A Large Block Cipher Involving a Key Applied on Both the Sides of the Plain Text

Vivek Vardhan Bariki[1]

[1]Dept. of Computer Science & Engg., CMRTECHNICAL CAMPUS, Hyderabad, India

Abstract: In this paper, we have developed a block cipher by modifying the Hill cipher. In this, the plain text matrix P is multiplied on both the sides by the key matrix. Here, the size of the key is 512 bits and the size of the plain text is 2048 bits. As the procedure adopted here is an iterative one, and as no direct linear relation between the cipher text C and the plain text P can be obtained, the cipher cannot be broken by any cryptanalytic attack.

Keywords: Block Cipher, Modular arithmetic inverse, Plain text, Cipher text, Key.

1. Introduction

The study of the block ciphers, which was initiated several centuries back, gained considerable impetus in the last quarter of the last century. Noting that diffusion and confusion play a vital role in a block cipher, Feistel etal, [1 – 2] developed a block cipher, called Feistel cipher. In his analysis, he pointed out that, the strength of the cipher increases when the block size is more, the key size is more, and the number of rounds in the iteration is more.

The popular cipher DES [3], developed in 1977, has a 56 bit key and a 64 bit plain text. The variants of the DES are double DES, and triple DES. In double DES, the size of the plain text block is 64 bits and the size of the key is 112 bits. In the triple DES, the key is of the length 168 bits and the plain text block is of the size is 64 bits. At the beginning of the century, noting that 64 bit block size is a drawback in DES, Joan Daemen and Vincent Rijmen, have developed a new block cipher called

AES [4], wherein the block size of the plain text is 128 bits and key is of length 128,

192, or 256 bits. In the subsequent development, on modifying Hill cipher, several researchers [5 – 9], have developed various cryptographical algorithms wherein the length of the key and the size of the plain text block are quite significant.

In the present paper, our objective is to develop a block cipher wherein the key size and the block size are significantly large. Here, we use Gauss reduction method for obtaining the modular arithmetic inverse of a matrix. In what follows, we present the plan of the paper.

In section 2, we have discussed the development of the cipher. In section 3, we have illustrated the cipher by considering an example. In section 4, we have dealt with the cryptanalysis of the cipher. Finally, in section 5, we have presented the computations and arrived at the conclusions.

2. Development of the cipher

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

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

where each P_{ij} is a decimal number which lies between 0 and 255.

Let us choose a key k consisting of a set of integers, which lie between 0 and 255. Let us generate a key matrix, denoted as K, given by

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

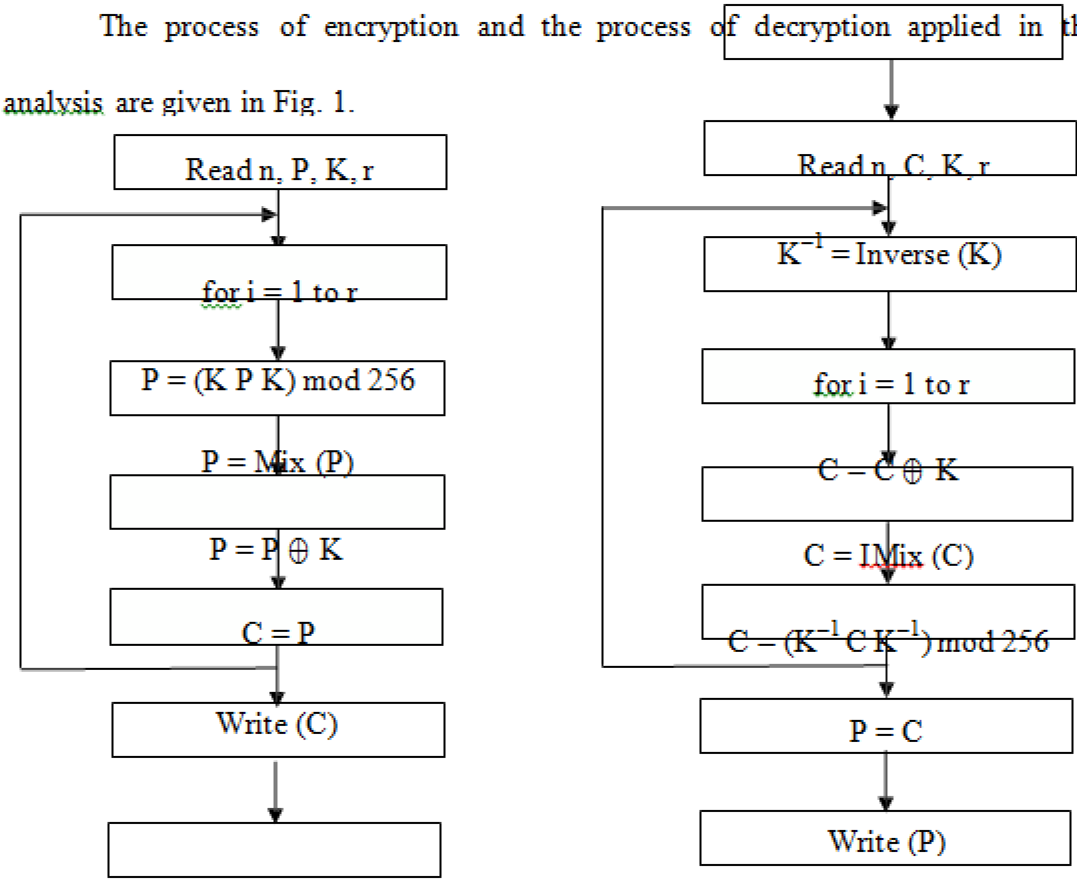
where each K_{ij} is also an integer in the interval [0 – 255].

