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 a Permuted Key and Modular Arithmetic Addition Operation

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 symmetric block cipher by modifying the classical Hill cipher. In this we have made use of iteration process, and introduced a key K_0 obtained by permuting the elements of the original key matrix K. This key K_0 strengthens the cipher, and it does not allow the cipher to be broken by the known plaintext attack. The avalanche effect and the cryptanalysis clearly indicate that the cipher is a strong one. This analysis clearly suggests that the matrix K_0 can be constructed in various other ways.

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

I. INTRODUCTION

The study of Hill cipher [1] has been a fascinating area of research since several years, and it has attracted the attention of several researchers.

The classical Hill cipher is governed by the relations

$$C = (KP) \bmod 26, \text{ and} \quad (1.1)$$

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

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

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

In the equations (1.1) to (1.3), mod 26 is used as the English alphabet contains 26 characters. By including appropriate number of columns of the plaintext and the corresponding columns of the ciphertext, equation (1.1) can be written in the form

$$Y = (KX) \bmod 26, \quad (1.4)$$

where X and Y are matrices whose size is the same as that of the key matrix K. On obtaining the modular arithmetic inverse of X, (1.4) can be written in the form

$$K = (YX^{-1}) \bmod 26. \quad (1.5)$$

This has shown that the classical Hill cipher can be broken by the known plaintext attack.

In the recent years, several modifications [2-13] of the classical Hill cipher have appeared in the literature of Cryptography. In all these block ciphers, wherein iteration, permutation and/or substitution are present, the strength of the cipher is found to be quite significant and the cipher cannot be broken by any cryptanalytic attack.

In the present paper, our objective is to develop a novel block cipher (called modern Hill cipher) wherein the plaintext and the ciphertext are basically governed by the relations.

$$C = (KP + K_0) \bmod N, \quad (1.6)$$

and

$$P = (K^{-1} (C - K_0)) \bmod N, \quad (1.7)$$

where N is any positive integer and K_0 is a permuted form of the key K. This additional K_0, introduced into the cipher, enables us to strengthen the cipher by ruling out the possibility of the known plaintext attack. In this analysis, we have introduced the concept of iteration and the concept of mixing, into the resulting plaintext at every stage of the iteration process, so that the cipher is strengthened by thorough confusion and diffusion.

Now, we mention the outlines of the paper. We have put forth the development of the cipher and presented the algorithms, for encryption and decryption, in section 2. We have illustrated the cipher and examined the avalanche effect in section3. We have analyzed the cryptanalysis in section 4. Finally, we have presented the computations and drawn conclusions, obtained from this analysis, in section 5.

II. 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

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

where 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

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

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

Let K_0 be another key matrix, obtained from K, by permuting the elements of K in a chosen manner.

In view of this fact, we take

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

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,

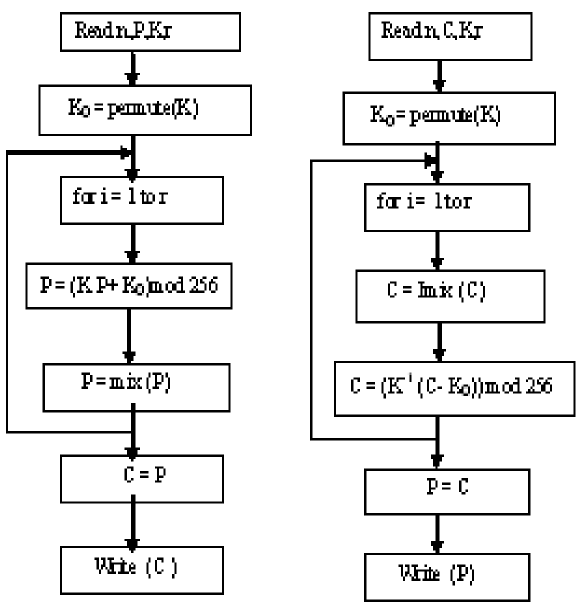
Though, we can adopt any other type of permutation, such as transpose, modular arithmetic inverse, etc., on K , here we have confined our attention only to this permutation, mentioned above.

On adopting the process of encryption we get the ciphertext denoted by C. This is given by the relation

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

in which all the elements of C also lie in [0-255].

The various steps involved in the process of encryption and in the process of decryption are given by the flow charts presented in Figure-1.



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

Figure 1. Schematic diagram of the Cipher

The algorithms for encryption and decryption are written below.

