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

A Large Block Cipher Having a Key on One Side of the Plain Text Matrix and its Inverse on the Other Side as Multiplicants

Dr. V. Umakanta Sastry*
Department of Computer Science and Engineering
SreeNidhi Institute of Science and Technology
Hyderabad – 501 301, Andhra Pradesh, India
vuksastry@rediffmail.com

D. S. R. Murthy
Department of Information Technology
SreeNidhi Institute of Science and Technology
Hyderabad – 501 301, Andhra Pradesh, India
dsrmurthy@sreenidhi.edu.in

Dr. S. Durga Bhavani
School of Information technology
Jawaharlal Nehru Technological University Hyderabad (JNTUH)
Hyderabad – 500 085, Andhra Pradesh, India
sdurga.bhavani@gmail.com

Abstract: In this paper, we have developed a large block cipher, by modifying the Hill cipher, by multiplying the plain text P with the key K one side and the modular arithmetic inverse K^{-1} on the other side. Here, the size of the key is 512 bits and the size of the plain text is 2048bits. From the cryptanalysis and the avalanche effect studied on this paper, we have seen that the cipher is a very strong one and it cannot be broken by any cryptanalytic attack.

Keywords: Block cipher, Key, Modular arithmetic inverse, Encryption, Decryption.

I. INTRODUCTION

In a recent investigation, we have modified the Hill cipher [1] and developed a large block cipher [2], in which the plain text block is of length 2048 bits and the key length is 512 bits. In this analysis, the cipher depends upon an iterative scheme, which includes the relations: (1) P = K P K mod 256, (2) P = Mix (P), (3) P = P ⊕ K. These are followed by C = P. Here, P is the plain text, K the key, ⊕ the XOR operation and Mix is a function, which mixes the modified plain text at every stage of the iteration. From the cryptanalysis carried out in this paper, we have seen that the cipher is a strong one, and it cannot be broken by any cryptanalytic attack.

In the present paper, our objective is to develop another large block cipher wherein the plain text block size is 2048 bits and the key size is 512 bits. In the previous paper, we have included K in encryption and K^{-1} in decryption, while in the present analysis, we would like to use, both K and K^{-1} (one on the left side and another on the right side of the plain text matrix) in encryption as well as in decryption. As in [2], here also we have made use of Mix ( ) function and applied the XOR operation between the plain text matrix and the key matrix. In section 2, we have presented the development of the cipher. We have illustrated the cipher in two different cases, and discussed the avalanche effect in section 3. We have carried out the cryptanalysis in section 4. Finally, we have arrived at the conclusions in section 5.

II. DEVELOPMENT OF A PROCEDURE FOR THE CRYPTOGRAPHY OF A GRAY LEVEL IMAGE

Consider a plain text P which can be represented in the form of a square matrix given by

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

where each P_{ij} is lies in [0, 255].

Let us choose a key k. Let it be represented in the form of a matrix given by

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

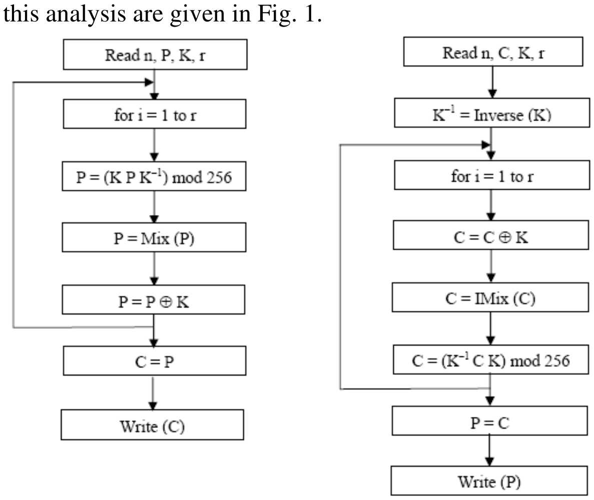
where each K_{ij} is an integer, which lies between 0 and 255.

Let

$$\mathbf{C} = [\mathbf{C}_{ij}], \quad i = 1 \text{ to } n, j = 1 \text{ to } n \qquad (2.3)$$

be the corresponding cipher text matrix.

The procedures for encryption and decryption adopted in this analysis are given in Fig. 1.



(a) Procedure for Encryption **(b) Procedure for Decryption**

Fig. 1. Schematic diagram of the cipher

Here r denotes the number of rounds in the iteration procedure. In the procedure for encryption, we have the iteration scheme given by

P = (KPK^{-1}) mod 256, (2.4)

P = Mix (P), (2.5)

and **P = P ⊕ K.** (2.6)

Here, (2.4) is used to achieve diffusion, while (2.5) and (2.6) are used to acquire confusion. The function **Mix (P)** mixes the plain text at every stage of the iteration. For a detailed discussion of this function, we may refer to [2]. In the process of decryption, the function IMix represents the reverse process of Mix.

Now, we present the algorithms for encryption, decryption, and for the modular arithmetic inverse of a square matrix.

Algorithm for Encryption

```
1.  Read n, P, K, r
2.  K^{-1} = Inverse (K)
3.  for i = 1 to r
    {
        P = (K P K^{-1}) mod 256
        P = Mix (P)
        P = P ⊕ K
    }
4.  C = P
5.  Write (C)
```

Algorithm for Decryption

```
1.  Read n, C, K, r
2.  K^{-1} = Inverse (K)
3.  for i = 1 to r
    {
        C = C ⊕ K
        C = IMix (C)
        C = (K^{-1} C K) mod 256
    }
4.  P = C
5.  Write (P)
```

Algorithm for Inverse (K)

```
//  The arithmetic inverse (A^{-1}), and the determinant of the
    matrix (Δ) are obtained
    by Gauss reduction method.
1.  A = K, N = 256
2.  A^{-1} = [A_ji] / Δ,  i = 1 to n, j = 1 to n
        //A_ji are the cofactors of a_ij, where a_ij are
            elements of A, and Δ is the determinant of A
3.  for i = 1 to n
    {
        if ((i Δ) mod N = 1)
                d = i;
        break;
    }
4.  B = [d A_ji] mod N
        // B is the modular arithmetic inverse of A
```

III. ILLUSTRATION OF THE CRYPTOGRAPHY OF AN IMAGE

Let us consider the following plain text.

