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 a Permuted Key and Modular Arithmetic Addition Operation

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 devoted our attention to the study of a block cipher by generalizing advanced Hill cipher by including a permuted key. In this analysis we find that the iteration process, the mix operation and the modular arithmetic operation involved in the cipher mixes the binary bits of the key and the plaintext in a thorough manner. The avalanche effect and the cryptanalysis markedly indicate that the cipher is a strong one.

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

INTRODUCTION

The study of the advanced Hill cipher [1], which depends mainly upon the concept of an involutory matrix (a matrix which is equal to its inverse), has roused the interest of researchers in the areas of cryptography and image cryptography. In a recent investigation, we [2-5] have studied several aspects of the advanced Hill cipher by including iteration process and a process of permutation in each round of the iteration. In all these analyses, we have established that the strength of the cipher is quite significant.

The basic relations supporting the development of the advanced Hill cipher can be mentioned as follows:

$$(A\,A^{-1}) \bmod N = I, \quad (1.1)$$
and
$$A^{-1} = A, \quad (1.2)$$

where A is a square matrix of size n, A^{-1} is the modular arithmetic inverse of A, and N is any non zero positive integer chosen appropriately.

From (1.1) and (1.2) we get
$$A^2 \bmod N = I, \quad (1.3)$$
in which I is an identity matrix.

From (1.3), the matrix A can be obtained by representing it in the form

$$A = \begin{bmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{bmatrix} \quad (1.4)$$

and taking A_{11}=K, where K is the key matrix.

The relations governing A_{22}, A_{12} and A_{21} are given by

$$A_{22} = -K, \quad (1.5)$$
$$A_{12} = [d(I - K)] \bmod N, \quad (1.6)$$
$$A_{21} = [\lambda(I + K)] \bmod N, \quad (1.7)$$
$$\text{where } (d\lambda) \bmod N = 1. \quad (1.8)$$

In order to have a detailed discussion for obtaining A, we refer to [2].

The advanced Hill cipher [2] is governed by the relations
$$C = (A\,P) \bmod N, \quad (1.9)$$
and
$$P = (A\,C) \bmod N. \quad (1.10)$$

In the present investigation, our objective is to develop a modern form of the advanced Hill cipher by using the ideas of the modern Hill cipher [6-7] and the advanced Hill cipher [2].

The cipher which we are going to develop here is governed by the basic relations
$$C = (AP + A_0) \bmod N, \quad (1.11)$$
and
$$P = (A(C - A_0)) \bmod N \quad (1.12)$$

where

$$A_0 = \begin{bmatrix} A_{22} & A_{21} \\ A_{12} & A_{11} \end{bmatrix} \quad (1.13)$$

is obtained by permuting the sub matrices of A.

In this analysis, we include iteration process, and a process of mixing in each round of the iteration.

Now let us mention the plan of the paper. In section 2, we have introduced the development of the cipher and presented the flow charts and algorithms for the encryption and the decryption. We have illustrated the cipher with a suitable example in section 3. Further, we have studied the avalanche effect in this section. Then we have carried out the cryptanalysis in section 4. Finally in section 5, we have devoted our attention to computations and conclusions.

DEVELOPMENT OF THE CIPHER

Let us consider a plaintext, P. On using EBCDIC code, let P be written in the form of a matrix given by

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

where n is any positive even integer, and each element of P is a decimal number lying between 0 and 255.

Let us take a key matrix K, which can be represented in the form

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

where each K_{ij} is also a decimal number in the interval 0 to 255.

