Volume 2, No. 3, May-June 2011
ISSN No. 0976-5697
International Journal of Advanced Research in Computer Science
RESEARCH PAPER
Available Online at www.ijarcs.info

A Modern Hill Cipher Involving a Pair of Keys, Modular Arithmetic Addition and Substitution

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

V. U. K. Sastry
Department of computer Science and Engineering,SNIST
Hyderabad, India,
vuksastry@rediffmail.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 involves a pair of keys. Here we have used iteration process which includes functions mix() and substitute() in each round of the iteration process. Function mix() is used for mixing the binary bits of the plaintext, and substitute() is employed for modifying the plaintext. The avalanche effect and the cryptanalysis carried out in this investigation indicate that this cipher cannot be broken by easy means and it is a strong one.

Keywords: symmetric block cipher, cryptanalysis, avalanche effect, ciphertext, pair of keys, modular arithmetic addition, mixing, substitution.

I. INTRODUCTION

The recent literature of the Cryptography is replete with a number of modifications of the Hill cipher [1-8]. In all these investigations the strength of the cipher is achieved by introducing iteration, and some sort of mechanisms such as permutation, mixing and interlacing of the plaintext characters and the key, in order to have confusion and diffusion in the development of the cipher.

The basic draw back of the classical Hill cipher is it can be broken by the known plaintext attack. This weakness was overcome by many authors in many ways. In a recent investigation, we [9-10] have developed a cipher called modern Hill cipher by including a modified key, in addition to the usual key. In [9], we have introduced the modified key by using modular arithmetic addition operation, while in [10], we have made use of XOR operation. In both these papers, we have carried out cryptanalysis and concluded that the strength of the cipher is significant.

In the present investigation, our objective is to develop a new type of Hill cipher. Here we use a pair of keys, wherein one key (K) is used as a multiplicant (as in the classical Hill cipher), and the other key (L) is included by using modular arithmetic addition operation. The basic equations governing the cipher are given by

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

and

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

where N is any positive integer, and K^{-1} is the modular arithmetic inverse of K. In this analysis, besides the usual iteration and mixing processes, we use a substitution process wherein the substitution table includes both the keys K and L. The keys involved in this analysis, and the processes mixing and substitution are expected to strengthen the cipher considerably (by overcoming all possible attacks in cryptography) as the cipher is subjected to strong diffusion and confusion.

Now, we mention the outlines of the paper. In section 2, we have put forth the development of the cipher and presented the algorithms, for encryption and decryption. In section 3, we have illustrated the cipher by giving a suitable example.

Further, here we have discussed the avalanche effect. Then in section 4, we have devoted our attention to cryptanalysis. Finally in section 5, we have presented the computations, and drawn conclusions obtained from this analysis.

II. DEVELOPMENT OF THE CIPHER

Consider a plaintext, P. On using EBCDIC code, P can be written in the form of a matrix given by

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

Let us take a pair of keys K and L, which can be represented in the form of matrices. Let

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

and

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

Here each element of the matrices P, K and L is a decimal number in the interval [0,255].

On adopting the process of encryption, we get the ciphertext C. This can be represented in the form

$$C = [C_{ij}], \quad i = 1 \text{ to } n, \ j = 1 \text{ to } n, \qquad (2.4)$$

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 Fig.1.

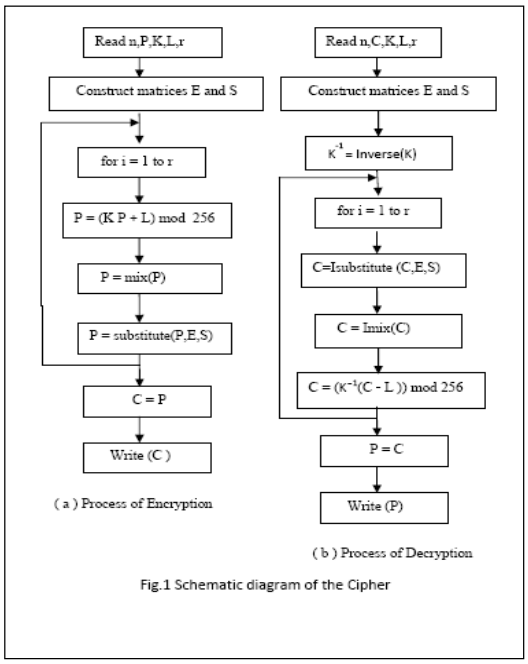

Fig.1 Schematic diagram of the Cipher

Figure 1: Schematic diagram of the cipher

The algorithms for encryption and decryption are written below.