Dear Friend! Do not worry about their criticism. Do take it very easy. All the countries and all the nations so to say, are our bosom friends; we supply nuclear weapons to one country, if it requests us. We provide the same nuclear weapons to other country, if it desires. We are never suggesting the countries to use weapons against each other. It is their responsibility to maintain peace, if they have got any wisdom. The rulers of the country are to be blamed, if they violate the fundamental rules of peace. (3.1)

Let us focus our attention on the first 256 characters of the above plain text. This is given by

Dear Friend! Do not worry about their criticism. Do take it very easy. All the countries and all the nations so to say, are our bosom friends; we supply nuclear weapons to one country, if it requests us. We provide the same nuclear weapons to other country (3.2)

On using the EBCDIC code, the plain text under consideration can be written in the decimal notation. On placing the first 16 numbers, corresponding to the first 16 characters of the plain text, in the first row, and the second 16 numbers in the second row, and so on, the plain text matrix P can be written in the form

$$P = \begin{bmatrix} 196 & 133 & 129 & 153 & 64 & 198 & 153 & 137 & 133 & 149 & 132 & 79 & 64 & 196 & 150 & 64 \\ 149 & 150 & 163 & 64 & 166 & 150 & 153 & 153 & 168 & 64 & 129 & 130 & 150 & 164 & 163 & 64 \\ 163 & 136 & 133 & 137 & 153 & 64 & 131 & 153 & 137 & 163 & 137 & 131 & 137 & 162 & 148 & 75 \\ 64 & 196 & 150 & 64 & 163 & 129 & 146 & 133 & 64 & 137 & 163 & 64 & 165 & 133 & 153 & 168 \\ 64 & 133 & 129 & 162 & 168 & 75 & 64 & 193 & 147 & 147 & 64 & 163 & 136 & 133 & 64 & 131 \\ 150 & 164 & 149 & 163 & 153 & 137 & 133 & 162 & 64 & 129 & 149 & 132 & 64 & 129 & 147 & 147 \\ 64 & 163 & 136 & 133 & 64 & 149 & 129 & 163 & 137 & 150 & 149 & 162 & 64 & 162 & 150 & 64 \\ 163 & 150 & 64 & 162 & 129 & 168 & 107 & 64 & 129 & 153 & 133 & 64 & 150 & 164 & 153 & 64 \\ 130 & 150 & 162 & 150 & 148 & 64 & 134 & 153 & 137 & 133 & 149 & 132 & 162 & 94 & 64 & 166 \\ 133 & 64 & 162 & 164 & 151 & 151 & 147 & 168 & 64 & 149 & 164 & 131 & 147 & 133 & 129 & 153 \\ 64 & 166 & 133 & 129 & 151 & 150 & 149 & 162 & 64 & 163 & 150 & 64 & 150 & 149 & 133 & 64 \\ 131 & 150 & 164 & 149 & 163 & 153 & 168 & 107 & 64 & 137 & 134 & 64 & 137 & 163 & 64 & 153 \\ 133 & 152 & 164 & 133 & 162 & 163 & 162 & 64 & 164 & 162 & 75 & 64 & 230 & 133 & 64 & 151 \\ 153 & 150 & 165 & 137 & 132 & 133 & 64 & 163 & 136 & 133 & 64 & 162 & 129 & 148 & 133 & 64 \\ 149 & 164 & 131 & 147 & 133 & 129 & 153 & 64 & 166 & 133 & 129 & 151 & 150 & 149 & 162 & 64 \\ 163 & 150 & 64 & 150 & 163 & 136 & 133 & 153 & 64 & 131 & 150 & 164 & 149 & 163 & 153 & 168 \end{bmatrix} \quad (3.3)$$

Let us choose a key k consisting of a set of 64 decimal numbers given by

$$k = \begin{bmatrix} 175 & 173 & 27 & 65 & 32 & 65 & 17 & 76 & 232 & 84 & 72 & 69 & 32 & 185 & 69 & 82 \\ 27 & 179 & 102 & 33 & 83 & 97 & 73 & 32 & 65 & 84 & 143 & 69 & 105 & 153 & 213 & 163 \\ 184 & 28 & 49 & 5 & 69 & 31 & 166 & 109 & 208 & 185 & 77 & 234 & 207 & 171 & 71 & 80 \\ 237 & 249 & 101 & 57 & 95 & 191 & 37 & 132 & 127 & 107 & 32 & 85 & 117 & 254 & 165 & 87 \end{bmatrix} \quad (3.4)$$

This can be written in the form of a matrix Q, where

$$Q = \begin{bmatrix} 175 & 173 & 27 & 65 & 32 & 65 & 17 & 76 \\ 232 & 84 & 72 & 69 & 32 & 185 & 69 & 82 \\ 27 & 179 & 102 & 33 & 83 & 97 & 73 & 32 \\ 65 & 84 & 143 & 69 & 105 & 153 & 213 & 163 \\ 184 & 28 & 49 & 5 & 69 & 31 & 166 & 109 \\ 208 & 185 & 77 & 234 & 207 & 171 & 71 & 80 \\ 237 & 249 & 101 & 57 & 95 & 191 & 37 & 132 \\ 127 & 107 & 32 & 85 & 117 & 254 & 165 & 87 \end{bmatrix} \quad (3.5)$$