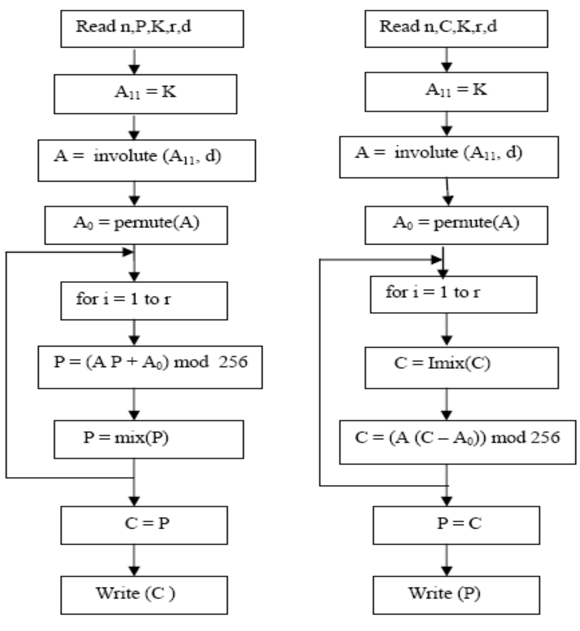
On using (1.4), taking the key matrix K, we get the matrix A. Then the ciphertext C can be written in the form

$C = (AP+A_0) \bmod N$, (2.3)

where N= 256, and A_0 is obtained from (1.13).

Here we take $C = [C_{ij}]$, i= 1 to n, j=1 to n.

The flow chart describing the cipher is given in Fig.1



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

Figure 1. Schematic diagram of the Cipher

In this, the function involute() includes the procedure, given by the relations (1.4) – (1.8), for obtaining the involutory matrix A. Here, we have included iteration process and the function mix() in each round of the iteration process to achieve thorough confusion and diffusion in arriving at the ciphertext. Further, here we have used the function permute() for obtaining A_0. The function Imix() denotes the reverse process of mix(). The detailed discussion of mix is given later.

The algorithms for encryption and decryption are written below.

Algorithm for Encryption

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

Algorithm for Decryption

1. Read n,C,K,r,d
2. $A_{11} = K$
3. $A = \text{involute}(A_{11},d)$
4. $A_0=\text{permute}(A)$
4. for i= 1 to r
   {
   C = Imix(C)
   $C= (A\,(C-A_0))\bmod 256$
   }
   P = C
4. Write (P)

In the above algorithms ‘r’ indicates the number of rounds.

Let us now consider the process of mixing, represented by the function mix(), in the encryption algorithm. In each stage of the iteration process, the plaintext matrix P is of size nxn, where each element can be represented in terms of eight binary bits. Thus the entire matrix can be written in the form of a string of binary bits containing $8n^2$ bits. Here, this string is divided into four substrings wherein each one is of size $2n^2$ binary bits. These strings can be written in the form

$$q_1 \quad q_2 \quad q_3 \quad q_4 \quad . \quad . \quad . \quad . \quad q_{2n^2},$$

$$r_1 \quad r_2 \quad r_3 \quad r_4 \quad . \quad . \quad . \quad . \quad r_{2n^2},$$

$$s_1 \quad s_2 \quad s_3 \quad s_4 \quad . \quad . \quad . \quad . \quad s_{2n^2},$$

$$t_1 \quad t_2 \quad t_3 \quad t_4 \quad . \quad . \quad . \quad . \quad t_{2n^2}.$$

Here, the mixing is done by arranging the binary bits of the different substrings as shown below:

$q_1\ r_1\ s_1\ t_1\ q_2\ r_2\ s_2\ t_2\ q_3\ r_3\ s_3\ t_3\ q_4\ r_4\ s_4\ t_4\ \ldots\ldots\ q_{2n^2}\ r_{2n^2}\ s_{2n^2}\ t_{2n^2}$.

Then this is decomposed into n^2 substrings by considering 8 bits at a time in order. On writing each substring in the form of a decimal number, we get a square matrix of size n.

ILLUSTRATION OF THE CIPHER

Consider the plaintext given below:

"Dear! Where are you? How are you? I have been waiting for your arrival with wide open eyes. Your mother and father are visiting several houses and seeing several matches for you. Of course I have got my belief in you and our love and affection are eternal. I know this fact and wait for you." (3.1)

We focus our attention on the first sixty four characters of the plaintext (3.1). This is given by
"Dear! Where are you? How are you? I have been waiting for your a" (3.2)