Let

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

be the corresponding cipher text matrix.

The process of encryption and the process of decryption applied in this analysis are given in Fig. 1.



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

Fig. 1. Schematic diagram of the cipher

Here r denotes the number of rounds.

In the process of encryption, we have used an iterative procedure which includes the relations

$$\mathbf{P = (K\,P\,K) \bmod 256,} \qquad (2.4)$$

$$\mathbf{P = Mix\,(P),} \qquad (2.5)$$ and $$\mathbf{P = P \oplus K} \qquad (2.6)$$

The relation (2.4) causes diffusion, while (2.5) and (2.6) lead to confusion. Thus, these three relations enhance the strength of the cipher.

Let us consider **Mix (P)**. In this the decimal numbers in P are converted into their binary form. Then we have a matrix of size n x 8n, and this is given by

$$\begin{pmatrix} P_{111}, P_{112}, \ldots, P_{118}, P_{121}, P_{122}, \ldots, P_{128}, \ldots, P_{1n1}, P_{1n2}, \ldots, P_{1n8} \\ P_{211}, P_{212}, \ldots, P_{218}, P_{221}, P_{222}, \ldots, P_{228}, \ldots, P_{2n1}, P_{2n2}, \ldots, P_{2n8} \\ \ldots \\ P_{n11}, P_{n12}, \ldots, P_{n18}, P_{n21}, P_{n22}, \ldots, P_{n28}, \ldots, P_{nn1}, P_{nn2}, \ldots, P_{nn8} \end{pmatrix}$$

Here, $P_{111}, P_{112}, \ldots, P_{118}$ are binary bits corresponding to P_{11}. Similarly, $P_{ij1}, P_{ij2}, \ldots, P_{ij8}$ are the binary bits representing P_{ij}.

The above matrix can be considered as a single string in a row wise manner. As the length of the string is $8n^2$, it is divided into n^2 substrings, wherein the length of each substring is 8 bits. If n^2 is divisible by 8, we focus our attention on the first 8 substrings. We place the first bits of these 8 binary substrings, in order, at one place and form a new binary substring. Similarly, we assemble the second 8 bits and form the second binary substring. Following the same procedure, we can get six more binary substrings in the same manner. Continuing in the same way, we exhaust all the binary substrings obtained from the plain text.

However, if n^2 is not divisible by 8, then we consider the remnant of the string, and divide it into two halves. Then we mix these two halves by placing the first bit of the second half, just after the first bit of the first half, the second bit of the second half, next to the second bit of the first half, etc. Thus we get a new binary substring corresponding to the remaining string. This completes the process of mixing.

