Volume 2, No. 5, May 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 PAIR OF KEYS, MODULAR ARITHMETIC ADDITION AND SUBSTITUTION

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

[1]Department of computer Science and Engineering,SNIST
Hyderabad, India,
varanasi.aruna2002@gmail.com
[*2]Department of computer Science and Engineering,SNIST
Hyderabad, India,
vuksastry@rediffmail.com
[3]Department of computer Science and Engineering,SNIST
Hyderabad, India,
uksusarla@rediffmail.com

Abstract: In this investigation, we have developed a symmetric block cipher which includes iteration process, a pair of keys, modular arithmetic addition, mixing and substitution. The mixing and substitution used in each round of the iteration is strengthening the cipher significantly. The avalanche effect and cryptanalysis carried out in this analysis clearly indicate that the strength of the cipher is considerable and it can be fairly used for the security of information.
Keywords: symmetric block cipher, cryptanalysis, avalanche effect, ciphertext, pair of keys, involutory matrix, modular arithmetic addition, mixing, substitution.

INTRODUCTION

In the recent years the study of the advanced Hill cipher [1], a variant of the classical Hill cipher, has become a popular topic of research. In this, the arithmetic inverse of a matrix is the same as the matrix itself. This sort of matrix is said to be an involutory matrix. In view of this fact, it has become unnecessary to find the modular arithmetic inverse of the key matrix which is inevitably required in the development of the Hill cipher. In our recent investigation, we have studied several aspects of the advanced Hill cipher [2-7] by including several aspects such as iteration, permutation, pair of keys, modular arithmetic addition, mixing and XOR operation. In all these analyses, we have found that the strength of the cipher is significant.

The basic relations governing the advanced Hill cipher are as follows:

$$A^{-1}= A, \qquad (1.1)$$

and

$$(A\,A^{-1}) \bmod N = I. \qquad (1.2)$$

where A is a square matrix of size n, A^{-1} is the arithmetic inverse of A, and N is any non zero positive integer chosen appropriately.
From (1.1) and (1.2) we get

$$A^2 \bmod N = I, \qquad (1.3)$$

in which I is the identity matrix.
From (1.3), the matrix A can be obtained by writing it in the form

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

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

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

$$A_{22} = - K, \qquad (1.5)$$

$$A_{12}=[d(I- K)] \bmod N, \qquad (1.6)$$

$$A_{21}=[\lambda(I+ K)] \bmod N, \qquad (1.7)$$

$$\text{where } (d\lambda) \bmod N =1, \qquad (1.8)$$

in which d is a chosen positive integer and λ is determined from (1.8). In order to have a detailed discussion related to obtaining A, we refer to [2].

The advanced Hill cipher [2] is governed by the relations

$$C= (A\,P) \bmod N, \qquad (1.9)$$

and

$$P = (A\,C) \bmod N. \qquad (1.10)$$

In the present investigation, our objective is to develop a modern advanced Hill cipher which includes a pair of keys K and L.

This cipher which we are going to develop here is governed by the basic relations

$$C = (AP+B) \bmod N, \qquad (1.11)$$

and

$$P = (A(C-B)) \bmod N \qquad (1.12)$$

where A and B are the involutory matrices, which include Keys K and L respectively.

Here A is governed by the relations (1.4) - (1.8), and B is to be obtained by using the relations which are similar to (1.4) - (1.8). Thus we take

© JGRCS 2011, All Rights Reserved

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

B_{11}=L, (1.14)
B_{22} = - L, (1.15)
B_{12}=[e(I- K)] mod N, (1.16)
B_{21}=[λ(I+ K)] mod N, (1.17)
where (eλ) mod N =1, (1.18)

in which e is a chosen positive integer constant, and the λ is determined from (1.18).

In this analysis, we use iteration process, modular arithmetic addition and mixing. In addition to these operations, we make use of a substitution process, which involves the keys K and L.

Now let us state briefly the plan of the paper. In section 2, we have discussed the development of the cipher, and depicted the flow charts and algorithms for the encryption and the decryption. In section 3, we have illustrated the cipher with a suitable example, and studied the avalanche effect. Then we have carried out the cryptanalysis in section 4. Finally in section 5, we have dealt with computations and conclusions.

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}], 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 in [0,255].
Let us take a pair of key matrices K and L, which can be represented in the form
K = [K_{ij}], i=1 to n/2, j=1 to n/2, (2.2)
L = [L_{ij}], i=1 to n/2, j=1 to n/2, (2.3)
where each element of K and L is also a decimal number in the interval [0,255].
On using (1.4) - (1.8), (1.13) - (1.18), taking the key matrices K and L, and the constants d and e, we get the involutory matrices A and B. Then the ciphertext C can be written in the form
C = (AP+B) mod N, (2.4)
where N= 256.
Here we take C = [C_{ij}], i= 1 to n, j=1 to n.
wherein, all the elements of C are in [0,255].

