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 Involving Permutation and Iteration

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

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

S.Udaya Kumar
Department of Computer Science and Engineering, SNIST
Hyderabad, India
uksusarla@rediffmail.com

Abstract: In this Paper we have developed a block cipher which depends upon iteration and permutation. In this we have used an involutory matrix (a matrix whose inverse is the same as the matrix) wherein the elements of the matrix depend upon the key chosen by us for encryption as well as decryption. As the permutation plays a prominent role in dissipating the characteristic features of the plaintext and the key, the strength of the cipher is found to be enhanced significantly. In this analysis obtaining the involutory matrix involves advanced concepts and elementary operations and hence obtaining it has become very simple. The avalanche effect and the cryptanalysis have clearly indicated that this cipher is a strong one.

Keywords: permutation, iteration, involutory matrix, key, ciphertext, modular arithmetic, cryptanalysis.

I. INTRODUCTION

In the area of Cryptography, classical Hill cipher [1] is a prominent block cipher. Though this cipher had its origin a century ago, approximately, it has gained considerable impetus in the recent years. Several authors have modified the Hill cipher [2-10] by introducing iteration and some other operations such as interlacing, mixing, permutation (key independent and key dependent), so that the strength of the cipher is enhanced enormously.

The Hill cipher is governed by the relations

$$C = (KP) \bmod 26, \qquad (1.1)$$

$$P = (K^{-1} C) \bmod 26, \qquad (1.2)$$

where P is the plaintext column vector, K the key matrix and C is the corresponding ciphertext column vector. Here K^{-1} is the modular arithmetic inverse of the K, governed by the relation

$$(K K^{-1}) \bmod 26 = I. \qquad (1.3)$$

In order to obtain the modular arithmetic inverse of a matrix, we use the concepts of arithmetic inverse of a matrix [11] and the modular arithmetic. We employ analytical method or numerical method, such as Gauss Jordon elimination method[12], for obtaining the modular arithmetic inverse depending upon the size of the matrix.

In the recent past Acharya et al[13] have developed an analytical method for obtaining the modular arithmetic inverse of a matrix, whose inverse is the same as the original matrix. This sort of matrix is said to be an involutory matrix[14]. This led to the development of Advanced Hill cipher.

The basic ideas in obtaining the modular arithmetic inverse of an involutory matrix can be summarized as follows:

Let $A = [a_{ij}]$, i= 1 to n. j=1 to n be a square matrix of size n. Let it be represented in the form

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

where all the sub matrices A_{11}, $A_{12,}$ A_{21} and A_{22} are square matrices of size n/2.

As the modular arithmetic inverse of an involutory matrix is governed by the relations

$$(A\,A^{-1}) \bmod N = I, \qquad (1.5)$$

and $A^{-1} = A$, (1.6)

we have $A^2 \bmod N = I$. (1.7)

Here I is an Identity Matrix and N is any non zero positive integer chosen appropriately.

From (1.7) and (1.4) we get

$$A_{22} \bmod N = -\,A_{11} \bmod N, \qquad (1.8)$$

$$A_{12}=[d(I- A_{11})] \bmod N, \qquad (1.9)$$

$$A_{21}=[\lambda(I+ A_{11})] \bmod N, \qquad (1.10)$$

where $(d\lambda) \bmod N = 1$. (1.11)

Given A_{11}, on selecting d, where d lies in the interval $0<d<N$, firstly we obtain λ from (1.11). Then we determine A_{22}, A_{12} and A_{21} by satisfying the relations (1.8)-(1.10).

If A_{11} is the key, a square matrix of size n/2, then we get the involutory matrix A of size n.

For example when N=13,

$A_{11} = \begin{bmatrix} 3 & 11 \\ 10 & 9 \end{bmatrix}$ and 'd' is taken as 2, we get λ=7. Then we have

$$A = \begin{bmatrix} 3 & 11 & 9 & 4 \\ 10 & 9 & 6 & 10 \\ 2 & 12 & 10 & 2 \\ 5 & 5 & 3 & 4 \end{bmatrix}.$$

In what follows we present the plan of the paper. We discuss the development of the cipher and present the algorithms for encryption and decryption in secion 2. We illustrate the cipher by taking an example in section 3. We analyze the cryptanalysis in section 4. Finally in section 5, we deal with computations and conclusions.

