bmatrix} 193 & 162 & 64 & 166 & 133 & 64 & 131 & 129 \\ 148 & 133 & 64 & 129 & 131 & 153 & 150 & 162 \\ 162 & 107 & 64 & 164 & 149 & 134 & 150 & 153 \\ 163 & 164 & 149 & 129 & 163 & 133 & 147 & 168 \\ 107 & 64 & 129 & 147 & 147 & 64 & 162 & 133 \\ 147 & 134 & 137 & 162 & 136 & 64 & 129 & 149 \\ 132 & 64 & 135 & 153 & 133 & 133 & 132 & 168 \\ 64 & 151 & 133 & 150 & 151 & 147 & 133 & 107 \end{bmatrix} \qquad (3.3)$$

Let us choose the key K in the form

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

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

© JGRCS 2010, All Rights Reserved

$$A=\begin{bmatrix} 215 & 111 & 19 & 147 & 62 & 19 & 167 & 39 \\ 223 & 99 & 254 & 12 & 195 & 26 & 198 & 92 \\ 56 & 1 & 127 & 174 & 88 & 157 & 70 & 182 \\ 59 & 146 & 189 & 81 & 47 & 138 & 233 & 16 \\ 72 & 133 & 145 & 17 & 41 & 145 & 237 & 109 \\ 85 & 76 & 106 & 132 & 33 & 157 & 2 & 244 \\ 104 & 75 & 128 & 250 & 200 & 255 & 129 & 82 \\ 73 & 198 & 95 & 6 & 197 & 110 & 67 & 175 \end{bmatrix} \quad (3.5)$$

On using (2.10) and (3.5), we get

$$A_0=\begin{bmatrix} 41 & 145 & 237 & 109 & 72 & 133 & 145 & 17 \\ 33 & 157 & 2 & 244 & 85 & 76 & 106 & 132 \\ 200 & 255 & 129 & 82 & 104 & 75 & 128 & 250 \\ 197 & 110 & 67 & 175 & 73 & 198 & 95 & 6 \\ 62 & 19 & 167 & 39 & 215 & 111 & 19 & 147 \\ 195 & 26 & 198 & 92 & 223 & 99 & 254 & 12 \\ 88 & 157 & 70 & 182 & 56 & 1 & 127 & 174 \\ 47 & 138 & 233 & 16 & 59 & 146 & 189 & 81 \end{bmatrix} \quad (3.6)$$

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

$$C=\begin{bmatrix} 150 & 239 & 213 & 252 & 227 & 178 & 205 & 47 \\ 83 & 83 & 147 & 31 & 197 & 185 & 96 & 83 \\ 39 & 255 & 79 & 1 & 4 & 187 & 143 & 244 \\ 50 & 183 & 44 & 114 & 6 & 72 & 191 & 58 \\ 100 & 120 & 118 & 203 & 198 & 213 & 120 & 11 \\ 42 & 248 & 76 & 57 & 164 & 218 & 91 & 92 \\ 157 & 73 & 228 & 60 & 176 & 182 & 231 & 43 \\ 119 & 14 & 229 & 19 & 199 & 52 & 86 & 235 \end{bmatrix} \quad (3.7)$$

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

Let us now study the avalanche effect, which tells us about the strength of the cipher.

To achieve this one, we replace the thirteenth character 'c' by 'b' in the plaintext (3.2). The EBCDIC codes of 'b' and 'c' are 130 and 131, which differ by one bit in their binary form. Now, on using the modified plaintext along with (3.5) and (3.6) and applying the encryption algorithm, we have the ciphertext C in the form

$$C=\begin{bmatrix} 71 & 245 & 119 & 211 & 223 & 154 & 227 & 50 \\ 198 & 229 & 53 & 64 & 159 & 85 & 8 & 200 \\ 226 & 137 & 17 & 175 & 240 & 181 & 40 & 96 \\ 147 & 117 & 29 & 111 & 231 & 64 & 189 & 212 \\ 139 & 112 & 81 & 62 & 214 & 226 & 102 & 128 \\ 139 & 18 & 131 & 151 & 33 & 162 & 165 & 144 \\ 67 & 9 & 166 & 158 & 228 & 174 & 210 & 192 \\ 172 & 211 & 14 & 150 & 145 & 152 & 184 & 142 \end{bmatrix} (3.8)$$

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 A_0, corresponding to the modified key, we apply the encryption algorithm (by taking the original plaintext), and obtain the corresponding ciphertext C. Thus we get

$$C\backslash=\begin{bmatrix} 82 & 31 & 150 & 136 & 158 & 252 & 27 & 182 \\ 135 & 186 & 182 & 197 & 53 & 31 & 110 & 112 \\ 92 & 66 & 111 & 242 & 247 & 182 & 110 & 189 \\ 117 & 222 & 32 & 217 & 236 & 235 & 71 & 63 \\ 9 & 3 & 146 & 73 & 55 & 207 & 180 & 226 \\ 220 & 129 & 241 & 186 & 175 & 240 & 27 & 160 \\ 61 & 143 & 67 & 26 & 226 & 73 & 104 & 149 \\ 62 & 221 & 190 & 217 & 186 & 240 & 129 & 215 \end{bmatrix} (3.9)$$

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

$$2^{136} = (2^{10})^{13.6} \approx (10^3)^{13.6} = 10^{40.8}.$$

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

$$\frac{10^{40.8}\times 10^{-7}}{365\times 24\times 60\times 60} = 3.171\times 10^{25.8} \text{ years}$$

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

$$C=M((AM((\ldots\ldots M((A\,M((AP) \bmod 256 \oplus A_0)) \bmod 256 \oplus A_0)\ \ldots\ldots) \bmod 256 \oplus A_0))\bmod 256 \oplus A_0). \quad (4.1)$$

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

© JGRCS 2010, All Rights Reserved

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

150	239	213	252	227	178	205	47
83	83	147	31	197	185	96	83
39	255	79	1	4	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
103	94	22	211	199	192	53	120
61	18	223	93	42	248	24	29
193	75	217	22	124	120	105	8
155	22	70	47	197	250	177	221
107	77	132	11	130	254	148	237
211	93	217	77	123	35	255	128
112	43	195	218	167	32	217	23
84	57	203	249	31	3	75	5
222	129	87	127	156	28	3	168
162	53	171	1	42	114	212	55
154	146	42	203	79	44	174	151
188	134	216	246	96	244	190	181
112	14	255	150	133	138	15	82
94	84	25	174	139	248	11	1
186	226	68	228	32	229	72	174
219	221	40	195	115	2	41	130
87	124	42	115	79	132	213	195
206	139	136	116	158	27	62	134
96	242	247	184	35	35	50	232
26	91	7	196	80	29	210	121
208	77	81	105	140	56	107	181
32	70	206	135	107	228	48	55
21	80	104	67	94	147	123	121
8	125	201	248	16	231	84	179
161	8	109	219	149	183	11	203
69	149	45	83	64	19	25	104
13	121	46	10	238	226	135	199
246	143	7	42	89	199	238	3
188	126	53	156	27	132	143	188
63	226	215	96	165	186	23	255
80	42	180	2	156	38	191	84
211	211	33	31	191	237	155	1

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

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

[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, S.Udaya Kumar, "Advanced Hill Cipher Involving Permutation and Iteration", International Journal of Advanced Research in

© JGRCS 2010, All Rights Reserved

Computer Science, Vol.1, No.4, pp. 141-145, Nov-Dec. 2010.

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.

© JGRCS 2010, All Rights Reserved