The length of the secret key (which is to be transmitted) is 512 bits. On using the above matrix, we generate a new key matrix K, given by

$$K = \begin{bmatrix} Q & R \\ S & U \end{bmatrix} \quad (3.6)$$

where $U = Q^T$, in which T denotes the transpose of a matrix, and R and S are obtained from Q and U as follows. On interchanging the 1st row and the 8th row of Q, the 2nd row and the 7th row of Q, etc., we get R. Similarly, we obtain S from U. Thus, we have

$$K = \begin{bmatrix}
175 & 173 & 27 & 65 & 32 & 65 & 17 & 76 & 127 & 107 & 32 & 85 & 117 & 254 & 165 & 87 \\
232 & 84 & 72 & 69 & 32 & 185 & 69 & 82 & 237 & 249 & 101 & 57 & 95 & 191 & 37 & 132 \\
27 & 179 & 102 & 33 & 83 & 97 & 73 & 32 & 208 & 185 & 77 & 234 & 207 & 171 & 71 & 80 \\
65 & 84 & 143 & 69 & 105 & 153 & 213 & 163 & 184 & 28 & 49 & 5 & 69 & 31 & 166 & 109 \\
184 & 28 & 49 & 5 & 69 & 31 & 166 & 109 & 65 & 84 & 143 & 69 & 105 & 153 & 213 & 163 \\
208 & 185 & 77 & 234 & 207 & 171 & 71 & 80 & 27 & 179 & 102 & 33 & 83 & 97 & 73 & 32 \\
237 & 249 & 101 & 57 & 95 & 191 & 37 & 132 & 232 & 84 & 72 & 69 & 32 & 185 & 69 & 82 \\
127 & 107 & 32 & 85 & 117 & 254 & 165 & 87 & 175 & 173 & 27 & 65 & 32 & 65 & 17 & 76 \\
76 & 82 & 32 & 163 & 109 & 80 & 132 & 87 & 175 & 232 & 27 & 65 & 184 & 208 & 237 & 127 \\
17 & 69 & 73 & 213 & 166 & 71 & 37 & 165 & 173 & 84 & 179 & 84 & 28 & 185 & 249 & 107 \\
65 & 185 & 97 & 153 & 31 & 171 & 191 & 254 & 27 & 72 & 102 & 143 & 49 & 77 & 101 & 32 \\
32 & 32 & 83 & 105 & 69 & 207 & 95 & 117 & 65 & 69 & 33 & 69 & 5 & 234 & 57 & 85 \\
65 & 69 & 33 & 69 & 5 & 234 & 57 & 85 & 32 & 32 & 83 & 105 & 69 & 207 & 95 & 117 \\
27 & 72 & 102 & 143 & 49 & 77 & 101 & 32 & 65 & 185 & 97 & 153 & 31 & 171 & 191 & 254 \\
173 & 84 & 179 & 84 & 28 & 185 & 249 & 107 & 17 & 69 & 73 & 213 & 166 & 71 & 37 & 165 \\
175 & 232 & 27 & 65 & 184 & 208 & 237 & 127 & 76 & 82 & 32 & 163 & 109 & 80 & 132 & 87
\end{bmatrix} \qquad (3.7)$$

It may be noted here that, the size of the key K is increased to 16 x 16 so that we can handle a plain text matrix of size 16 x 16 (i.e., 2048 bits) at a time, in the cipher.

On using the algorithm given in section 2, the modular arithmetic inverse of K can be obtained as

$$K^{-1} = \begin{bmatrix}
251 & 24 & 106 & 200 & 158 & 133 & 226 & 83 & 167 & 67 & 140 & 200 & 10 & 73 & 96 & 177 \\
189 & 50 & 239 & 168 & 171 & 96 & 93 & 45 & 253 & 21 & 6 & 20 & 58 & 97 & 122 & 2 \\
167 & 129 & 255 & 47 & 0 & 60 & 68 & 133 & 57 & 42 & 124 & 111 & 233 & 10 & 229 & 62 \\
252 & 3 & 168 & 207 & 100 & 111 & 0 & 6 & 93 & 115 & 162 & 210 & 132 & 123 & 13 & 244 \\
55 & 187 & 60 & 254 & 50 & 101 & 174 & 15 & 19 & 101 & 152 & 140 & 246 & 118 & 90 & 5 \\
5 & 75 & 51 & 226 & 243 & 127 & 150 & 253 & 239 & 137 & 52 & 104 & 219 & 178 & 175 & 4 \\
38 & 75 & 1 & 220 & 99 & 46 & 155 & 104 & 22 & 249 & 205 & 162 & 104 & 202 & 208 & 108 \\
167 & 33 & 253 & 52 & 36 & 37 & 128 & 104 & 115 & 92 & 2 & 82 & 229 & 6 & 164 & 201 \\
83 & 226 & 133 & 158 & 200 & 106 & 24 & 251 & 177 & 96 & 73 & 10 & 200 & 140 & 67 & 167 \\
45 & 93 & 96 & 171 & 168 & 239 & 50 & 189 & 2 & 122 & 97 & 58 & 20 & 6 & 21 & 253 \\
133 & 68 & 60 & 0 & 47 & 255 & 129 & 167 & 62 & 229 & 10 & 233 & 111 & 124 & 42 & 57 \\
6 & 0 & 111 & 100 & 207 & 168 & 3 & 252 & 244 & 13 & 123 & 132 & 210 & 162 & 115 & 93 \\
15 & 174 & 101 & 50 & 254 & 60 & 187 & 55 & 5 & 90 & 118 & 246 & 140 & 152 & 101 & 19 \\
253 & 150 & 127 & 243 & 226 & 51 & 75 & 5 & 4 & 175 & 178 & 219 & 104 & 52 & 137 & 239 \\
104 & 155 & 46 & 99 & 220 & 1 & 75 & 38 & 108 & 208 & 202 & 104 & 162 & 205 & 249 & 22 \\
104 & 128 & 37 & 36 & 52 & 253 & 33 & 167 & 201 & 164 & 6 & 229 & 82 & 2 & 92 & 115
\end{bmatrix} \qquad (3.8)$$