II. DEVELOPMENT OF THE CIPHER

Consider a plaintext. On using EBCDIC code, let us represent the characters in the plaintext in the form of a column vector P, having n elements, wherein each element lies in [0-255]. Thus we have

$P = [P_i]^T$, i= 1 to n, (2.1)

in which T denotes the transpose.

Let K be the key matrix given by

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

where n is an even number.

Here each element of K is lying in [0-255].

Let us construct an involutory matrix A, where

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

in which A_{12}, A_{21} and A_{22} are obtained by taking A_{11}= K, and using the relations (1.8) – (1.11).

The basic relations governing the encryption are

P= (A P) mod 256,

and

P=Permute(P).

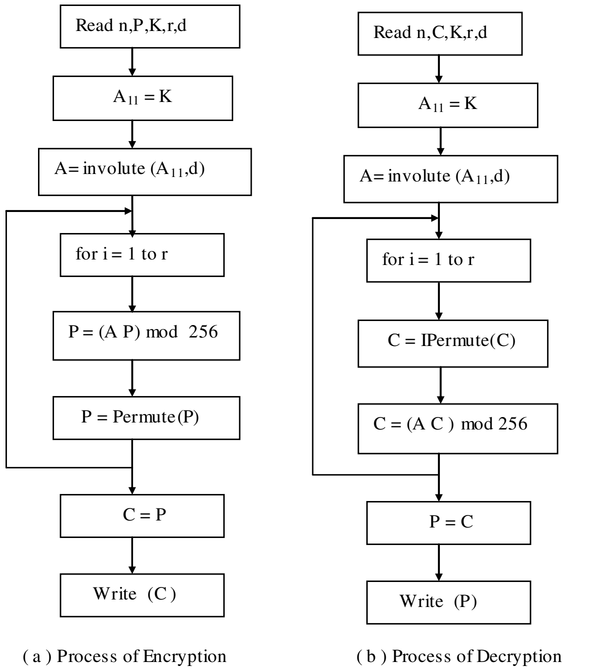
The corresponding steps in decryption are

C = IPermute(C),

and

C = (A C) mod 256.

The flow chart for encryption and decryption are presented in Figure-1.



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

Figure 1. Schematic diagram of the Cipher

In developing the function Permute() we have adofollowing procedure. We convert each component of the column vector P into its binary form. Thus we get a matrix having n rows and eight columns. This is given by

$$\begin{bmatrix}
P_{11} & P_{12} & . & . & . & . & P_{17} & P_{18} \\
. & & & & & & & . \\
. & & & & & & & . \\
. & & & & & & & . \\
. & & . & & & & & . \\
.P_{m1} & P_{m2} & & . & & & P_{m7} & P_{m8} \\
. & & & & . & & & . \\
. & & & & & . & & . \\
. & & & & & & & . \\
. & & & & & & & . \\
P_{n1} & P_{n2} & . & . & . & . & P_{n7} & P_{n8}
\end{bmatrix},$$

Taking the upper portion of the above matrix (consisting of m rows), starting from mth row last element Pm8, we move towards P_{11} in the back ward direction and form the first four columns of the new matrix shown below. The remaining four columns of the following matrix are filled, in column wise manner, with the lower half of the above matrix by starting with the (m+1)th row first element $P_{(m+1)1}$ and going up to the last element P_{n8} of that portion of the matrix in order.

$$\begin{bmatrix}
P_{m8} & . & . & P_{(m+1)1} & . & \\
P_{m7} & & & P_{(m+1)2} & & . \\
P_{m6} & & & P_{(m+1)3} & & . \\
P_{m5} & & & P_{(m+1)4} & & . \\
. & . & & & & . \\
. & & . & & & \\
. & & & & . & . \\
. & P_{14} & & & . & P_{n5} \\
. & P_{13} & & & & P_{n6} \\
 & P_{12} & & & & P_{n7} \\
 & .P_{11} & & . & . & P_{n8}
\end{bmatrix}$$

On converting the eight bits in each row in to its decimal equivalent, we get the transformed P.

Now let us consider an example. When n=8, let us take

$P=[\ 193\ \ 140\ \ 224\ \ 186\ \ 211\ \ 93\ \ 188\ \ 222\ ]^T$.

