A MODERN ADVANCED HILL CIPHER INVOLVING A PAIR OF KEYS, XOR OPERATION AND SUBSTITUTION

Aruna Varanasi¹, V.U.K.Sastry ² and S.Udaya Kumar³

¹Department of computer Science and Engineering,SNIST
Hyderabad, India,
varanasi.aruna2002@gmail.com

²Department of computer Science and Engineering,SNIST
Hyderabad, India,
vuksastry@rediffmail.com

³Department 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, XOR operation, mixing and substitution. All these additional features are expected to strengthen the cipher as the plaintext undergoes several transformations which are causing confusion and diffusion. From the avalanche effect and the cryptanalysis carried out in this investigation, we have noticed that this cipher is a strong one, and it can be utilized effectively for the transmission of information in a secured manner.

Keywords: symmetric block cipher, cryptanalysis, avalanche effect, ciphertext, pair of keys, involutory matrix, XOR operation., mixing, substitution.

INTRODUCTION

In a recent investigation [1], we have devoted our attention to the study of a modern advanced Hill cipher involving a pair of keys. In this, we have introduced modular arithmetic addition operation, mixing and substitution in each round of the iteration process. The basic equations governing this cipher are

\[
C = (AP + B) \mod N, \quad (1.1)
\]

and

\[
P = (A (C - B)) \mod N, \quad (1.2)
\]

where \( P \) is a plaintext matrix, \( A \) and \( B \) are square matrices of size \( n \), \( N \) a positive integer, chosen appropriately, and \( C \) is the corresponding ciphertext matrix. In this analysis, matrices \( A \) and \( B \) are involutory matrices, which include the pair of keys \( K \) and \( L \) respectively.

Here it is to be noted that an involutory matrix is a matrix whose arithmetic inverse is the same as the matrix itself. The equations that are required for obtaining \( A \) are given by

\[
A^{-1} = A, \quad (1.3)
\]

\[
(A A^{-1}) \mod N = I, \quad (1.4)
\]

\[
A^2 \mod N = I, \quad (1.5)
\]

\[
A = \begin{bmatrix}
A_{11} & A_{12} \\
A_{21} & A_{22}
\end{bmatrix}, \quad (1.6)
\]

\[
A_{11} = K, \quad (1.7)
\]

\[
A_{22} = - K, \quad (1.8)
\]

where \( A^{-1} \) is the arithmetic inverse of \( A \), \( I \) the identity matrix, \( d \) a chosen positive integer and \( \lambda \) is determined from (1.11). Similar equations can be obtained for obtaining \( B \) (see [1]).

In order to have a detailed discussion concerned to the relations for obtaining an involutory matrix, we refer to [2].

In the present paper our objective is to develop a variant of the modern advanced Hill cipher, discussed in [1], by replacing the addition operation with XOR operation. The relations governing the block cipher that we are going to develop in this analysis are

\[
C = (A \oplus B) \mod N, \quad (1.12)
\]

and

\[
P = (A(C \oplus B)) \mod N. \quad (1.13)
\]

where \( A \), \( B \), \( C \) are matrices of size \( n \) and \( N \) a positive integer, chosen appropriately. In this analysis also we have included the iteration process, the functions \( \text{mix}() \) and \( \text{substitute}() \) in each round of the iteration. All these features together with the XOR operation are expected to strengthen the cipher significantly.

In this analysis also we have included the iteration process, the functions \( \text{mix}() \) and \( \text{substitute}() \) in each round of the iteration. All these features together with the XOR operation are expected to strengthen the cipher significantly.