On using (3.7) and (3.8), it can be readily shown that

$$\mathbf{K\,K^{-1} \bmod 256 = K^{-1}K \bmod 256 = I}. \qquad (3.9)$$

On applying the encryption algorithm, described in Section 2, we get the cipher text C in the form

$$C = \begin{bmatrix}
182 & 32 & 5 & 46 & 171 & 116 & 89 & 165 & 219 & 156 & 20 & 60 & 105 & 225 & 40 & 150 \\
155 & 22 & 169 & 188 & 205 & 224 & 128 & 13 & 28 & 218 & 46 & 253 & 20 & 186 & 238 & 137 \\
50 & 170 & 128 & 57 & 156 & 91 & 223 & 251 & 39 & 121 & 34 & 130 & 135 & 86 & 172 & 220 \\
57 & 24 & 239 & 193 & 53 & 75 & 13 & 200 & 106 & 2 & 81 & 248 & 3 & 239 & 191 & 209 \\
14 & 201 & 187 & 193 & 72 & 14 & 183 & 186 & 92 & 185 & 228 & 112 & 157 & 197 & 39 & 114 \\
195 & 111 & 38 & 210 & 218 & 107 & 177 & 111 & 131 & 149 & 47 & 43 & 149 & 122 & 72 & 24 \\
107 & 176 & 169 & 194 & 109 & 60 & 69 & 157 & 162 & 45 & 117 & 107 & 192 & 8 & 27 & 127 \\
224 & 4 & 112 & 32 & 154 & 170 & 10 & 96 & 175 & 104 & 69 & 218 & 37 & 163 & 95 & 69 \\
155 & 243 & 59 & 211 & 112 & 119 & 35 & 120 & 62 & 110 & 161 & 225 & 73 & 0 & 44 & 83 \\
8 & 156 & 152 & 243 & 159 & 9 & 113 & 125 & 194 & 49 & 61 & 65 & 82 & 204 & 11 & 183 \\
94 & 212 & 134 & 79 & 41 & 142 & 211 & 62 & 92 & 251 & 147 & 239 & 49 & 79 & 252 & 184 \\
170 & 192 & 71 & 150 & 0 & 116 & 233 & 1 & 215 & 87 & 128 & 191 & 177 & 94 & 14 & 60 \\
229 & 251 & 221 & 159 & 70 & 42 & 243 & 10 & 140 & 147 & 89 & 177 & 33 & 119 & 228 & 147 \\
159 & 149 & 20 & 5 & 212 & 185 & 189 & 224 & 170 & 211 & 251 & 152 & 16 & 204 & 165 & 161 \\
46 & 12 & 88 & 29 & 245 & 42 & 99 & 175 & 228 & 59 & 42 & 237 & 29 & 81 & 34 & 34 \\
43 & 35 & 82 & 35 & 186 & 239 & 172 & 69 & 52 & 223 & 235 & 3 & 23 & 47 & 6 & 186
\end{bmatrix} \qquad (3.10)$$

On using (3.7), (3.8), and (3.10), and applying the decryption algorithm described in section 2, we get the Plain text P, which is the same as (3.3).

Let us now examine the avalanche effect. Here, we modify the 88th character 's' in (3.2) to 't'. Then the plain text changes only in one binary bit as the EBCDIC codes of s and t are 162 and 163 respectively.

On using the modified plain text and the encryption algorithm, we get the cipher text C in the form

$$C = \begin{bmatrix}
98 & 173 & 249 & 92 & 248 & 116 & 57 & 19 & 215 & 166 & 142 & 27 & 56 & 175 & 238 & 174 \\
133 & 242 & 107 & 218 & 210 & 140 & 101 & 111 & 7 & 43 & 14 & 31 & 48 & 250 & 121 & 247 \\
79 & 103 & 250 & 180 & 248 & 237 & 205 & 136 & 153 & 141 & 105 & 161 & 246 & 136 & 174 & 155 \\
85 & 243 & 238 & 169 & 33 & 47 & 177 & 176 & 162 & 106 & 163 & 86 & 99 & 241 & 251 & 97 \\
158 & 22 & 146 & 123 & 25 & 98 & 81 & 68 & 42 & 106 & 148 & 86 & 198 & 68 & 215 & 109 \\
62 & 111 & 227 & 62 & 94 & 79 & 201 & 74 & 49 & 236 & 31 & 52 & 77 & 50 & 152 & 122 \\
30 & 219 & 202 & 136 & 200 & 35 & 164 & 58 & 26 & 230 & 42 & 184 & 206 & 133 & 145 & 37 \\
22 & 7 & 121 & 24 & 11 & 64 & 31 & 74 & 188 & 58 & 11 & 69 & 170 & 227 & 227 & 146 \\
250 & 253 & 2 & 247 & 148 & 167 & 105 & 21 & 209 & 52 & 91 & 174 & 145 & 158 & 80 & 223 \\
96 & 2 & 11 & 32 & 38 & 124 & 0 & 16 & 164 & 150 & 149 & 114 & 11 & 247 & 162 & 8 \\
215 & 105 & 236 & 17 & 157 & 40 & 237 & 145 & 4 & 244 & 62 & 59 & 48 & 10 & 227 & 226 \\
63 & 21 & 186 & 14 & 57 & 203 & 130 & 92 & 107 & 169 & 159 & 13 & 27 & 3 & 171 & 175 \\
152 & 218 & 155 & 28 & 146 & 163 & 217 & 250 & 124 & 42 & 124 & 236 & 47 & 28 & 14 & 192 \\
167 & 168 & 2 & 127 & 154 & 9 & 227 & 139 & 131 & 166 & 36 & 201 & 55 & 180 & 91 & 157 \\
25 & 129 & 209 & 151 & 157 & 235 & 244 & 50 & 102 & 144 & 207 & 230 & 30 & 100 & 5 & 77 \\
151 & 168 & 209 & 237 & 124 & 143 & 254 & 44 & 69 & 85 & 196 & 239 & 224 & 26 & 67 & 209
\end{bmatrix} \qquad (3.11)$$

On comparing (3.10) and (3.11), we find that the two cipher texts differ in 920 bits out of 2048 bits, which is quite significant.