Algorithm for Encryption

1. Read n,P,K,L,r
2. for i = 1 to 16
   {
   for j = 1 to 16
   {
   E(i,j) =16(i-1)+(j-1)
   }
   }
3. S= Table(E,K,L)
4. for i = 1 to r
   {
   P = (K P + L) mod 256
   P= mix(P)
   P=substitute(P,E,S)
   }
   C = P
5. Write(C)

Algorithm for Decryption

1. Read n,C,K,L,r
2. for i = 1 to 16
   {
   for j = 1 to 16
   {
   E(i,j) =16(i-1)+(j-1)
   }
   }

3. S= Table(E,K,L)
4. K^{-1} = Inverse(K)

5. for i = 1 to r
   {

   C= Isubstitute(C,E,S)
   C = Imix(C)
   C= (K^{-1} (C - L))mod 256

   }
   P = C
6. 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 $\Delta \neq 0$.
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.

Let us now discuss the functions mix() and substitute() which are used in the encryption algorithm.
In the function mix(), at each stage of the iteration process, the resulting plaintext P is a square matrix of size n. In this matrix, 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 can be divided into four substrings wherein each one is of size $2n^2$ binary bits. These strings can be written in the form

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

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

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

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

The mixing is carried out by arranging the binary bits of the different substrings as shown below:

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

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 get a square matrix of size n.

Let us now deal with the process of substitution. In the EBCDIC code, characters are represented by the numbers 0-255. These numbers can be represented by a matrix E in the form

E (i , j) = 16(i-1)+(j-1), i=1 to 16 and j=1 to 16. (2.5)

In the development of the substitution table consisting of 16 rows and 16 columns, the first two rows of the table are filled with the elements of the keys K and L in order. The subsequent rows of the table are filled with the remaining elements of E (excluding the elements occurring in K and L). Thus we get the substitution table, which can be visualized as the matrix S(i,j), i=1 to 16, j=1 to 16.

In order to have a clear insight into the substitution process, let us consider a plaintext. Let it be transformed (see encryption algorithm in section 2) by using the relations

P = (KP+L) mod 256 (2.6)

and

P = mix(P). (2.7)

Now the resulting plaintext contains a set of numbers. On using the substitution matrix S, each one of these numbers is to be replaced by the corresponding number. If the number in the resulting plaintext is E(i,j), it is to be replaced by S(i,j).

For a clear cut idea of the substitution process, let us consider a simple example. After applying the relations (2.6) and (2.7) on the plaintext P, let one of the decimal numbers in the resulting plaintext be 50, which can be readily seen as E(4,3). This number is to be replaced by S(4,3), that is, 50 is to be replaced by 26 (see the substitution table given in section 3). In the same manner substitution can be carried out for all the other numbers present in the resulting plaintext.

As it is seen in the algorithm the substitution process is carried out by using the substitution matrix S in each round of the iteration process.

It may be noted here that the function Imix() and Isubstitute(), in the process of decryption, can readily be obtained by reversing the processes of mix() and substitute().