In order to perform the exclusive or operation in $P = P \oplus K$, we write the matrices, both P and K, in their binary form, and carryout the XOR operation between the corresponding binary bits.

In the process of decryption, the function IMix represents the reverse process of Mix.

In what follows, we present the algorithms for encryption, and decryption. We also provide an algorithm for finding the modular arithmetic inverse of a square matrix.

Algorithm for Encryption

1. Read n, P, K, r

2. for i = 1 to r

{

$P = (K\ P\ K) \bmod 256$

$P = Mix (P)$ $P = P \oplus K$

}

3. $C = P$

4. Write (C)

Algorithm for Decryption

1. Read n, C, K, r

2. $K^{-1} = Inverse (K)$

3. for i = 1 to r

{

$C = C \oplus K$

$C = IMix (C)$

$C = (K^{-1}\ C\ K^{-1}) \bmod 256$

}

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. $A^{-1} = [A_{ji}] / \Delta$, 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

3. Illustration of the cipher

Let us consider the following plain text.

International Journal of Engineering Research and General Science Volume 4, Issue 1, January-February, 2016
ISSN 2091-2730

No country wants to bring in calamities to its own people. If the people do not have any respect for the country, then the Government has to take appropriate measures and take necessary action to keep the people in order. No country can excuse the erratic behaviour of the people, even though something undue happened to them in the past. Take the appropriate action in the light of this fact. Invite all the people to come into the fold of the Government. Try to persuade them as far as possible. Let us see!! (3.1)

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

No country wants to bring in calamities to its own people. If the people do not have any respect for the country, then the Government has to take appropriate measures and take necessary action to keep the people in order. No country can excuse the erratic !! (3.2)

On using EBCDIC code, we get 26 numbers, corresponding to 256 characters.

Now on placing 16 numbers in each row, we get the plain text matrix P in the decimal

form

$$P = \begin{array}{cccccccccccccccc}
64 & 163 & 150 & 64 & 130 & 153 & 137 & 149 & 135 & 64 & 137 & 149 & 64 & 131 & 129 & 147 \\
129 & 148 & 137 & 163 & 137 & 133 & 162 & 64 & 163 & 150 & 64 & 137 & 163 & 162 & 64 & 150 \\
166 & 149 & 64 & 151 & 133 & 150 & 151 & 147 & 133 & 75 & 64 & 201 & 134 & 64 & 163 & 136 \\
133 & 64 & 151 & 133 & 150 & 151 & 147 & 133 & 64 & 132 & 150 & 64 & 149 & 150 & 163 & 64 \\
136 & 129 & 165 & 133 & 64 & 129 & 149 & 168 & 64 & 153 & 133 & 162 & 151 & 133 & 131 & 163 \\
64 & 134 & 150 & 153 & 64 & 163 & 136 & 133 & 64 & 131 & 150 & 164 & 149 & 163 & 153 & 168 \\
107 & 64 & 163 & 136 & 133 & 149 & 64 & 163 & 136 & 133 & 64 & 199 & 150 & 165 & 133 & 153 \\
149 & 148 & 133 & 149 & 163 & 64 & 136 & 129 & 162 & 64 & 163 & 150 & 64 & 163 & 129 & 146 \\
133 & 64 & 129 & 151 & 151 & 153 & 150 & 151 & 153 & 137 & 129 & 163 & 133 & 64 & 148 & 133 \\
129 & 162 & 164 & 153 & 133 & 162 & 64 & 129 & 149 & 132 & 64 & 163 & 129 & 146 & 133 & 64 \\
149 & 133 & 131 & 133 & 162 & 162 & 129 & 153 & 168 & 64 & 129 & 131 & 163 & 137 & 150 & 149 \\
64 & 163 & 150 & 64 & 146 & 133 & 133 & 151 & 64 & 163 & 136 & 133 & 64 & 151 & 133 & 150 \\
151 & 147 & 133 & 64 & 137 & 149 & 64 & 150 & 153 & 132 & 133 & 153 & 75 & 64 & 213 & 150 \\
64 & 131 & 150 & 164 & 149 & 163 & 153 & 168 & 64 & 131 & 129 & 149 & 64 & 133 & 167 & 131 \\
164 & 162 & 133 & 64 & 163 & 136 & 133 & 64 & 133 & 153 & 153 & 129 & 163 & 137 & 131 & 64
\end{array} \qquad (3.3)$$

Obviously, here the length of the plain text block is 16 x 16 x 8 (2048) bits.