The flow charts describing the cipher are given in Fig.1

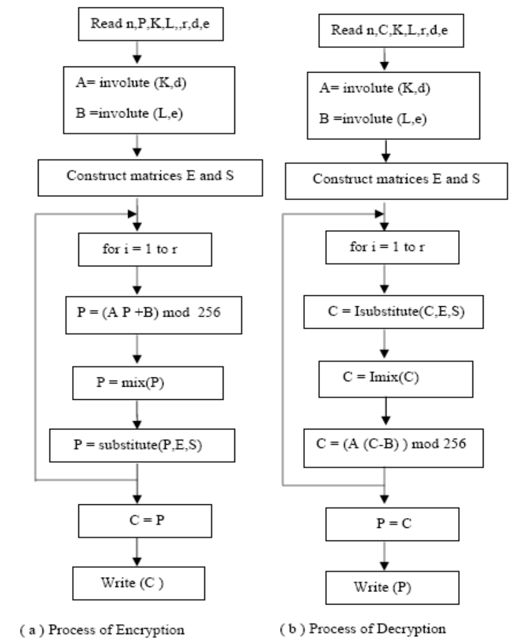

Fig.1 Schematic diagram of the Cipher

In this, the function involute() includes the procedure (see section 2) for obtaining the involutory matrix. Here, we have included iteration process, and the functions mix() and substitute() in each round of the iteration process. With these operations, we achieve thorough confusion and diffusion in arriving at the ciphertext.. The functions Imix() and Isubstitute() represent the reverse processes of mix() and substitute() respectively. The detailed discussion of the functions mix() and the substitute() are given later.

The algorithms for encryption and decryption are as follows.

© JGRCS 2011, All Rights Reserved

Algorithm for Encryption

1. Read n,P,K,L,r,d,e
2. A = involute(K,d)
   B = involute(L,e)
3. Construct matrices E, S
4. for i = 1 to r
   {
   P = (A P + B) 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,d,e
2. A = involute(K,d)
   B = involute (L,e)
3. Construct matrices E,S
4. for i= 1 to r
   {
   C = Isubstitute(C,E,S)
   C = Imix(C)
   C= (A (C-B))mod 256
   }
   P = C
5. Write (P)

In the above algorithms 'r' indicates the number of rounds. In this analysis we take r=16.

Let us now consider the development of the mix() function. In the encryption algorithm, at each stage of the iteration process, as the plaintext matrix P is of size nxn, it can be written in the form of four binary strings, wherein each string has $2n^2$ binary bits as shown below:

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

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

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

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

These strings can be mixed by writing them in the form of a single string given 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.

Let us now introduce the process of substitution. In the EBCDIC code, we require the numbers 0-255 for the representation of the characters. These numbers can be represented by a matrix E in the form

$$E(i, j) = 16(i-1)+(j-1), \quad i=1 \text{ to } 16 \text{ and } j=1 \text{ to } 16. \qquad (2.5)$$

Consider the development of the substitution table consisting of 16 rows and 16 columns. Let us fill up the first two rows of the table with the elements of the keys K and L in order. Let the subsequent rows of this table be filled with the remaining elements of E (excluding the elements occurring in K and L) in order. Thus we get the substitution table. This can be represented in the form of a matrix called 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 P. Let us transform this P by applying the relations

$$P = (AP+B) \bmod 256, \qquad (2.6)$$

and

$$P = mix(P), \qquad (2.7)$$

which are present in the encryption algorithm.

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

For a clear insight in to 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 21 (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.

ILLUSTRATION OF THE CIPHER

Let us consider the plaintext given below:

" Hello friend! I have come to India. I have seen several election campaigns. Each one is very interesting. All the parties are floating voters in money and liquor. Though winning is unknown, each party strives to play a wonderful role by blaming the other parties and pointing out that the leaders of the other party are unethical. Only GOD knows how the country is moving and how the people are progressing. " (3.1)

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

" Hello friend! I have come to India. I have seen several election" (3.2)

On applying the EBCDIC code, the above plaintext can be written in the form

© JGRCS 2011, All Rights Reserved

Volume 2, No. 5, May 2011
Journal of Global Research in Computer Science
ISSN-2229-371X
RESEARCH PAPER
Available Online at www.jgrcs.info

$$P = \begin{bmatrix} 200 & 133 & 147 & 147 & 150 & 64 & 134 & 153 \\ 137 & 133 & 149 & 132 & 79 & 64 & 201 & 64 \\ 136 & 129 & 165 & 133 & 64 & 131 & 150 & 148 \\ 133 & 64 & 163 & 150 & 64 & 201 & 149 & 132 \\ 137 & 129 & 75 & 64 & 201 & 64 & 136 & 129 \\ 165 & 133 & 64 & 162 & 133 & 133 & 149 & 64 \\ 162 & 133 & 165 & 133 & 153 & 129 & 147 & 64 \\ 133 & 147 & 133 & 131 & 163 & 137 & 150 & 149 \end{bmatrix} \qquad (3.3)$$