On using the EBCDIC code, the plaintext under consideration can be written in the form

$$P = \begin{bmatrix} 196 & 133 & 129 & 153 & 79 & 64 & 230 & 136 \\ 133 & 153 & 133 & 64 & 129 & 153 & 133 & 64 \\ 168 & 150 & 164 & 111 & 64 & 200 & 150 & 166 \\ 64 & 129 & 153 & 133 & 64 & 168 & 150 & 164 \\ 111 & 64 & 201 & 64 & 136 & 129 & 165 & 133 \\ 64 & 130 & 133 & 133 & 149 & 64 & 166 & 129 \\ 137 & 163 & 137 & 149 & 135 & 64 & 134 & 150 \\ 153 & 64 & 168 & 150 & 164 & 153 & 64 & 129 \end{bmatrix} \quad (3.3)$$

Let us take the key K in the form

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

On using the relations (1.4) - (1.8) and taking d=99, we get

$$A = \begin{bmatrix} 123 & 25 & 9 & 67 & 210 & 85 & 133 & 23 \\ 134 & 17 & 20 & 11 & 46 & 208 & 68 & 191 \\ 48 & 199 & 209 & 75 & 112 & 11 & 144 & 255 \\ 39 & 55 & 85 & 92 & 235 & 187 & 33 & 207 \\ 84 & 83 & 163 & 161 & 133 & 231 & 247 & 189 \\ 66 & 70 & 220 & 57 & 122 & 239 & 236 & 245 \\ 16 & 77 & 134 & 249 & 208 & 57 & 47 & 181 \\ 109 & 29 & 231 & 63 & 217 & 201 & 171 & 164 \end{bmatrix} \quad (3.5)$$

From this, on using (1.13), we get

$$A_0 = \begin{bmatrix} 133 & 231 & 247 & 189 & 84 & 83 & 163 & 161 \\ 122 & 239 & 236 & 245 & 66 & 70 & 220 & 57 \\ 208 & 57 & 47 & 181 & 16 & 77 & 134 & 249 \\ 217 & 201 & 171 & 164 & 109 & 29 & 231 & 63 \\ 210 & 85 & 133 & 23 & 123 & 25 & 9 & 67 \\ 46 & 208 & 68 & 191 & 134 & 17 & 20 & 11 \\ 112 & 11 & 144 & 255 & 48 & 199 & 209 & 75 \\ 235 & 187 & 33 & 207 & 39 & 55 & 85 & 92 \end{bmatrix} \quad (3.6)$$

Now, on using A, A_0 and P, given by (3.5),(3.6) and (3.3), and the encryption algorithm, with r=16, we get the ciphertext C. This is given by

$$C = \begin{bmatrix} 251 & 11 & 5 & 105 & 173 & 143 & 204 & 145 \\ 193 & 115 & 144 & 83 & 153 & 214 & 71 & 43 \\ 156 & 207 & 113 & 92 & 2 & 49 & 22 & 68 \\ 251 & 11 & 122 & 165 & 12 & 217 & 250 & 4 \\ 73 & 5 & 120 & 124 & 241 & 0 & 17 & 3 \\ 69 & 166 & 161 & 70 & 31 & 205 & 243 & 215 \\ 185 & 187 & 131 & 79 & 68 & 147 & 41 & 84 \\ 91 & 211 & 162 & 57 & 89 & 209 & 252 & 127 \end{bmatrix} \quad (3.7)$$

On using (3.5), (3.6) and (3.7), and applying the decryption algorithm, we get back the original plaintext given by (3.3).

Let us now focus our attention on the avalanche effect, which yields a measure regarding the strength of the cipher.

To carry out this one, firstly we replace the ninth character 'e' of the plaintext (3.2) by'd'. The EBCDIC codes of'd ' and 'e ' are 132 and 133 . On converting these two numbers into their binary form, we find that they differ by one bit. On using the plaintext, including afore mentioned modification, the A and A_0 given by (3.5) and (3.6), we apply the encryption algorithm, and find the ciphertext C. Thus we have

$$C = \begin{bmatrix} 142 & 183 & 242 & 74 & 187 & 174 & 88 & 222 \\ 25 & 126 & 7 & 58 & 148 & 111 & 197 & 73 \\ 251 & 13 & 32 & 246 & 141 & 187 & 200 & 159 \\ 148 & 106 & 193 & 178 & 30 & 203 & 233 & 229 \\ 141 & 205 & 193 & 164 & 237 & 223 & 46 & 200 \\ 169 & 235 & 60 & 223 & 79 & 5 & 8 & 204 \\ 127 & 47 & 240 & 22 & 169 & 246 & 99 & 125 \\ 249 & 1 & 164 & 201 & 81 & 22 & 195 & 152 \end{bmatrix} \quad (3.8)$$