International Journal of Engineering Research and General Science Volume 4, Issue 1, January-February, 2016
ISSN 2091-2730

Let us choose a key k consisting of 64 numbers. This can be written in the form of a matrix given by

$$Q = \begin{matrix} 175 & 173 & 27 & 65 & 32 & 65 & 17 & 76 \\ 232 & 84 & 72 & 69 & 32 & 185 & 69 & 82 \\ 27 & 179 & 102 & 33 & 83 & 97 & 73 & 32 \\ 65 & 84 & 143 & 69 & 105 & 153 & 213 & 163 \\ 184 & 28 & 49 & 5 & 69 & 31 & 166 & 109 \\ 208 & 185 & 77 & 234 & 207 & 171 & 71 & 80 \end{matrix} \qquad (3.4)$$

The length of the secret key (which is to be transmitted) is 512 bits. On using this key, we can generate a new key K in the form

$$K = \begin{bmatrix} Q & R \\ S & U \end{bmatrix} \qquad (3.5)$$

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

$$K = \begin{bmatrix} 175 & 173 & 27 & 65 & 32 & 65 & 17 & 76 & 127 & 107 & 32 & 85 & 117 & 254 & 165 & 87 \\ 232 & 84 & 72 & 69 & 32 & 185 & 69 & 82 & 237 & 249 & 101 & 57 & 95 & 191 & 37 & 132 \\ 27 & 179 & 102 & 33 & 83 & 97 & 73 & 32 & 208 & 185 & 77 & 234 & 207 & 171 & 71 & 80 \\ 65 & 84 & 143 & 69 & 105 & 153 & 213 & 163 & 184 & 28 & 49 & 5 & 69 & 31 & 166 & 109 \\ 184 & 28 & 49 & 5 & 69 & 31 & 166 & 109 & 65 & 84 & 143 & 69 & 105 & 153 & 213 & 163 \\ 208 & 185 & 77 & 234 & 207 & 171 & 71 & 80 & 27 & 179 & 102 & 33 & 83 & 97 & 73 & 32 \\ 237 & 249 & 101 & 57 & 95 & 191 & 37 & 132 & 232 & 84 & 72 & 69 & 32 & 185 & 69 & 82 \\ 127 & 107 & 32 & 85 & 117 & 254 & 165 & 87 & 175 & 173 & 27 & 65 & 32 & 65 & 17 & 76 \\ 76 & 82 & 32 & 163 & 109 & 80 & 132 & 87 & 175 & 232 & 27 & 65 & 184 & 208 & 237 & 127 \\ 17 & 69 & 73 & 213 & 166 & 71 & 37 & 165 & 173 & 84 & 179 & 84 & 28 & 185 & 249 & 107 \\ 65 & 185 & 97 & 153 & 31 & 171 & 191 & 254 & 27 & 72 & 102 & 143 & 49 & 77 & 101 & 32 \\ 32 & 32 & 83 & 105 & 69 & 207 & 95 & 117 & 65 & 69 & 33 & 69 & 5 & 234 & 57 & 85 \\ 65 & 69 & 33 & 69 & 5 & 234 & 57 & 85 & 32 & 32 & 83 & 105 & 69 & 207 & 95 & 117 \\ 27 & 72 & 102 & 143 & 49 & 77 & 101 & 32 & 65 & 185 & 97 & 153 & 31 & 171 & 191 & 254 \\ 173 & 84 & 179 & 84 & 28 & 185 & 249 & 107 & 17 & 69 & 73 & 213 & 166 & 71 & 37 & 165 \\ 175 & 232 & 27 & 65 & 184 & 208 & 237 & 127 & 76 & 82 & 32 & 163 & 109 & 80 & 132 & 87 \end{bmatrix} \qquad (3.6)$$

whose size is 16 x 16.