On converting each element of P into its binary form, we get the matrix given by

$$\begin{bmatrix}
1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\
1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\
1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 \\
1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 \\
0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 \\
1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\
1 & 1 & 0 & 1 & 1 & 1 & 1 & 0
\end{bmatrix}.$$

On filling up the first four columns and the later four columns of the new matrix with the upper half and the lower half of the above matrix respectively, as stated earlier, we get

$$\begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \end{bmatrix}.$$

Thus we have the P in its final form and this is given by

$$P=[\,27\ \ 141\ \ 34\ \ 175\ \ 135\ \ 199\ \ 89\ \ 252\,].^T$$

This function Permute() scatters the binary bits of the Product of K and P at every stage of the iteration process. This causes a lot of diffusion and confusion in the development of the cipher.

The function IPermute(), used in the decryption , carries out the inverse operation of the Permute().

The algorithms concerned to the processes of the encryption and the 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. for i = 1 to r
   {
           P = (A P ) mod 256
           P= Permute(P)
   }
   C = P
5. Write( C )
```

Algorithm for Decryption

```
1. Read n,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)
   {
           $\lambda$ = i;
           break;
   }
}
3. $A_{12}$=[d(I- $A_{11}$)] mod 256
4. $A_{21}$=[$\lambda$(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. 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 focus our attention on the first eight characters:

'All the ' (3.2)

On using the EBCDIC code we get the plaintext P in the form

$$P= [193\ \ 147\ \ 147\ \ \ 64\ \ \ 163\ \ 136\ \ 133\ \ \ 64]^{\,T} \quad (3.3)$$

Let us take the key matrix K in the form

$$K=\begin{bmatrix} 128 & 12 & 45 & 34 \\ 189 & 200 & 9 & 99 \\ 245 & 135 & 59 & 33 \\ 72 & 122 & 27 & 109 \end{bmatrix}. \qquad (3.4)$$

Let us choose a value for d. Let d be equal to 179. This can also be considered as key. Then on taking A_{11}=K, and using the function involute(), mentioned in section 2, we get

$$A=\begin{bmatrix} 128 & 12 & 45 & 34 & 51 & 156 & 137 & 58 \\ 189 & 200 & 9 & 99 & 217 & 219 & 181 & 199 \\ 245 & 135 & 59 & 33 & 177 & 155 & 114 & 237 \\ 72 & 122 & 27 & 109 & 168 & 178 & 31 & 124 \\ 251 & 196 & 159 & 86 & 128 & 244 & 211 & 222 \\ 207 & 147 & 83 & 145 & 67 & 56 & 247 & 157 \\ 183 & 221 & 212 & 219 & 11 & 121 & 197 & 223 \\ 152 & 158 & 249 & 218 & 184 & 134 & 229 & 147 \end{bmatrix} (3.5)$$

On using the encryption algorithm, discussed in section 2, and carrying out the 16 rounds of the iteration process, we obtain the ciphertext in the form

$$C= [108\ \ \ 117\ \ \ 105\ \ \ 111\ \ \ 198\ \ \ \ 67\ \ \ \ 21\ \ \ 185]^T \quad (3.6)$$

Now, on using (3.5) and (3.6), and applying the decryption algorithm, we notice that the ciphertext (3.6) yields the original plaintext given by (3.3).

Now let us discuss the avalanche effect, which is a bench mark for the strength of the cipher. To this end we change the 7th character 'e' of the plaintext to 'd'. The EBCDIC code of 'e' and 'd' are 133 and 132 respectively. These numbers in their binary form differ by one binary bit. On using the modified plaintext and the involutory matrix, A given by (3.5), and the encryption algorithm, given in section 2, we obtain the corresponding ciphertext given by

$$C=[\,79\ \ \ \ 102\ \ \ 250\ \ \ 141\ \ \ \ 95\ \ \ \ 236\ \ \ 250\ \ \ 180]^T \quad (3.7)$$

On converting (3.6) and (3.7) into their binary form, we find that the two ciphertexts differ by 34 bits (out of 64 bits). This indicates that the cipher is a strong one.