Let us now put forth the plan of the paper. In section 2, we have introduced the development of the cipher, and presented the flowcharts and algorithms for encryption and decryption. In section 3, we have illustrated the cipher and mentioned the avalanche effect. Section 4 is devoted to cryptanalysis. Finally in section 5, we have discussed the computations and drawn conclusions.
DEVELOPMENT OF THE CIPHER

In the development of this cipher, the plaintext $P$, the pair of keys $K$ and $L$ (basing upon which the involutory matrices $A$ and $B$ are found), and the ciphertext $C$ are given by the relations

\[ P = [P_{ij}], \quad i=1 \text{ to } n, \quad j=1 \text{ to } n, \quad (2.1) \]
\[ K = [K_{ij}], \quad i=1 \text{ to } n/2, \quad j=1 \text{ to } n/2, \quad (2.2) \]
\[ L = [L_{ij}], \quad i=1 \text{ to } n/2, \quad j=1 \text{ to } n/2, \quad (2.3) \]
\[ C = [C_{ij}], \quad i=1 \text{ to } n, \quad j=1 \text{ to } n. \quad (2.4) \]

Here $n$ is an even positive integer and each element of $P$, $K$, $L$ and $C$ are decimal numbers, lying in $[0, 255]$, as we have made use of EBCDIC code.

On using the keys $K$ and $L$, and taking $N=256$, the involutory matrices $A$ and $B$ can readily be found by using the relations, mentioned in section 1 (see (1.3) to (1.11)).

As we have already pointed out in section 1, the relations governing the encryption and the decryption are (1.12) and (1.13). In what follows, we present the flowcharts and the algorithms.

**Algorithm for Encryption**

1. Read $n,P,K,L,r,d,e$
2. $A = \text{involute}(K,d)$
   $B = \text{involute}(L,e)$
3. Construct matrices $E,S$
4. for $i = 1 \text{ to } r$
   \begin{verbatim}
   P = (A P \oplus B) \mod 256
   P = \text{mix}(P)
   P = \text{substitute}(P,E,S)
   \end{verbatim}
5. Write $C$

**Algorithm for Decryption**

1. Read $n,C,K,L,r,d,e$
2. $A = \text{involute}(K,d)$
   $B = \text{involute}(L,e)$
3. Construct matrices $E,S$
4. for $i = 1 \text{ to } r$
   \begin{verbatim}
   C = \text{substitute}(C,E,S)
   C = \text{mix}(C)
   C = (A(C \oplus B)) \mod 256
   \end{verbatim}
5. Write $P$

In this analysis, we have denoted the number of rounds as $r$, and it is taken as 16. The $d$ and $e$ are positive integers which are chosen in finding the involutory matrices $A$ and $B$. The function involute() is used for obtaining the involutory matrix.

The functions mix() and substitute() used in the encryption algorithm can be mentioned as follows:

At each stage of the iteration process, the matrix $P$ is of size $n \times n$. It can be written in the form of four binary strings, wherein each string has $2n^2$ binary bits as shown below:

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

On mixing these strings, we get a single string given by

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

On taking 8 bits at a time, the above string, containing $8n^2$ binary bits can be written in the form of a square matrix of size $n$.

Let us now develop the process of substitution. We know that the EBCDIC code, requires the numbers 0-255 for the representation of the characters. These numbers can be written in the form of a matrix $E$ given by

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

Let us now see the development of the substitution table consisting of 16 rows and 16 columns. In order to achieve this one, let us firstly fill up the first two columns of the table with the elements of the keys $K$ and $L$ in order. Then rest of the table is filled with the remaining elements of $E$, in order in a row wise manner, excluding the numbers contained in $K$ and $L$. This process yields the substitution table. This table can be represented in the form of a substitution matrix denoted by $S(i,j)$.

For a detailed discussion of the process of substitution, we refer to [1].
It may be noted here that the functions $\text{Imix()}$ and $\text{Isubstitute()}$, used in the decryption algorithm, are obtained by reversing the processes of $\text{mix()}$ and $\text{substitute()}$.

**ILLUSTRATION OF THE CIPHER**

Consider the plaintext given below:

“Hello X! I am waiting for your email. I have already completed my B. Tech. examinations very well. My father is compelling me to do IAS, and to become a collector in this country. It is unfortunate! When are you completing your PhD program? I would like to come to you and finish there my MS. What about our marriage? I am waiting for your reply.”