On using the algorithm for modular arithmetic inverse (See Section 2), we get

$$K^{-1} = \begin{array}{cccccccccccccccc}
251 & 24 & 106 & 200 & 158 & 133 & 226 & 83 & 167 & 67 & 140 & 200 & 10 & 73 & 96 & 177 \\
189 & 50 & 239 & 168 & 171 & 96 & 93 & 45 & 253 & 21 & 6 & 20 & 58 & 97 & 122 & 2 \\
167 & 129 & 255 & 47 & 0 & 60 & 68 & 133 & 57 & 42 & 124 & 111 & 233 & 10 & 229 & 62 \\
252 & 3 & 168 & 207 & 100 & 111 & 0 & 6 & 93 & 115 & 162 & 210 & 132 & 123 & 13 & 244 \\
55 & 187 & 60 & 254 & 50 & 101 & 174 & 15 & 19 & 101 & 152 & 140 & 246 & 118 & 90 & 5 \\
5 & 75 & 51 & 226 & 243 & 127 & 150 & 253 & 239 & 137 & 52 & 104 & 219 & 178 & 175 & 4 \\
38 & 75 & 1 & 220 & 99 & 46 & 155 & 104 & 22 & 249 & 205 & 162 & 104 & 202 & 208 & 108 \\
167 & 33 & 253 & 52 & 36 & 37 & 128 & 104 & 115 & 92 & 2 & 82 & 229 & 6 & 164 & 201 \\
83 & 226 & 133 & 158 & 200 & 106 & 24 & 251 & 177 & 96 & 73 & 10 & 200 & 140 & 67 & 167 \\
45 & 93 & 96 & 171 & 168 & 239 & 50 & 189 & 2 & 122 & 97 & 58 & 20 & 6 & 21 & 253 \\
133 & 68 & 60 & 0 & 47 & 255 & 129 & 167 & 62 & 229 & 10 & 233 & 111 & 124 & 42 & 57 \\
6 & 0 & 111 & 100 & 207 & 168 & 3 & 252 & 244 & 13 & 123 & 132 & 210 & 162 & 115 & 93 \\
15 & 174 & 101 & 50 & 254 & 60 & 187 & 55 & 5 & 90 & 118 & 246 & 140 & 152 & 101 & 19 \\
253 & 150 & 127 & 243 & 226 & 51 & 75 & 5 & 4 & 175 & 178 & 219 & 104 & 52 & 137 & 239 \\
104 & 155 & 46 & 99 & 220 & 1 & 75 & 38 & 108 & 208 & 202 & 104 & 162 & 205 & 249 & 22 \\
104 & 128 & 37 & 36 & 52 & 253 & 33 & 167 & 201 & 164 & 6 & 229 & 82 & 2 & 92 & 115
\end{array} \qquad (3.7)$$