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

Let us now focus our attention on a one bit change in the key K. In order to achieve this one, we replace the first row fourth column element " 67 " of (3.4), by " 66 ". After obtaining A and the corresponding A_0, we perform the encryption (using the original plaintext). Thus we get the ciphertext given by

$$C = \begin{bmatrix} 82 & 199 & 217 & 55 & 3 & 67 & 65 & 76 \\ 197 & 14 & 108 & 193 & 39 & 213 & 88 & 140 \\ 69 & 247 & 186 & 101 & 101 & 110 & 227 & 118 \\ 106 & 76 & 105 & 28 & 180 & 46 & 197 & 185 \\ 114 & 199 & 245 & 174 & 223 & 130 & 9 & 112 \\ 79 & 115 & 94 & 127 & 148 & 24 & 51 & 44 \\ 33 & 111 & 186 & 212 & 52 & 25 & 127 & 119 \\ 82 & 100 & 115 & 122 & 106 & 37 & 74 & 128 \end{bmatrix} \quad (3.9)$$

Now on comparing (3.7) and (3.9), in their binary form, we find that they differ by 278 bits (out of 512 bits). This also thoroughly suggests that the cipher is a potential one.

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

In all these attacks, the primary objective is to determine either the key or a function of the key so that the cipher can be broken. This is the desire of the cryptanalyst.

Let us now consider, firstly, the ciphertext only attack. In this analysis the key K, given by (3.4), is consisting of 16 numbers wherein each number can be represented in the form of 8 binary bits. In addition to this key, we have made use of an integer'd', which can be considered as an additional key, in the development of the involutory matrix, A. This key requires eight more binary bits, and hence the total length of the key, which controls the cipher, is 136 bits. Thus the size of the key space is

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

If the time required for obtaining the plaintext with one value of the key in the key space is 10^{-7} seconds, then the time for carrying out the determination of the plaintext with all the possible keys in the key space is

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

As this number is a formidable one, it is simply impossible to break the cipher by this attack.

In the case of the known plaintext attack, we have as many pairs of plaintext and ciphertext as we wish. In this analysis, as we have the prominent features, namely, iteration, mixing and modular arithmetic addition operation, involving A_0, by the time we reach the final stage of the iteration process, we get a relation between the ciphertext, the involutory matrix A (including the key K) and the original plaintext P in the form

$$C = M((AM((\ldots\ldots. M((A M((AP + A_0) \bmod 256) + A_0) \bmod 256) \ldots\ldots.+A_0)\bmod 256)+A_0)\bmod 256)$$

for r=16. (4.1)

In the above relation, A_0 is obtained by permuting A, see (1.13), and the M() stands for the function mix(). In (4.1) the matrix A (containing the key K) is multiplied with the plaintext P, and it is added to A_0. Then mixing is carried out after performing the mod 256. On account of this sort of operations, the binary bits of the key and the plaintext are thoroughly mixed at various stages, and hence it is impossible to decipher the key or a function of the key, which enables the cryptanalyst to break the cipher. From this we conclude that the cipher cannot be broken by the known plaintext attack.

With all effort, basing upon intuition, no special choice of either the plaintext or the ciphertext appears to yield a scope for breaking the cipher.

In the light of the above discussion of cryptanalysis, we firmly conclude that the cipher is a strong one, and it cannot be broken by any means.

COMPUTATIONS AND CONCLUSIONS

In this paper, we have developed a block cipher called modern advanced Hill cipher. In this the Hill cipher has taken a very refined shape from the view point of the analysis and the strength of the cipher.