Algorithm for Encryption

1. Read n,P,K,r
2. K_0=permute(K)
3. for i = 1 to r
   {
   P = (K P + K_0) mod 256
   P= mix(P)
   }
   C = P
4. Write(C)

Algorithm for Decryption

1. Read n,C,K,r
2. K^{-1} = Inverse(K)
   K_0=permute(K)
3. for i= 1 to r
   {
   C = Imix(C)
   C= (K^{-1} (C-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 $[A_{ji}]$/ Δ, 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.

Let us now consider the function mix(), utilized in the encryption algorithm. At each stage of the iteration process, the resulting plaintext P is a matrix of size nxn. In this, 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

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

The mixing is carried out by placing 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. Thus we get n^2 decimal numbers, corresponding to the binary bits, and hence we obtain a square matrix of size n.

It may be noted here that the function Imix(), in the process of decryption, denotes the reverse process of the mix().

III. ILLUSTRATION OF THE CIPHER

Consider the plaintext mentioned below:

When rains are pouring and wind is blasting, no scientist and no engineer can come to our rescue. We loose all the crop. Finally politicians come to our doors and they say we are with you. (3.1)

Let us focus our attention on the first sixteen characters of the plaintext (3.1). This is given by

When rains are p. (3.2)

On using EBCDIC code the plaintext (3.2) can be brought to the form of a matrix, P given by

$$P = \begin{bmatrix} 230 & 136 & 133 & 149 \\ 64 & 153 & 129 & 137 \\ 149 & 162 & 64 & 129 \\ 153 & 133 & 64 & 151 \end{bmatrix}. \qquad (3.3)$$

Let us take the key, K in the form

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

On applying the permutation, mentioned earlier in section 2, on the key K, 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 the above K and K_0, and the encryption algorithm, with r=16, we get the ciphertext C corresponding to the plaintext P given in (3.3). Thus we have

$$C = \begin{bmatrix} 40 & 126 & 133 & 76 \\ 157 & 250 & 192 & 121 \\ 192 & 15 & 139 & 253 \\ 148 & 236 & 144 & 195 \end{bmatrix}. \qquad (3.6)$$

On adopting the decryption algorithm, we obtain the original plaintext given by (3.3).

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

To this end we replace the second character 'h' of the plaintext (3.2) by 'i'. The EBCDIC codes of 'h' and 'i' are 136 and 137. These two differ by one bit in their binary form. Thus, on using the modified plaintext (obtained after changing h to i), the key K (3.4), the permuted key K_0 (3.5) and the encryption algorithm, the corresponding ciphertext C can be obtained in the form

$$C = \begin{bmatrix} 136 & 135 & 89 & 202 \\ 174 & 32 & 237 & 128 \\ 101 & 238 & 172 & 134 \\ 139 & 119 & 64 & 54 \end{bmatrix}. \qquad (3.7)$$

On converting (3.6) and (3.7) into their binary form, we find that the two ciphertexts differ by 72 bits (out of 128 bits). This clearly shows that the cipher is markedly a strong one.

Let us now consider a one bit change in the key, K. To achieve this one, we replace the first row third column element "9" of (3.4), by "8". On performing the encryption with the modified key, with the corresponding permuted key K_0, and with the original plaintext intact, we get the ciphertext given by

$$C = \begin{bmatrix} 158 & 167 & 115 & 10 \\ 118 & 23 & 224 & 60 \\ 87 & 199 & 228 & 147 \\ 63 & 240 & 123 & 16 \end{bmatrix}. \qquad (3.8)$$

Now on comparing the binary forms of (3.6) and (3.8), we find that they differ by 73 bits (out of 128 bits). This also shows that the cipher is an excellent 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

In this analysis the key K is consisting of 16 numbers wherein each number can be represented in the form of 8 binary bits. Hence the length of the key is 128 bits and the size of the key space is

$$2^{128} = (2^{10})^{12.8} \approx (10^3)^{12.8} = 10^{38.4}.$$

If the time required for the determination of the plaintext for one value of the key in the key space is taken as 10^{-7} seconds, then the time required for obtaining the plaintext by considering all the possible keys in the key space is

$$\frac{10^{38.4} \times 10^{-7}}{365 \times 24 \times 60 \times 60} = 7965 \times 10^{20} \text{ years}$$

As this number is very large, it is impracticable to break the cipher.

In the case of the known plaintext attack, we know as many pairs of plaintext and ciphertext as we require. Let us now see what happens to the ciphertext C as we confine our attention to different stages of the iteration process, corresponding to r=1, 2, 3,….16, in the encryption process. Thus we have

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

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

..