III. ILLUSTRATION OF THE CIPHER

Consider the plaintext mentioned below:

My father worked as a servant in the field of a landlord. My grand father also worked in the same field. My father was a drunkard and my grand father too. We were not allowed to enter into any temple. What shall I do! Now I am working as a terrorist, day and night, for the betterment of the society. (3.1)

Let us consider the first sixteen characters of the plaintext (3.1). This is given by

My father worked (3.2)

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

$$P = \begin{bmatrix} 212 & 168 & 64 & 134 \\ 129 & 163 & 136 & 133 \\ 153 & 64 & 166 & 150 \\ 153 & 146 & 133 & 132 \end{bmatrix} \quad (3.3)$$

Let us take the keys, K and L in the form

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

and

$$L = \begin{bmatrix} 102 & 21 & 33 & 45 \\ 117 & 121 & 89 & 97 \\ 79 & 49 & 53 & 23 \\ 10 & 133 & 254 & 237 \end{bmatrix} \quad (3.5)$$

On using (2.5), (3.4), and (3.5), and adopting the procedure, for the creation of the substitution table, mentioned in section2, we get the substitution table as shown in Table 1.

On using (3.3) to (3.5), substitution matrix S, and the encryption algorithm with r=16, we get the ciphertext C

$$\begin{bmatrix} 95 & 118 & 109 & 143 \\ 58 & 186 & 79 & 26 \\ 226 & 66 & 184 & 109 \\ 190 & 96 & 5 & 92 \end{bmatrix}. \quad (3.6)$$

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

Let us now discuss the avalanche effect, which gives a measure for the strength of the cipher.

To this end, we replace the sixteenth character ‘d’ of the plaintext (3.2) by ‘e’. The EBCDIC codes of ‘d’ and ‘e’ are 132 and 133. These two differ by one bit in their binary form. Thus, on using the modified plaintext (obtained after changing d to e), the keys K and L given by (3.4) and (3.5), the substitution matrix S, and the encryption algorithm, the corresponding ciphertext C can be obtained in the form

$$C = \begin{bmatrix} 138 & 26 & 126 & 48 \\ 3 & 180 & 147 & 171 \\ 191 & 183 & 7 & 14 \\ 16 & 153 & 41 & 238 \end{bmatrix}. \quad (3.7)$$

On converting (3.6) and (3.7) into their binary form, we find that the two ciphertexts differ by 75 bits (out of 128 bits). This clearly shows that the cipher is a strong one.

Let us now consider a one bit change in one of the keys, say key, K. To this end, we replace the first row first column element “123” of (3.4), by “122”. On performing the encryption with the modified key K, with the original plaintext P, the corresponding substitution matrix S, keeping the other key L intact, we get the ciphertext given by

$$C = \begin{bmatrix} 236 & 155 & 222 & 73 \\ 99 & 85 & 13 & 255 \\ 3 & 234 & 218 & 28 \\ 97 & 250 & 93 & 83 \end{bmatrix}. \quad (3.8)$$

Now on comparing the binary strings corresponding to (3.6) and (3.8), we find that they differ by 70 bits (out of 128 bits). This also shows that the cipher is a potential one.

123	25	9	67	134	17	20	11	48	199	209	75	39	55	85	92
102	21	33	45	117	121	89	97	79	49	53	23	10	133	254	237
0	1	2	3	4	5	6	7	8	12	13	14	15	16	18	19
22	24	26	27	28	29	30	31	32	34	35	36	37	38	40	41
42	43	44	46	47	50	51	52	54	56	57	58	59	60	61	62
63	64	65	66	68	69	70	71	72	73	74	76	77	78	80	81
82	83	84	86	87	88	90	91	93	94	95	96	98	99	100	101
103	104	105	106	107	108	109	110	111	112	113	114	115	116	118	119
120	122	124	125	126	127	128	129	130	131	132	135	136	137	138	139
140	141	142	143	144	145	146	147	148	149	150	151	152	153	154	155
156	157	158	159	160	161	162	163	164	165	166	167	168	169	170	171
172	173	174	175	176	177	178	179	180	181	182	183	184	185	186	187
188	189	190	191	192	193	194	195	196	197	198	200	201	202	203	204
205	206	207	208	210	211	212	213	214	215	216	217	218	219	220	221
222	223	224	225	226	227	228	229	230	231	232	233	234	235	236	238
239	240	241	242	243	244	245	246	247	248	249	250	251	252	253	255

Table 1: Substitution Table.