Now let us change the key in (3.7) by 1 binary bit. This can be achieved by replacing the 60^{th} element 5 of the key k by 4. Then on using the original plain text (3.3), the modified key and the encryption algorithm, we get C in the form

$$C = \begin{bmatrix}
255 & 140 & 149 & 235 & 186 & 150 & 242 & 166 & 194 & 175 & 43 & 47 & 103 & 28 & 188 & 146 \\
180 & 230 & 195 & 174 & 17 & 255 & 9 & 149 & 123 & 17 & 57 & 125 & 47 & 254 & 23 & 81 \\
208 & 16 & 239 & 155 & 146 & 53 & 130 & 198 & 13 & 7 & 77 & 195 & 200 & 67 & 194 & 60 \\
227 & 56 & 47 & 9 & 255 & 66 & 25 & 7 & 190 & 55 & 114 & 126 & 191 & 113 & 132 & 70 \\
84 & 188 & 68 & 89 & 14 & 238 & 68 & 101 & 156 & 22 & 124 & 71 & 222 & 17 & 168 & 222 \\
68 & 97 & 221 & 204 & 247 & 9 & 212 & 143 & 168 & 100 & 41 & 27 & 255 & 194 & 38 & 16 \\
21 & 31 & 195 & 87 & 154 & 67 & 215 & 138 & 122 & 227 & 145 & 11 & 152 & 4 & 184 & 22 \\
184 & 191 & 26 & 237 & 179 & 75 & 176 & 121 & 81 & 135 & 54 & 47 & 209 & 88 & 90 & 248 \\
245 & 35 & 107 & 109 & 146 & 123 & 173 & 236 & 52 & 228 & 95 & 147 & 92 & 140 & 247 & 49 \\
23 & 202 & 116 & 71 & 156 & 217 & 31 & 139 & 15 & 254 & 71 & 56 & 107 & 131 & 55 & 28 \\
88 & 50 & 28 & 204 & 117 & 140 & 198 & 36 & 60 & 119 & 90 & 228 & 138 & 124 & 192 & 136 \\
207 & 237 & 206 & 18 & 110 & 251 & 248 & 8 & 113 & 196 & 151 & 226 & 95 & 16 & 120 & 18 \\
40 & 121 & 28 & 0 & 190 & 158 & 247 & 183 & 16 & 21 & 153 & 64 & 232 & 75 & 141 & 225 \\
88 & 82 & 141 & 227 & 190 & 25 & 223 & 161 & 81 & 122 & 191 & 143 & 11 & 164 & 158 & 157 \\
192 & 216 & 3 & 84 & 162 & 32 & 125 & 254 & 168 & 73 & 174 & 130 & 31 & 18 & 72 & 12 \\
161 & 177 & 154 & 244 & 137 & 195 & 142 & 16 & 145 & 235 & 55 & 135 & 227 & 13 & 166 & 2
\end{bmatrix} \qquad (3.12)$$

On comparing (3.12) with (3.10), we find that the cipher texts differ in 889 bits out of 2048 bits.

From the above analysis, we find that the Avalanche effect is quite pronounced and hence the cipher is a strong one.

On dividing the entire plain text given by (3.1) into blocks, we get 2 blocks, each is of size 256 characters. The cipher text corresponding to the first block is given in (3.9). The cipher text for the second block (in decimal form) is given by

$$\begin{matrix}
131 & 62 & 171 & 67 & 76 & 230 & 69 & 148 & 7 & 92 & 25 & 9 & 238 & 109 & 112 & 214 \\
179 & 186 & 163 & 194 & 215 & 16 & 225 & 166 & 206 & 61 & 103 & 1 & 97 & 222 & 235 & 10 \\
163 & 180 & 171 & 64 & 225 & 101 & 86 & 37 & 168 & 240 & 53 & 218 & 170 & 125 & 29 & 128 \\
10 & 14 & 183 & 167 & 98 & 88 & 160 & 75 & 100 & 76 & 167 & 146 & 220 & 1 & 10 & 71 \\
248 & 52 & 99 & 198 & 136 & 222 & 99 & 78 & 193 & 1 & 179 & 91 & 18 & 41 & 178 & 186 \\
211 & 100 & 161 & 131 & 242 & 163 & 160 & 162 & 216 & 166 & 52 & 69 & 81 & 123 & 42 & 176 \\
191 & 186 & 65 & 182 & 166 & 130 & 86 & 47 & 72 & 59 & 63 & 120 & 145 & 119 & 113 & 204 \\
161 & 63 & 45 & 95 & 73 & 4 & 171 & 234 & 6 & 209 & 65 & 198 & 246 & 38 & 138 & 175 \\
92 & 136 & 55 & 184 & 253 & 24 & 255 & 137 & 213 & 207 & 225 & 7 & 99 & 163 & 95 & 163 \\
189 & 81 & 215 & 146 & 205 & 251 & 214 & 74 & 197 & 115 & 168 & 48 & 0 & 253 & 243 & 35 \\
73 & 42 & 106 & 192 & 191 & 42 & 25 & 251 & 55 & 34 & 231 & 135 & 123 & 139 & 223 & 250 \\
160 & 77 & 191 & 120 & 117 & 33 & 45 & 202 & 157 & 174 & 159 & 126 & 3 & 91 & 86 & 228 \\
150 & 255 & 40 & 191 & 155 & 122 & 249 & 25 & 241 & 197 & 73 & 201 & 125 & 70 & 75 & 13 \\
240 & 6 & 105 & 64 & 227 & 43 & 82 & 0 & 148 & 47 & 61 & 107 & 159 & 160 & 23 & 121 \\
24 & 37 & 148 & 27 & 104 & 157 & 115 & 42 & 191 & 5 & 137 & 40 & 226 & 59 & 227 & 118 \\
243 & 101 & 186 & 179 & 198 & 62 & 46 & 193 & 124 & 185 & 106 & 1 & 237 & 194 & 230 & 125
\end{matrix}$$