.

$$C = M((KM((\ldots\ldots M((K\, M((KP + K_0) \bmod 256) + K_0) \bmod 256) \ldots\ldots + K_0) \bmod 256) + K_0) \bmod 256)$$

$$\text{for } r=16. \quad (4.3)$$

In writing the above relations the function mix() is replaced by M() for elegance.
The relation (4.1) can be written in the form

$$\text{Imix}(C) = (KP + K_0) \bmod 256. \quad (4.4)$$

From (4.4), it is apparently seen that this cipher cannot be broken (even when we confine to r=1) as the addition of K_0 do not allow the determination of K in any way. The relation (4.3), obtained at the end of the iteration process, firmly indicates that the cipher is a strong one and it cannot be broken by the known plaintext attack as the elements of the key K are thoroughly mixed in each round of the iteration process.

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

In view of the above discussion, we conclude that the cipher is a potential one.

V. COMPUTATIONS AND CONCLUSIONS

In this paper, we have offered a modification to the Hill cipher in a modern way. The computations in this analysis are carried out by writing programs for encryption and decryption in Java. The ciphertext corresponding to the entire plaintext given by (3.1) is obtained in the form

40	126	133	76	157	250	192	121	192	15	139	253	148	236	144	[illegible]
118	46	55	245	147	189	94	37	220	158	53	38	119	34	249	[illegible]
30	132	86	194	248	21	215	48	83	88	74	32	129	108	41	[illegible]
82	150	113	3	96	193	117	128	65	156	32	13	137	65	198	[illegible]
229	166	103	217	167	118	20	136	31	90	163	241	104	228	246	[illegible]
195	0	13	178	225	254	136	143	110	193	96	230	146	211	220	[illegible]
39	40	232	44	253	224	171	80	165	143	66	208	231	241	102	[illegible]
28	7	164	208	117	148	141	240	157	137	200	168	26	18	36	[illegible]
21	93	183	210	161	211	2	104	23	132	81	173	12	19	132	[illegible]
221	56	254	193	181	180	49	56	155	244	92	50	136	190	232	[illegible]
112	233	117	153	10	15	20	181	142	36	112	41	51	82	199	[illegible]
189	174	180	41	148	64	19	168	23	61	97	188	122	215	23	[illegible]

In obtaining the ciphertext we have divided the plaintext (3.1) into twelve blocks. As the last block is in shortage of four characters, it is supplemented with blank characters.

From the discussion of the avalanche effect and the cryptanalysis, it is interesting to note that this cipher is a very strong one.

Here it may be pointed out that, in the development of the modern Hill cipher, K_0 can be obtained from K in various other forms, such as K^T(transpose of K), K^{-1}(inverse of K), or any other permutation of K.

VI. REFERENCES

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

[2] B.Thilaka and K.Rajalakshmi, " An extension to Hill Cipher Using Generalized Inverses and m^{th} Residue modulo n" Cryptologia 29:4, pp.367-376, Oct 2005.

[3] V.U.K.Sastry, S.Udaya Kumar, and A.Vinaya Babu, " A Large Block Cipher Using an Iterative Method and the Modular Arithmetic Inverse of a Key Matrix",IAENG International Journal of Computer Science, Vol.32, No.4,pp.395-401, 2006.

[4] 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.

[5] V.U.K.Sastry, S.Udaya Kumar, and A.Vinaya Babu, " A Block Cipher Involving Interlacing and Decomposition", Journal of Information Technology, Vol.6, No.3,pp. 396-404, 2007.

[6] 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.

[7] 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.

[8] V.U.K.Sastry, D.S.R.Murthy, S. Durga Bhavani, "A Block Cipher Involving a Key Applied on both the Sides of the Plaintext", International journal of computer and network security (IJCNS), Vol.1, No.1, pp.27-30, October. 2009.

[9] 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 as a Multiplicant", International journal of computer and network security (IJCNS), Vol.2, No.2, pp.10-13, February. 2010.

[10] 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.

[11] V.U.K.Sastry, Aruna Varanasi, Dr.S.Udaya Kumar, "A Modified Hill Cipher Involving a Pair of Keys and a Permutation", International journal of computer and network security (IJCNS),Vol.2,No.9, pp.105-108, September 2010.

[12] 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.

[13] V.U.K.Sastry, Aruna Varanasi,"A Modified Hill Cipher Involving Permutation, Iteration and the Key in a Specified Position", International journal of computer and network security (IJCNS),Vol.2,No.10, pp.157-162-108, 2010.