IV. CRYPTANALYSIS

The general well known attacks which are available in the literature for breaking the cipher are

1. Ciphertext only attack (Brute force attack)
2. Known plaintext attack
3) Chosen plaintext attack and
4) Chosen ciphertext attack

Let us consider the ciphertext only attack. In this analysis the keys K and L are consisting of 16 numbers each.

time required for breaking the cipher with all possible values of the keys in the key space is

$$\frac{10^{76.8} \times 10^{-7}}{365 \times 24 \times 60 \times 60} = 31.71 \times 10^{60.8} \, years$$

As this number is very large, it is impossible to break the cipher by the brute force attack.

In the case of the known plaintext attack, we know as many pairs of plaintext and ciphertext as we require. On using the different steps in the encryption algorithm, at the end of the sixteenth iteration, we get the ciphertext C. This can be written in the form

95	118	109	143	58	186	79	26	226	66	184	109	190	96	5	92
102	22	50	163	79	14	35	18	118	94	170	61	13	237	187	18
180	85	241	68	241	67	234	102	204	69	182	22	207	140	253	219
21	96	14	85	211	212	199	70	111	98	92	16	91	242	186	122
213	76	119	72	24	171	50	245	91	41	219	241	2	124	227	95
84	211	252	200	61	86	228	211	252	54	204	23	37	235	228	80
78	8	180	56	31	145	15	142	249	215	113	141	202	58	153	68
135	184	7	168	110	109	177	102	7	230	180	48	36	37	131	242
180	78	159	112	48	160	188	149	175	118	176	36	7	17	50	114
207	252	220	182	237	71	16	38	58	124	62	118	102	99	161	159
204	159	157	37	2	221	233	73	141	49	203	208	130	203	110	111
30	147	249	84	81	174	17	79	253	172	149	131	168	23	132	165
19	60	207	18	133	28	77	27	251	24	33	190	41	33	245	41
138	177	242	250	237	13	199	38	70	112	90	156	192	199	61	47
134	55	58	255	162	200	177	171	205	39	122	243	17	249	207	202
191	220	237	7	105	209	174	146	189	80	138	247	196	44	103	78
160	105	146	99	56	134	173	170	150	198	188	159	197	179	147	47
228	19	235	243	168	109	7	184	175	102	182	59	50	155	229	39
78	90	186	77	124	43	187	170	32	52	94	161	52	103	211	32

It is worth exploring the cryptanalysis concerned to the last two attacks (attacks 3 and 4). However, the analysis in these two cases is expected to be quite involved [11-12].

In the light of the above facts, we conclude that this cipher cannot be broken by easy means, and it is some what a strong one.

V. COMPUTATIONS AND CONCLUSIONS

In this paper, we have developed a block cipher which includes a pair of keys and modular arithmetic addition. This cipher is supported by the functions mix () and substitute (). 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

In obtaining the ciphertext we have divided the plaintext (3.1) into 19 blocks. As the last block is in shortage of 4 characters, it is supplemented with 4 blank characters.

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

The substitution table used in this analysis can be developed in various other ways. For example, we can fill up the first two columns of the table (instead of the first two rows) by the elements of the keys, K and L. It can also be formed by filling up the diagonals with the elements of K and L. Some work is already in progress with this sort of substitution tables.

Finally we conclude that this block cipher is an interesting one and it can be applied for the security of information.

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, Aruna Varanasi. S. Udaya Kumar, "A Modern Hill cipher Involving Permuted Key and Modular Arithmetic Addition Operation", International Journal of Advanced Research in Computer Science (IJARCS), Vol.2, No.1, pp.162-165, Jan-Feb 2011.

[10]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 (IJARCS), Vol.2, No.1, pp.153-155, Jan-Feb 2011.

[11] Biham, E., and Shamir, A. Differential Cryptanalysis of the Data Encryption Standard. New York: Springer-Verlag, 1993.

[12] Matsui, M. " Linear Cryptanalysis Method for DES Cipher", Proceedings, EUROCRYPT'93,1993: New York- Springer-Verlag.