Now let us change the key by one binary bit. This is achieved by replacing the second row second column element of K, given by (3.4), from 200 to 201. Correspondingly the involutory matrix assumes the form

$$A=\begin{bmatrix}128 & 12 & 45 & 34 & 51 & 156 & 137 & 58\\ 189 & 201 & 9 & 99 & 217 & 40 & 181 & 199\\ 245 & 135 & 59 & 33 & 177 & 155 & 114 & 237\\ 72 & 122 & 27 & 109 & 168 & 178 & 31 & 124\\ 251 & 196 & 159 & 86 & 128 & 244 & 211 & 222\\ 207 & 14 & 83 & 145 & 67 & 55 & 247 & 157\\ 183 & 221 & 212 & 219 & 11 & 121 & 197 & 223\\ 152 & 158 & 249 & 218 & 184 & 134 & 229 & 147\end{bmatrix} \quad (3.8)$$

On using the original plaintext (3.3), modified A given by (3.8) and the encryption algorithm, we get the ciphertext, C given by

$$C=\begin{bmatrix}242 & 76 & 142 & 170 & 211 & 155 & 122 & 147\end{bmatrix}^T \quad (3.9)$$

On transforming (3.6) and (3.9) into their binary form, we notice that these two ciphertexts differ by 35 bits (out of 64 bits). This also clearly shows that this cipher is a potential one.

IV. Cryptanalysis

In Cryptography, the study of the cryptanalysis is the crucial step, which enables us to decide the strength of a cipher. In the literature of cryptography, the various well known attacks for finding the strength of a cipher are

1. ciphertext only attack (Brute force attack),
2. known plaintext attack,
3. chosen plaintext attack, and
4. chosen ciphertext attack.

In this cipher the key matrix is a square matrix of size n/2. Thus the number of elements in the key is n/2xn/2 that is $n^2/4$. As each element can be represented in terms of eight binary bits, the size of the key space is 2^{2n^2} .

Here it is to be noted that we are having one more number d, which lies between 0 and 255, in our control. This is also to be considered as a key. In the light of this fact the key space is of size 2^{2n^2+8}.

Let us assume that the time required for obtaining the plaintext from the given ciphertext with one value of the key in the key space is 10^{-7} seconds. Thus the time required for the computation of the problem with all possible keys in the key space is

$$\frac{2^{2n^2+8}\times10^{-7}}{365\times24\times60\times60}=8.11\times2^{2n^2}\times10^{-13}\text{ years}$$

If n=8, then the time required

$$=8.11\times2^{128}\times10^{-13}=8.11\times\left(2^{10}\right)^{12.8}\times10^{-13}$$
$$\approx 8.11\,\text{x}\left(10^{38.4}\,\text{x}10^{-13}\right)$$
$$=8.11\times10^{25.4}\text{ years}$$

Hence the cipher cannot be broken by the brute force attack.

In the known plaintext attack we are having as many plaintext and ciphertext pairs as we require at our disposal. In the cipher under consideration each plaintext is multiplied by A, which is containing the key K. On account of the mod operation the product of A and P undergoes change. Then the function Permute() shuffles the binary bits of the resulting product and hence the bits of the key are scattered in each round of the iteration process enormously. Thus by the time we get the ciphertext, after the completion of all the rounds, the key and the plaintext are no more in their shape, and hence the possibility of obtaining modular arithmetic inverse of the plaintext matrix (which is usually done in breaking the Hill cipher) does not arise in this case. Hence the cipher cannot be broken in this case also.

The last two cases require a special vision and the possibility of breaking the cipher arises very rarely.

Thus, in this case, we do not find any possibility with all effort.

From the above discussion we finally conclude that this cipher is a strong one and breaking the cipher by any means is impossible.

V. Computations and Conclusions

The algorithms for encryption and decryption, presented in section 2, are written in java.

The plaintext given by (3.1) can be divided into 32 blocks, wherein each block contains 8 characters. On adopting the procedure mentioned in section 3, the ciphertext corresponding to the entire plaintext (all the thirty two blocks) is obtained as follows