(3.1)

Let us now consider the first sixty four characters of the plaintext given by (3.1). Thus we have

“Hello X! I am waiting for your email. I have already completed m”   (3.2)

On using the EBCDIC code, (3.2) can be written in the form

$$P = \begin{bmatrix}
200 & 133 & 147 & 147 & 150 & 64 & 231 & 79 \\
64 & 201 & 64 & 129 & 148 & 64 & 166 & 129 \\
137 & 163 & 137 & 149 & 135 & 64 & 134 & 150 \\
153 & 64 & 168 & 150 & 164 & 153 & 64 & 133 \\
148 & 129 & 137 & 147 & 75 & 64 & 201 & 64 \\
136 & 129 & 165 & 133 & 64 & 129 & 147 & 153 \\
133 & 129 & 132 & 168 & 64 & 131 & 150 & 148 \\
151 & 147 & 133 & 163 & 133 & 132 & 64 & 148
\end{bmatrix}$$

(3.3)

Let us choose the keys $K$ and $L$ in the form

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

(3.4)

and

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

(3.5)

Let us now construct the involutory matrices $A$ and $B$ by adopting the process mentioned in section 1 (see (1.3) - (1.11). In obtaining $A$ and $B$, we have taken $d = 99$ and $e = 189$ respectively. Thus we get

$$A = \begin{bmatrix}
69 & 124 & 27 & 167 & 180 & 12 & 143 & 107 \\
135 & 79 & 99 & 111 & 203 & 214 & 183 & 19 \\
248 & 199 & 209 & 75 & 24 & 11 & 144 & 255 \\
239 & 45 & 255 & 92 & 147 & 153 & 99 & 207 \\
130 & 84 & 233 & 237 & 187 & 132 & 229 & 89 \\
141 & 112 & 1 & 133 & 121 & 177 & 157 & 145 \\
168 & 77 & 134 & 249 & 8 & 57 & 47 & 181 \\
95 & 47 & 181 & 63 & 17 & 211 & 1 & 164
\end{bmatrix}$$

(3.6)

and

$$B = \begin{bmatrix}
215 & 113 & 19 & 147 & 2 & 147 & 249 & 121 \\
223 & 109 & 254 & 12 & 93 & 68 & 122 & 36 \\
56 & 1 & 127 & 174 & 168 & 67 & 250 & 138 \\
59 & 146 & 189 & 81 & 113 & 54 & 119 & 240 \\
184 & 197 & 15 & 143 & 41 & 143 & 237 & 109 \\
203 & 6 & 214 & 252 & 33 & 147 & 2 & 244 \\
152 & 149 & 128 & 70 & 200 & 255 & 129 & 82 \\
87 & 250 & 1 & 186 & 197 & 110 & 67 & 175
\end{bmatrix}$$

(3.7)

As we have mentioned in section 2, the substitution matrix $S$ can be written in terms of Table 1.

On using (3.3), (3.4), and (3.5), and the encryption algorithm (which uses the substitution process), we get

$$C = \begin{bmatrix}
9 & 204 & 21 & 245 & 209 & 19 & 10 & 192 \\
202 & 15 & 30 & 64 & 115 & 112 & 75 & 180 \\
128 & 157 & 223 & 223 & 114 & 195 & 241 & 185 \\
152 & 12 & 38 & 108 & 70 & 94 & 145 & 233 \\
208 & 153 & 64 & 199 & 251 & 56 & 53 & 27 \\
40 & 143 & 184 & 154 & 226 & 19 & 152 & 41 \\
84 & 198 & 231 & 32 & 157 & 102 & 102 & 137 \\
126 & 144 & 115 & 68 & 74 & 90 & 176 & 70
\end{bmatrix}$$

(3.8)

On adopting the decryption algorithm, with the required inputs, it can be readily verified that we get back the original plaintext given by (3.3).

Let us now examine the avalanche effect, which gives an idea about the quality of the cipher.