Let us take the pair of keys K and L in the form

$$K = \begin{bmatrix} 69 & 124 & 27 & 167 \\ 135 & 79 & 99 & 111 \\ 248 & 199 & 209 & 75 \\ 239 & 45 & 255 & 92 \end{bmatrix}. \qquad (3.4)$$

and

$$L = \begin{bmatrix} 215 & 113 & 19 & 147 \\ 223 & 109 & 254 & 12 \\ 56 & 1 & 127 & 174 \\ 59 & 146 & 189 & 81 \end{bmatrix}. \qquad (3.5)$$

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

$$A = \begin{bmatrix} 69 & 124 & 27 & 167 & 180 & 12 & 143 & 107 \\ 135 & 79 & 99 & 111 & 203 & 214 & 183 & 19 \\ 248 & 199 & 209 & 75 & 24 & 11 & 144 & 255 \\ 239 & 45 & 255 & 92 & 147 & 153 & 99 & 207 \\ 130 & 84 & 233 & 237 & 187 & 132 & 229 & 89 \\ 141 & 112 & 1 & 133 & 121 & 177 & 157 & 145 \\ 168 & 77 & 134 & 249 & \text{C =} & 57 & 47 & 181 \\ 5 & 47 & 181 & 63 & [illegible] & 211 & 1 & 164 \end{bmatrix} \qquad (3.6)$$

Now, on using the relations (1.13) - (1.18) and taking e=189, we have

© JGRCS 2011, All Rights Reserved

$$B = \begin{bmatrix} 215 & 113 & 19 & 147 & 2 & 147 & 249 & 121 \\ 223 & 109 & 254 & 12 & 93 & 68 & 122 & 36 \\ 56 & 1 & 127 & 174 & 168 & 67 & 250 & 138 \\ 59 & 146 & 18[illegible] & [illegible] & 113 & 54 & 119 & 240 \\ 184 & 197 & 15 & 14[illegible] & 41 & 143 & 237 & 109 \\ 203 & 6 & 214 & 252 & 33 & 147 & 2 & 244 \\ 152 & 149 & 128 & 70 & 200 & 255 & 129 & 82 \\ 87 & 250 & 1 & 186 & 197 & 110 & 67 & 175 \end{bmatrix} \quad (3.7)$$

On using the ideas (given in section 2) concerned to the development of the substitution table, we get the substitution table in the form

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

encryption algorithm, we get the ciphertext C in the form

$$\begin{bmatrix} 92 & 96 & 204 & 13 & 123 & 241 & 190 & 134 \\ 172 & 151 & 117 & 86 & 178 & 206 & 43 & 108 \\ 19 & 117 & 157 & 23 & 137 & 110 & 178 & 99 \\ 125 & 99 & [illegible] & [illegible]1 & 227 & 192 & 202 & 32 \\ 168 & 172 & 58 & 106 & 7 & 238 & 103 & 207 \\ 223 & 55 & 206 & 242 & 202 & 255 & 66 & 251 \\ 87 & 9 & 68 & 76 & 140 & 154 & 100 & 3 \\ 71 & 73 & 192 & 209 & 140 & 240 & 115 & 179 \end{bmatrix} \quad (3.8)$$

© JGRCS 2011, All Rights Reserved

Now on applying the decryption algorithm, with the required inputs, we get back the original plaintext given by (3.3).

Let us now consider the avalanche effect, which throws light on the strength of the cipher.

To this end, firstly we replace the 23rd character 'o' of the plaintext (3.2) by 'p'. The EBCDIC codes of 'o' and 'p' are 150 and 151. Here we notice that these two numbers differ by one bit in their binary form. On using the modified plaintext, which is currently obtained, and the other inputs required for carrying out the encryption. We have

$$C = \begin{bmatrix} 115 & 111 & 229 & 80 & 92 & 167 & 39 & 106 \\ 14 & 121 & 203 & 0 & 246 & 88 & 51 & 171 \\ 96 & 188 & 124 & 97 & 231 & 219 & 196 & 125 \\ 233 & 129 & 188 & 30 & 144 & 87 & 175 & 32 \\ 39 & 155 & 215 & 61 & 255 & 11 & 61 & 118 \\ 115 & 7 & 54 & 66 & 230 & 16 & 171 & 88 \\ 117 & 70 & 25 & 115 & 166 & 115 & 167 & 99 \\ 148 & 178 & 141 & 163 & 82 & 34 & 31 & 106 \end{bmatrix} \qquad (3.8)$$

On comparing (3.8) and (3.9), in their binary form, we find that the two ciphertexts differ by 275 binary bits (out of 512 bits). This shows that the cipher is a strong one.