108	117	105	111	198	67	21	185
116	234	154	49	91	182	192	43
64	122	155	250	204	238	221	73
250	114	180	58	80	208	42	234
203	100	36	1	27	77	66	40
83	88	63	178	215	72	212	97
26	116	135	6	8	183	32	16
128	111	93	32	10	116	13	71
230	165	66	120	236	136	75	175
110	75	255	78	2	69	39	32
94	229	46	129	35	15	210	195
210	119	105	103	1	17	253	123
199	91	80	195	59	127	241	12
20	105	10	186	222	224	212	19
15	95	167	31	112	134	43	179
179	154	97	32	94	229	54	94
24	150	141	201	201	164	157	171
101	150	25	145	111	60	241	83
33	73	65	209	192	82	157	227
99	191	166	41	155	151	135	157
42	52	238	95	21	90	10	180
86	43	107	14	50	181	152	120
74	107	61	76	55	53	246	86
140	115	201	135	171	249	227	247
127	37	194	224	14	252	10	197
71	134	118	240	87	44	41	76
82	209	91	231	35	82	184	39
72	85	40	97	235	93	209	107
107	167	84	119	21	33	48	189
21	160	13	30	207	25	233	108
88	132	83	247	144	136	171	28
107	152	116	111	203	15	131	240

Here it is to be noted that, in the case of the last block, we have appended six more characters as the length of the block is less than eight.

In this analysis, the key K is embedded at the left most top corner of the involutary matrix A. In the case of involutary matrix as A^{-1}=A, the computations which are to be carried out for obtaining the inverse of A are much less in comparison with those required for computing the inverse of any matrix in general. In the light of this factor, the advanced Hill cipher which is applied in developing this cipher is far superior to any other modified Hill cipher. Here the key K is of size 4x4 and it is placed in A whose size is 8x8. As A is participating in all the operations, such as multiplication and permutation of the cipher, the binary bits of K are getting scattered in all the directions of the Ciphertext in each and every round of the iteration process. Thus the strength of the cipher in this analysis has increased significantly. From the above analysis, we conclude that the advanced Hill cipher is a marked advancement in the area of Cryptography.

VI. References

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

[2] V.U.K.Sastry, S.Udaya Kumar, A.Vinaya Babu, " A Large Block Cipher using Modular Arithmetic Inverse of a Key Matrix and Mixing of the Key Matrix and the Plaintext", Journal of Computer Science 2(9),pp.698-703,2006.

[3] V.U.K.Sastry, S.Udaya Kumar, and A.Vinaya Babu, " A Block Cipher Basing upon Permutation, Substitution, and Iteration", Journal of Information Privacy and Security, Vol.3, No.1, 2007.

[4] V.U.K.Sastry, N.Ravi Shankar, "Modified Hill Cipher for a Large Block of Plaintext with Interlacing and Iteration", Journal of Computer Science 4(1), pp.15-20,2008.

[5] V.U.K.Sastry, V.Janaki, "A Modified Hill Cipher with Multiple Keys", International Journal of Computational Science, Vol.2, No.6, pp.815-826, Dec.2008.

[6] Aruna Varanasi, S.Udayakumar, "A Block Cipher using Feistal's Approach Involving Permutation and Mixing of the Plaintext and the Additive Inverse of Key Matrix", Journal of Computer Science, vol.4(2), pp.117-124, 2008.

[7] V.U.K.Sastry, D.S.R.Murthy, S. Durga Bhavani, "A Large Block Cipher Involving a Key Applied on both the Sides of the Plaintext", Vol.2, No.2, pp.10-13, February. 2010.

[8] V.U.K.Sastry, N.Ravi Shankar, S.Durga Bhavani, "A Modified Hill Cipher Involving Interweaving and Iteration", International journal of network security, Vol.11(1), pp.11-16, July 2010.

[9] V.U.K.Sastry, V.Aruna, Dr.S.Udaya Kumar, "A Modified Hill Cipher Involving a Pair of Keys and a Permutation", Vol.2, No.9, pp.105-108, September 2010.

[10] V.U.K.Sastry, D.S.R.Murthy, S.Durga Bhavani, " A Block Cipher Having a Key on One Side of the Plaintext Matrix and its Inverse on the Other Side", International Journal of Computer Theory and Engineering (IJCTE), Vol.2, No.5, Oct.2010.

[11] Sastry, V.U.K., and Janaki, V., " On the Modular Arithmetic Inverse in the Cryptology of Hill Cipher", Proceedings of North American Technology and Business Conference, September 2005, Montreal, Canada.

[12] William H.Press, Brain P.Flannery, Saul A. Teukolsky, William T. Vetterling, "Numerical Recipes in C: The Art of Scientific Computing", Second Edition, Cambridge University Press, pp.36-39,1992.

[13] 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.

[14] mathworld.wolfram.com