This problem can also be studied in the case wherein K and K^{-1} are interchanged. Then, (2.4) is to be replaced by

$$\mathbf{P = (K^{-1}\,P\,K) \bmod 256}. \qquad (3.13)$$

In this case, the cipher text, C can be obtained as

$$C = \begin{pmatrix}
182 & 32 & 5 & 46 & 171 & 116 & 89 & 165 & 219 & 156 & 20 & 60 & 105 & 225 & 40 & 150 \\
155 & 22 & 169 & 188 & 205 & 224 & 128 & 13 & 28 & 218 & 46 & 253 & 20 & 186 & 238 & 137 \\
50 & 170 & 128 & 57 & 156 & 91 & 223 & 251 & 39 & 121 & 34 & 130 & 135 & 86 & 172 & 220 \\
57 & 24 & 239 & 193 & 53 & 75 & 13 & 200 & 106 & 2 & 81 & 248 & 3 & 239 & 191 & 209 \\
14 & 201 & 187 & 193 & 72 & 14 & 183 & 186 & 92 & 185 & 228 & 112 & 157 & 197 & 39 & 114 \\
195 & 111 & 38 & 210 & 218 & 107 & 177 & 111 & 131 & 149 & 47 & 43 & 149 & 122 & 72 & 24 \\
107 & 176 & 169 & 194 & 109 & 60 & 69 & 157 & 162 & 45 & 117 & 107 & 192 & 8 & 27 & 127 \\
224 & 4 & 112 & 32 & 154 & 170 & 10 & 96 & 175 & 104 & 69 & 218 & 37 & 163 & 95 & 69 \\
155 & 243 & 59 & 211 & 112 & 119 & 35 & 120 & 62 & 110 & 161 & 225 & 73 & 0 & 44 & 83 \\
8 & 156 & 152 & 243 & 159 & 9 & 113 & 125 & 194 & 49 & 61 & 65 & 82 & 204 & 11 & 183 \\
94 & 212 & 134 & 79 & 41 & 142 & 211 & 62 & 92 & 251 & 147 & 239 & 49 & 79 & 252 & 184 \\
170 & 192 & 71 & 150 & 0 & 116 & 233 & 1 & 215 & 87 & 128 & 191 & 177 & 94 & 14 & 60 \\
229 & 251 & 221 & 159 & 70 & 42 & 243 & 10 & 140 & 147 & 89 & 177 & 33 & 119 & 228 & 147 \\
159 & 149 & 20 & 5 & 212 & 185 & 189 & 224 & 170 & 211 & 251 & 152 & 16 & 204 & 165 & 161 \\
46 & 12 & 88 & 29 & 245 & 42 & 99 & 175 & 228 & 59 & 42 & 237 & 29 & 81 & 34 & 34 \\
43 & 35 & 82 & 35 & 186 & 239 & 172 & 69 & 52 & 223 & 235 & 3 & 23 & 47 & 6 & 186
\end{pmatrix} \quad (3.14)$$

Though we have got a different cipher text, on account of modifications, we have obtained the same plain text P by performing decryption.

When the plain text P is changed by one bit (i.e., when the 88^{th} character ‘s’ is changed to ‘t’), then the corresponding cipher text obtained is of the form

$$C = \begin{pmatrix}
98 & 173 & 249 & 92 & 248 & 116 & 57 & 19 & 215 & 166 & 142 & 27 & 56 & 175 & 238 & 174 \\
133 & 242 & 107 & 218 & 210 & 140 & 101 & 111 & 7 & 43 & 14 & 31 & 48 & 250 & 121 & 247 \\
79 & 103 & 250 & 180 & 248 & 237 & 205 & 136 & 153 & 141 & 105 & 161 & 246 & 136 & 174 & 155 \\
85 & 243 & 238 & 169 & 33 & 47 & 177 & 176 & 162 & 106 & 163 & 86 & 99 & 241 & 251 & 97 \\
158 & 22 & 146 & 123 & 25 & 98 & 81 & 68 & 42 & 106 & 148 & 86 & 198 & 68 & 215 & 109 \\
62 & 111 & 227 & 62 & 94 & 79 & 201 & 74 & 49 & 236 & 31 & 52 & 77 & 50 & 152 & 122 \\
30 & 219 & 202 & 136 & 200 & 35 & 164 & 58 & 26 & 230 & 42 & 184 & 206 & 133 & 145 & 37 \\
22 & 7 & 121 & 24 & 11 & 64 & 31 & 74 & 188 & 58 & 11 & 69 & 170 & 227 & 227 & 146 \\
250 & 253 & 2 & 247 & 148 & 167 & 105 & 21 & 209 & 52 & 91 & 174 & 145 & 158 & 80 & 223 \\
96 & 2 & 11 & 32 & 38 & 124 & 0 & 16 & 164 & 150 & 149 & 114 & 11 & 247 & 162 & 8 \\
215 & 105 & 236 & 17 & 157 & 40 & 237 & 145 & 4 & 244 & 62 & 59 & 48 & 10 & 227 & 226 \\
63 & 21 & 186 & 14 & 57 & 203 & 130 & 92 & 107 & 169 & 159 & 13 & 27 & 3 & 171 & 175 \\
152 & 218 & 155 & 28 & 146 & 163 & 217 & 250 & 124 & 42 & 124 & 236 & 47 & 28 & 14 & 192 \\
167 & 168 & 2 & 127 & 154 & 9 & 227 & 139 & 131 & 166 & 36 & 201 & 55 & 180 & 91 & 157 \\
25 & 129 & 209 & 151 & 157 & 235 & 244 & 50 & 102 & 144 & 207 & 230 & 30 & 100 & 5 & 77 \\
151 & 168 & 209 & 237 & 124 & 143 & 254 & 44 & 69 & 85 & 196 & 239 & 224 & 26 & 67 & 209
\end{pmatrix} \quad (3.15)$$