On using (3.6) and (3.7), it can be readily shown that

$$\mathbf{K\,K^{-1} \bmod 256 = K^{-1}K \bmod 256 = I}. \qquad (3.8)$$

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

$$C = \begin{array}{cccccccccccccccc}
57 & 57 & 108 & 41 & 0 & 4 & 105 & 26 & 38 & 128 & 194 & 61 & 148 & 67 & 11 & 71 \\
116 & 195 & 96 & 224 & 213 & 18 & 92 & 194 & 42 & 125 & 198 & 39 & 226 & 90 & 56 & 234 \\
174 & 156 & 30 & 14 & 207 & 134 & 166 & 65 & 233 & 207 & 151 & 29 & 93 & 237 & 11 & 201 \\
50 & 100 & 40 & 36 & 47 & 202 & 17 & 243 & 232 & 47 & 145 & 191 & 45 & 39 & 39 & 100 \\
76 & 147 & 3 & 79 & 51 & 44 & 141 & 49 & 122 & 20 & 153 & 121 & 75 & 143 & 128 & 5 \\
25 & 1 & 212 & 6 & 195 & 243 & 47 & 75 & 50 & 165 & 103 & 85 & 92 & 130 & 47 & 184 \\
127 & 163 & 199 & 174 & 221 & 85 & 43 & 207 & 203 & 168 & 137 & 28 & 186 & 100 & 156 & 98 \\
140 & 28 & 151 & 78 & 245 & 132 & 217 & 175 & 218 & 189 & 223 & 78 & 51 & 92 & 100 & 30 \\
166 & 222 & 199 & 196 & 10 & 120 & 202 & 101 & 167 & 48 & 154 & 46 & 32 & 197 & 196 & 36 \\
186 & 25 & 214 & 134 & 103 & 134 & 52 & 104 & 154 & 202 & 207 & 122 & 108 & 141 & 52 & 204 \\
6 & 100 & 188 & 114 & 107 & 19 & 185 & 201 & 31 & 53 & 106 & 235 & 228 & 171 & 102 & 69 \\
216 & 104 & 181 & 34 & 122 & 95 & 196 & 142 & 253 & 142 & 59 & 199 & 102 & 199 & 49 & 146 \\
167 & 137 & 157 & 25 & 55 & 162 & 102 & 211 & 91 & 159 & 19 & 83 & 225 & 220 & 251 & 149 \\
109 & 14 & 88 & 147 & 93 & 16 & 7 & 208 & 93 & 46 & 2 & 160 & 90 & 61 & 198 & 116 \\
252 & 104 & 35 & 60 & 222 & 157 & 64 & 207 & 212 & 239 & 203 & 79 & 24 & 10 & 40 & 55 \\
25 & 129 & 49 & 123 & 117 & 82 & 228 & 172 & 130 & 104 & 79 & 189 & 47 & 209 & 12 & 143
\end{array} \qquad (3.9)$$

On using (3.7) and (3.9), and applying the decryption algorithm presented in section 2, we get the Plain text P.

This is the same as (3.3).

Let us now find out the avalanche effect. To this end, we focus our attention on the plain text (3.2), and modify the 88th character 'y' to 'z'. Then the plain text changes only in one binary bit as the EBCDIC code of y is 168 and that of z is 169.

On using the encryption algorithm, we get the cipher text C corresponding to the modified plain text (wherein y is replaced by z) in the form

$$C = \begin{matrix} 119 & 213 & 181 & 74 & 20 & 56 & 48 & 122 & 209 & 55 & 60 & 43 & 150 & 252 & 154 & 247 \\ 224 & 97 & 64 & 47 & 160 & 153 & 76 & 194 & 250 & 98 & 160 & 49 & 221 & 74 & 225 & 63 \\ 117 & 169 & 215 & 90 & 103 & 102 & 47 & 62 & 163 & 210 & 63 & 242 & 30 & 153 & 218 & 163 \\ 22 & 87 & 232 & 166 & 71 & 179 & 220 & 230 & 215 & 250 & 255 & 67 & 156 & 48 & 120 & 241 \\ 236 & 60 & 224 & 27 & 162 & 28 & 74 & 49 & 158 & 99 & 206 & 97 & 220 & 119 & 32 & 120 \\ 251 & 31 & 248 & 20 & 146 & 64 & 117 & 76 & 35 & 59 & 35 & 181 & 119 & 58 & 110 & 10 \\ 227 & 102 & 247 & 97 & 16 & 73 & 247 & 64 & 165 & 41 & 60 & 249 & 187 & 251 & 47 & 221 \\ 223 & 219 & 51 & 108 & 15 & 23 & 227 & 118 & 244 & 106 & 52 & 46 & 253 & 228 & 137 & 209 \\ 202 & 31 & 162 & 67 & 159 & 76 & 5 & 117 & 156 & 163 & 249 & 62 & 193 & 29 & 169 & 150 \\ 187 & 57 & 226 & 189 & 141 & 85 & 91 & 66 & 68 & 24 & 117 & 109 & 199 & 108 & 224 & 83 \\ 126 & 236 & 118 & 190 & 173 & 148 & 149 & 35 & 21 & 59 & 248 & 176 & 5 & 132 & 100 & 222 \\ 247 & 230 & 224 & 201 & 212 & 0 & 231 & 137 & 43 & 251 & 118 & 87 & 179 & 230 & 231 & 97 \\ 212 & 73 & 90 & 156 & 41 & 108 & 241 & 42 & 62 & 147 & 39 & 93 & 114 & 231 & 102 & 182 \\ 54 & 23 & 85 & 48 & 211 & 253 & 249 & 131 & 135 & 210 & 212 & 119 & 5 & 24 & 121 & 79 \\ 229 & 37 & 225 & 196 & 235 & 2 & 172 & 113 & 94 & 88 & 192 & 100 & 56 & 107 & 156 & 0 \\ 184 & 244 & 252 & 74 & 119 & 203 & 231 & 175 & 244 & 143 & 202 & 175 & 36 & 155 & 230 & 114 \end{matrix} \quad (3.10)$$