Here the computations are carried out by writing programs for encryption and decryption in Java.

The ciphertext corresponding to the complete plaintext, given by (3.1), is obtained in the form

251	11	5	105	173	143	204	145
193	115	144	83	153	214	71	43
156	207	113	92	2	49	22	68
251	11	122	165	12	217	250	4
73	5	120	124	241	0	17	3
69	166	161	70	31	205	243	215
185	187	131	79	68	147	41	84
91	211	162	57	89	209	252	127
98	244	81	243	134	204	255	46
191	222	29	239	252	120	244	86
249	251	236	68	174	157	193	132
22	151	197	13	62	184	91	69
135	11	0	154	207	20	164	168
133	249	94	165	100	104	76	79
168	54	233	76	31	71	198	187
49	23	220	77	238	40	109	107
57	96	222	162	148	79	79	119
124	136	1	32	145	221	235	108
201	239	112	202	220	213	221	23
77	85	143	124	0	158	107	140
91	74	199	6	230	207	223	65
238	187	27	80	55	139	226	229
184	103	37	136	5	23	77	244
110	46	200	53	36	129	49	207
32	240	126	205	98	10	166	198
28	148	225	203	1	63	8	218
190	126	93	20	106	45	33	216
82	232	31	104	176	235	183	109
48	194	5	255	227	189	119	110
221	205	196	124	193	154	157	218
209	137	143	230	218	74	253	83
83	111	69	179	246	100	6	144
129	214	129	94	154	132	136	3
147	78	92	91	166	242	149	201
176	192	164	255	69	188	245	48
244	199	120	62	63	179	120	191
213	254	220	161	210	20	90	125
77	237	216	30	136	114	249	222
80	49	163	182	109	248	136	116
119	63	104	145	164	191	120	107

In obtaining this ciphertext, we have divided the plaintext (3.1) into five blocks. Of course, in the last block we have added twenty nine blank characters to make it a complete block.

From the significance of the avalanche effect and the consideration of the cryptanalysis, here it is interesting to note that this block cipher is a strong one, and it is quite comparable with any other block cipher in all respects.

In this analysis A_0 is obtained by permuting A in a particular manner. Here it is to be noted that A_0 can be obtained in many other ways by permuting A. For example A_0 can be taken as A^T(transpose of A) or it can be obtained by interchanging rows and or columns in any desired fashion.

REFERENCES

[1] 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.

[2] V.U.K.Sastry, Aruna Varanasi, S.Udaya Kumar, "Advanced Hill Cipher Involving Permutation and Iteration", International Journal of Advanced Research in Computer Science, Vol.1, No.4, pp. 141-145, Nov-Dec. 2010.

[3] V.U.K.Sastry, Aruna Varanasi, S.Udaya Kumar, "Advanced Hill Cipher Handling the Entire Plaintext as a Single Block", International Journal of Advanced Research in Computer Science, Vol.1, No.4, pp. 180-184, Nov-Dec. 2010.

[4] V.U.K.Sastry, Aruna Varanasi, S.Udaya Kumar, "Advanced Hill Cipher Involving a Key Applied on Both the Sides of the Plaintext", International Journal of Computational Intelligence and Information Security,Vol. 1 No. 9, pp. 70-78, November 2010.

[5] V.U.K.Sastry, Aruna Varanasi, S.Udaya Kumar," Advanced Hill Cipher Involving a Pair of Keys", International Journal of Computational Intelligence and Information Security, Vol.2 No.1, pp 100-108, January 2011.

[6] V.U.K.Sastry, Aruna Varanasi, S.Udaya Kumar," A Modern Hill Cipher Involving a Permuted Key and Modular Arithmetic Addition Operation", International Journal of Advanced Research in Computer Science, Vol.2, No.1, pp.162-165, Jan-Feb 2011.

[7] V.U.K.Sastry, Aruna Varanasi, S.Udaya Kumar," A Modern Hill Cipher Involving XOR operation and a Permuted Key ", International Journal of Advanced Research in Computer Science, Vol.2, No.1, pp.153-155, Jan-Feb 2011..

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

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.