Thus in this case, the change in the cipher text is 920 bits out of 2048 bits.

On changing 1 bit in the key (i.e., replacing 5 by 4), we have

$$C = \begin{pmatrix}
255 & 140 & 149 & 235 & 186 & 150 & 242 & 166 & 194 & 175 & 43 & 47 & 103 & 28 & 188 & 146 \\
180 & 230 & 195 & 174 & 17 & 255 & 9 & 149 & 123 & 17 & 57 & 125 & 47 & 254 & 23 & 81 \\
208 & 16 & 239 & 155 & 146 & 53 & 130 & 198 & 13 & 7 & 77 & 195 & 200 & 67 & 194 & 60 \\
227 & 56 & 47 & 9 & 255 & 66 & 25 & 7 & 190 & 55 & 114 & 126 & 191 & 113 & 132 & 70 \\
84 & 188 & 68 & 89 & 14 & 238 & 68 & 101 & 156 & 22 & 124 & 71 & 222 & 17 & 168 & 222 \\
68 & 97 & 221 & 204 & 247 & 9 & 212 & 143 & 168 & 100 & 41 & 27 & 255 & 194 & 38 & 16 \\
21 & 31 & 195 & 87 & 154 & 67 & 215 & 138 & 122 & 227 & 145 & 11 & 152 & 4 & 184 & 22 \\
184 & 191 & 26 & 237 & 179 & 75 & 176 & 121 & 81 & 135 & 54 & 47 & 209 & 88 & 90 & 248 \\
245 & 35 & 107 & 109 & 146 & 123 & 173 & 236 & 52 & 228 & 95 & 147 & 92 & 140 & 247 & 49 \\
23 & 202 & 116 & 71 & 156 & 217 & 31 & 139 & 15 & 254 & 71 & 56 & 107 & 131 & 55 & 28 \\
88 & 50 & 28 & 204 & 117 & 140 & 198 & 36 & 60 & 119 & 90 & 228 & 138 & 124 & 192 & 136 \\
207 & 237 & 206 & 18 & 110 & 251 & 248 & 8 & 113 & 196 & 151 & 226 & 95 & 16 & 120 & 18 \\
40 & 121 & 28 & 0 & 190 & 158 & 247 & 183 & 16 & 21 & 153 & 64 & 232 & 75 & 141 & 225 \\
88 & 82 & 141 & 227 & 190 & 25 & 223 & 161 & 81 & 122 & 191 & 143 & 11 & 164 & 158 & 157 \\
192 & 216 & 3 & 84 & 162 & 32 & 125 & 254 & 168 & 73 & 174 & 130 & 31 & 18 & 72 & 12 \\
161 & 177 & 154 & 244 & 137 & 195 & 142 & 16 & 145 & 235 & 55 & 135 & 227 & 13 & 166 & 2
\end{pmatrix} \quad (3.16)$$

From (3.14) and (3.16), we notice the change in C is 889 bits out of 2048 bits. From the above analysis, we find that the Avalanche effect is quite significant and hence this cipher is also is a very strong one.

On dividing the entire plain text given in (3.1) into blocks, wherein each block is of size 256 characters, we get the corresponding cipher text in the decimal form. The first block is already presented in (3.9). Rest of the cipher text is given by

$$\begin{matrix}
131 & 62 & 171 & 67 & 76 & 230 & 69 & 148 & 7 & 92 & 25 & 9 & 238 & 109 & 112 & 214 \\
179 & 186 & 163 & 194 & 215 & 16 & 225 & 166 & 206 & 61 & 103 & 1 & 97 & 222 & 235 & 10 \\
163 & 180 & 171 & 64 & 225 & 101 & 86 & 37 & 168 & 240 & 53 & 218 & 170 & 125 & 29 & 128 \\
10 & 14 & 183 & 167 & 98 & 88 & 160 & 75 & 100 & 76 & 167 & 146 & 220 & 1 & 10 & 71 \\
248 & 52 & 99 & 198 & 136 & 222 & 99 & 78 & 193 & 1 & 179 & 91 & 18 & 41 & 178 & 186 \\
211 & 100 & 161 & 131 & 242 & 163 & 160 & 162 & 216 & 166 & 52 & 69 & 81 & 123 & 42 & 176 \\
191 & 186 & 65 & 182 & 166 & 130 & 86 & 47 & 72 & 59 & 63 & 120 & 145 & 119 & 113 & 204 \\
161 & 63 & 45 & 95 & 73 & 4 & 171 & 234 & 6 & 209 & 65 & 198 & 246 & 38 & 138 & 175 \\
92 & 136 & 55 & 184 & 253 & 24 & 255 & 137 & 213 & 207 & 225 & 7 & 99 & 163 & 95 & 163 \\
189 & 81 & 215 & 146 & 205 & 251 & 214 & 74 & 197 & 115 & 168 & 48 & 0 & 253 & 243 & 35 \\
73 & 42 & 106 & 192 & 191 & 42 & 25 & 251 & 55 & 34 & 231 & 135 & 123 & 139 & 223 & 250 \\
160 & 77 & 191 & 120 & 117 & 33 & 45 & 202 & 157 & 174 & 159 & 126 & 3 & 91 & 86 & 228 \\
150 & 255 & 40 & 191 & 155 & 122 & 249 & 25 & 241 & 197 & 73 & 201 & 125 & 70 & 75 & 13 \\
240 & 6 & 105 & 64 & 227 & 43 & 82 & 0 & 148 & 47 & 61 & 107 & 159 & 160 & 23 & 121 \\
24 & 37 & 148 & 27 & 104 & 157 & 115 & 42 & 191 & 5 & 137 & 40 & 226 & 59 & 227 & 118 \\
243 & 101 & 186 & 179 & 198 & 62 & 46 & 193 & 124 & 185 & 106 & 1 & 237 & 194 & 230 & 125
\end{matrix}$$