On comparing (3.9) and (3.10), we find that the two cipher texts differ in 898 bits, out of 2048 bits, which is quite considerable. However, it may be mentioned here that, the impact of changing 1 bit is not that copious, as the size of the plain text is very large. Even then it is remarkable.

Now let us change the key K given in (3.6) by one binary bit. To this end, we replace the 60th element 5 by 4. Then on using the original plain text given by (3.3),

we get C in the form

$$C = \begin{matrix} 13 & 0 & 2 & 74 & 218 & 57 & 239 & 116 & 240 & 123 & 248 & 155 & 123 & 226 & 199 & 97 \\ 214 & 46 & 176 & 82 & 224 & 159 & 65 & 89 & 114 & 153 & 103 & 141 & 90 & 39 & 149 & 117 \\ 207 & 38 & 134 & 116 & 4 & 150 & 109 & 244 & 181 & 245 & 46 & 37 & 112 & 20 & 55 & 224 \\ 9 & 208 & 90 & 166 & 110 & 162 & 51 & 145 & 130 & 211 & 113 & 169 & 166 & 182 & 243 & 219 \\ 220 & 212 & 58 & 153 & 191 & 123 & 155 & 14 & 8 & 26 & 124 & 250 & 141 & 178 & 212 & 187 \\ 142 & 133 & 151 & 95 & 44 & 230 & 219 & 14 & 63 & 150 & 206 & 24 & 49 & 138 & 6 & 144 \\ 118 & 209 & 75 & 27 & 60 & 74 & 15 & 105 & 101 & 203 & 216 & 57 & 207 & 38 & 86 & 59 \\ 150 & 224 & 52 & 39 & 226 & 91 & 210 & 126 & 163 & 214 & 163 & 163 & 5 & 133 & 15 & 205 \\ 157 & 112 & 61 & 108 & 16 & 37 & 196 & 128 & 18 & 138 & 195 & 115 & 147 & 143 & 136 & 84 \\ 100 & 189 & 55 & 90 & 38 & 178 & 219 & 150 & 108 & 141 & 241 & 205 & 169 & 104 & 26 & 136 \\ 218 & 174 & 206 & 39 & 170 & 249 & 129 & 175 & 44 & 133 & 229 & 242 & 223 & 119 & 85 & 95 \\ 40 & 212 & 255 & 90 & 188 & 66 & 184 & 37 & 81 & 143 & 24 & 17 & 214 & 24 & 86 & 71 \\ 214 & 158 & 227 & 168 & 247 & 39 & 190 & 158 & 159 & 41 & 94 & 184 & 196 & 158 & 160 & 5 \\ 205 & 127 & 57 & 145 & 126 & 151 & 31 & 230 & 30 & 241 & 66 & 106 & 17 & 59 & 177 & 210 \\ 238 & 58 & 117 & 129 & 63 & 116 & 195 & 84 & 98 & 38 & 180 & 234 & 219 & 107 & 46 & 251 \end{matrix} \quad (3.11)$$

On comparing (3.9) and (3.11), we find that the cipher texts differ in 915 bits, out of 2048 bits

From the above analysis, we find that the avalanche effect is quite pronounced and shows very clearly that the cipher is a strong one.

4. Cryptanalysis

In the literature of cryptography, it is well known that the different types of attacks for breaking a cipher are:

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

In the first attack, the cipher text is known to us together with the algorithm. In this case, we can determine the plain text, only if the key can be found. As the key contains 64 decimal numbers, the key space is of size

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

which is very large. Hence, the cipher cannot be broken by applying the brute force approach.