Let us now consider a one bit change in one of the pair of keys, say key K. In order to have this one, we replace the 2nd row 4th column element "111" of (3.4), by "110". After obtaining the corresponding A (keeping the B intact), we carry out the encryption by using the original plaintext. Thus we get the ciphertext in the form

$$C = \begin{bmatrix} 111 & 132 & 63 & 85 & 160 & 107 & 197 & 43 \\ 126 & 94 & 190 & 119 & 249 & 13 & 52 & 133 \\ 90 & 160 & 227 & 8 & 237 & 103 & 102 & 143 \\ 47 & 80 & 26 & 60 & 167 & 245 & 183 & 81 \\ 3 & 117 & 124 & 217 & 86 & 215 & 125 & 116 \\ 178 & 148 & 187 & 135 & 157 & 127 & 69 & 239 \\ 188 & 184 & 129 & 207 & 141 & 255 & 190 & 74 \\ 241 & 255 & 141 & 204 & 93 & 159 & 42 & 200 \end{bmatrix} \qquad (3.9)$$

Now on comparing (3.7) and (3.9), in their binary form, we find that they differ by 268 bits (out of 512 bits). This also clearly indicates that the cipher is a potential one.

CRYPTANALYSIS

The conventional attacks which are used 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.

Let us now consider, firstly, the brute force attack. In this analysis the pair of keys K and L, given by (3.4) and (3.5), both put together, are consisting of 32 decimal numbers. In addition to these two keys, we have used two integers, namely 'd' and 'e' (chosen in the development of the involutory matrices, A and B), which can also be considered as additional keys. Thus, the length of all the keys put together is 34 decimal numbers, wherein each number can be represented in the form of 8 binary bits. Thus the size of the key (involving all the keys) is 272 binary bits. Hence the size of the key space is

$$2^{272} = (2^{10})^{27 \cdot 2} \approx (10^3)^{27 \cdot 2} = 10^{81.6}.$$

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 required for the execution of the cipher with all the possible keys in the key space is

$$\frac{10^{81.6} \times 10^{-7}}{365 \times 24 \times 60 \times 60} = 3.171 \times 10^{66.6} \text{ years}$$

As this number is a very large one, it is simply impractical to break this 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, pair of keys, mixing, substitution and modular arithmetic addition operation, by the time we reach the final stage of the iteration process, the relation that we have between the plaintext and the ciphertext can be seen in the form

$$C = \Psi (M((A\Psi (M((\ldots\ldots \Psi (M((A \Psi (M((AP + B) \bmod 256)) + B) \bmod 256)) \ldots\ldots) \bmod 256)) + B) \bmod 256)). \qquad (4.1)$$

In writing (4.1), the function mix() is replaced by M(), and the substitution process carried out by the function substitute(), is represented by Ψ (). This representation is done for the sake of elegance. Here we notice that (4.1) can never be written in the form

$$C = F(K,L,M,\Psi)\, P$$

where F is a function, depending upon K,L,M and Ψ.

Thus, as (4.1) is a complicated relation, we cannot determine P or a function of P in terms of the other quantities. Hence, unlike in the case of classical Hill cipher, this cipher cannot be broken by the known plaintext attack.

With all effort, basing upon intuition, we do not find any scope for the chosen plaintext attack or for the chosen ciphertext attack for breaking this cipher.

© JGRCS 2011, All Rights Reserved

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

COMPUTATIONS AND CONCLUSIONS

In this paper, we have developed a block cipher, called modern advanced Hill cipher, with a pair of keys. In this we have introduced iteration, modular arithmetic addition, mixing and substitution for transforming the plaintext before it becomes the ciphertext.

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

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

In obtaining this ciphertext, we have divided the plaintext (3.1) into 7 blocks. However, in the last block, as we have only 23 characters, we have added 41 blank characters to make it a complete block consisting of 64 characters.

From the avalanche effect and the cryptanalysis carried out in this investigation, it is worth noticing that this block cipher is expected to be a strong one, and it is quite comparable with any other block cipher in the literature.

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, May 2009.

© JGRCS 2011, All Rights Reserved

[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, and S.Udaya Kumar, " A Modern Advanced Hill cipher Involving a Permuted Key and Modular Arithmetic Addition Operation", Journal of Global Research in Computer Science, Vol.2 No.4, pp. 92-97 , April 2011.

[7] V.U.K.Sastry, Aruna Varanasi, and S.Udaya Kumar, " A Modern Advanced Hill cipher Involving XOR Operation and a Permuted Key ", Journal of Global Research in Computer Science, Vol.2 No.4, pp. 98-102 , April 2011.

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.

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.

© JGRCS 2011, All Rights Reserved