IV. CRYPTANALYSIS

The different types of cryptanalytical attacks available in the literature are:

(1) Cipher text only attack, (2) Known plain text attack,
(3) Chosen plain text attack, (4) Chosen cipher text attack.

When the cipher text is known to us, we can determine the plain text, provided the key is known to us. As the key contains 64 decimal numbers, the size of the key space is

$$2^{512} \simeq (10^3)^{51.2} = 10^{153.6}$$

which is very large. Hence it takes a very long time for the determination of the key. Thus the cipher text only attack is impossible.

We know that, the Hill cipher can be broken by the known plain text attack, as there exists a direct relation between C and P. But in the present modification, which involves K and K^{-1}, one on the left side of P and the other on the right side of P, and the process of iteration together with the Mix function and the XOR operation, we cannot get a direct relation between C and P. Hence, this cipher developed in the present analysis cannot be broken by the known plain text attack.

The chosen plain / cipher text attack is ruled out.

V. CONCLUSIONS

In this paper, we have modified the Hill cipher, governed by the single relation

$$\mathbf{C = (K\,P) \bmod 26}, \qquad (5.1)$$

in two different cases.

In case one, the iterative scheme includes the relations

$$\mathbf{P = (K\,P\,K^{-1}) \bmod 256}, \qquad (5.2)$$

$$\mathbf{P = Mix\,(P)}, \qquad (5.3)$$

and $\mathbf{P = P \oplus K}$, (5.4)

and in case two, we have the relation (5.2) modified as

$$\mathbf{P = (K^{-1}\,P\,K) \bmod 256}, \qquad (5.5)$$

while (5.3) and (5.4) are the same.

In this analysis, the length of the plain text block is 2048 bits and the length of the key is 512 bits. As the avalanche effect and the cryptanalysis clearly reveal that, the cipher is a strong one and it cannot be broken by any cryptanalytic attack. This analysis can be extended to a block of any size by using the concept of interlacing [3].

VI. REFERENCES

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

[2] 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 Plain Text", International Journal of Computer and Network Security (IJCNS), Vol. 1, No. 1, pp. 27 – 30, Oct. 2009.

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

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. He is a Member, Editorial Board and Reviewer of International Journal of Computational Intelligence and Information Security (IJCIIS), Senior Member of International Association of Computer Science and Information Technology (IACSIT) and Reviewer of International Journal of Computer and Network Security (IJCNS). His research interests are Network Security & Cryptography, Image Processing, Data Mining and Genetic Algorithms and published research papers in International Journal of Computer and Network Security (IJCNS), International Journal of Computer Theory and Engineering (IJCTE) and International Journal of Computational Intelligence and Information Security (IJCIIS).

Dr. S. Durga Bhavani is presently working as Professor in School of Information Technology (SIT), JNTUH, Hyderabad, India. She has more than 18 years of teaching experience. Her research area includes Evidential Reasoning, Cryptography and Image Processing. She has no. of research publications to her credit.

Prof. D. S. R. Murthy obtained B. E. (Electronics) from Bangalore University in 1982, M. Tech. (CSE) from Osmania University in 1985 and presently pursuing Ph.D. from JNTUH, Hyderabad since 2007. He is presently working as Professor in the Dept. of Information Technology (IT), SNIST since Oct. 2004. He earlier worked as Lecturer in CSE, NIT (formerly REC), Warangal, India during Sep. 1985 – Feb. 1993, as Assistant Professor in CSE, JNTUCE, Anantapur, India during Feb. 1993 – May 1998, as Academic Coordinator, ISM, Icfaian Foundation, Hyderabad, India during May 1998 – May 2001 and as Associate Professor in CSE, SNIST during May 2001 - Sept. 2004. He worked as Head of the Dept. of CSE, JNTUCE, Anantapur during Jan. 1996 – Jan 1998, Dept. of IT, SNIST during Apr. 2005 – May 2006, and Oct. 2007 – Feb. 2009. He is a Fellow of IE(I), Fellow of IETE, Senior Life Member of CSI, Life Member of ISTE, Life Member of SSI, DOEACC Expert member, and Chartered Engineer (IE(I) & IETE). He is a Reviewer of International Journal of Advanced Research in Computer Science (IJARCS), International Journal of Computational Intelligence and Information Security (IJCIIS) and International Journal of Computer Science and Information Technology (IJCSIT). He is a member of International Association of Computer Science and Information Technology (IACSIT). He published a text book on C Programming & Data Structures. His research interests are Image Processing and Image Cryptography and published research papers in International Journal of Computer and Network Security (IJCNS), International Journal of Computer Theory and Engineering (IJCTE), International Journal of Computational Intelligence and Information Security (IJCIIS) and in International Journal of Advanced Research in Computer Science (IJARCS).