We know that, the Hill cipher [1] can be broken by the known plain text attack, as there is a direct linear relation between C and P. But in the present modification, as we have all nonlinear relations in the iterative scheme, the C can never be expressed in terms of P, thus P cannot be determined by any means in terms of other quantities. Hence, this cipher cannot be broken by the known plain text attack.

As there are three relations, which are typical in nature, in the iterative process for finding C, no special choice of either the plain text or the cipher text or both can be conceived to break the cipher.

5. Conclusions

In the present paper, we have developed a large block cipher by modifying the Hill cipher. In the case of the Hill cipher, it is governed by the single, linear relation

$$\mathbf{C = (K\ P)\ mod\ 26}, \quad (5.1)$$

while in the present case, the cipher is governed by an iterative scheme, which includes the relations

$$\mathbf{P = (K\ P\ K)\ mod\ 256}, \quad (5.2)$$

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

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

Further, it is followed by $\mathbf{C = P}$ (5.5)

In the case of the Hill cipher, we are able to break the cipher as there is a direct linear relation between C and P. On the other hand, in the case of the present cipher, as we cannot obtain a direct relation between C and P, this cipher cannot be broken by the known plain text attack.

By decomposing the entire plain text given by (3.1) into blocks, wherein each block is of size 256 characters, the corresponding cipher text can be obtained in the decimal form. The first block is already presented in (3.9) and the rest of the cipher text is given by

185	14	96	57	33	156	10	74	214	184	19	44	237	13	121	141
157	250	120	112	34	186	172	9	89	206	225	222	59	115	173	136
30	181	147	17	186	218	133	206	47	55	79	64	113	114	218	70
106	93	172	169	102	146	109	190	49	150	211	208	39	112	3	191
154	131	34	159	83	47	154	232	44	156	122	78	253	61	184	98
166	122	142	238	193	253	202	250	43	137	116	45	70	197	245	52
40	44	78	134	13	38	123	162	194	198	210	191	247	248	144	234
78	104	122	55	244	183	248	240	99	91	160	212	66	244	85	197
137	169	82	213	145	176	103	211	19	15	226	208	154	192	241	92
17	101	116	186	230	110	63	238	183	118	126	148	17	3	202	117
162	54	8	58	190	226	244	214	254	99	125	39	197	200	112	108
90	232	19	216	95	226	25	133	180	56	190	121	247	209	174	60
71	134	138	47	69	232	67	136	63	208	50	145	35	188	81	126
165	182	219	38	135	174	69	215	192	253	164	76	91	168	214	26
96	9	88	227	107	140	131	82	59	148	1	171	235	9	203	97
32	14	122	27	122	90	225	6	140	48	17	115	172	106	125	234

In this analysis, the length of the plain text block is 2048 bits and the length of the key is 512 bits. As the cryptanalysis clearly indicates, this 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 [5]

REFERENCES:

1. Feistel H, "*Cryptography and Computer Privacy*", Scientific American, May1973.
2. Feistel H, Notz W, Smith J, "*Some Cryptographic Techniques for Machine-to- Machine Data Communications*", Proceedings of the IEEE, Nov. 1975.
3. William Stallings, *Cryptography and Network Security*, Principles and Practice, Third Edition, Pearson, 2003.
4. Daemen J, Rijmen V, "*Rijdael: The Advanced Encryption Standard*", Dr. Dobb'sJournal, March 2001.
5. V. U. K. Sastry, V. Janaki, "*On the Modular Arithmetic Inverse in the Cryptology of Hill Cipher*",Proceedings of North American Technology and Business Conference, Sep. 2005, Canada.

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

7. V. U. K. Sastry, V. Janaki, "*A Block Cipher Using Linear Congruences*", Journal of Computer Science 3(7), 556 – 561, 2007.

8. 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.

9. V. U. K. Sastry, D. S. R. Murthy, S. Durga Bhavani, "*A Block Cipher Involving a Key Applied on Both the Sides of the Plain Text*", Sent for publication.