To this end, in the plaintext (3.2), we replace the 18th character ‘t’ by ‘s’. As the EBCDIC codes of ‘t’ and ‘s’ are 163 and 162, they differ by one bit in their binary form. Now, on using the modified plaintext along with (3.4) and (3.5), and applying the encryption algorithm, we have the ciphertext $C$ in the form
On converting (3.8) and (3.9), in to their binary form, and comparing the corresponding strings, we notice that the two ciphertexts differ by 271 bits (out of 512 bits). This shows that the strength of the cipher is expected to be up to the mark.

Let us now focus our attention on one bit change in one of the keys, say key $K$. To achieve this one we change the 2nd row 1st column element of the key $K$, given by (3.4), from 135 to 134. On using the original plaintext (3.3), the modified key $K$, keeping the other key $L$ intact, and using the encryption algorithm, we get

Now on comparing (3.8) and (3.10) in their binary form, we find that they differ by 278 bits (out of 512 bits). This also shows that the strength of the cipher is considerable.

In what follows, let us now consider the cryptanalysis, which exhibits more firmly about the strength of the cipher.

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

Table 1: Substitution Table.

<table>
<thead>
<tr>
<th>9</th>
<th>18</th>
<th>203</th>
<th>50</th>
<th>195</th>
<th>232</th>
<th>67</th>
<th>144</th>
</tr>
</thead>
<tbody>
<tr>
<td>235</td>
<td>242</td>
<td>235</td>
<td>148</td>
<td>117</td>
<td>141</td>
<td>72</td>
<td>219</td>
</tr>
<tr>
<td>93</td>
<td>167</td>
<td>93</td>
<td>158</td>
<td>76</td>
<td>0</td>
<td>180</td>
<td>57</td>
</tr>
<tr>
<td>233</td>
<td>17</td>
<td>69</td>
<td>191</td>
<td>173</td>
<td>63</td>
<td>163</td>
<td>3</td>
</tr>
<tr>
<td>189</td>
<td>175</td>
<td>189</td>
<td>104</td>
<td>206</td>
<td>7</td>
<td>152</td>
<td>51</td>
</tr>
<tr>
<td>39</td>
<td>180</td>
<td>135</td>
<td>138</td>
<td>134</td>
<td>76</td>
<td>26</td>
<td>34</td>
</tr>
<tr>
<td>162</td>
<td>111</td>
<td>132</td>
<td>214</td>
<td>230</td>
<td>145</td>
<td>199</td>
<td>255</td>
</tr>
<tr>
<td>223</td>
<td>131</td>
<td>138</td>
<td>119</td>
<td>187</td>
<td>131</td>
<td>89</td>
<td>94</td>
</tr>
</tbody>
</table>

C =

\[
\begin{pmatrix}
9 & 18 & 203 & 50 & 195 & 232 & 67 & 144 \\
235 & 242 & 235 & 148 & 117 & 141 & 72 & 219 \\
93 & 167 & 93 & 158 & 76 & 0 & 180 & 57 \\
233 & 17 & 69 & 191 & 173 & 63 & 163 & 3 \\
189 & 175 & 189 & 104 & 206 & 7 & 152 & 51 \\
39 & 180 & 135 & 138 & 134 & 76 & 26 & 34 \\
162 & 111 & 132 & 214 & 230 & 145 & 199 & 255 \\
223 & 131 & 138 & 119 & 187 & 131 & 89 & 94
\end{pmatrix}
\]

(3.9)

C =

\[
\begin{pmatrix}
64 & 149 & 123 & 14 & 122 & 220 & 136 & 86 \\
92 & 48 & 64 & 65 & 52 & 38 & 97 & 124 \\
122 & 42 & 193 & 20 & 165 & 158 & 150 & 241 \\
186 & 233 & 224 & 199 & 72 & 98 & 53 & 149 \\
34 & 213 & 182 & 72 & 31 & 70 & 219 & 126 \\
111 & 34 & 134 & 47 & 50 & 155 & 137 & 225 \\
1 & 188 & 232 & 137 & 83 & 28 & 134 & 214 \\
25 & 202 & 28 & 121 & 209 & 17 & 222 & 234
\end{pmatrix}
\]

(3.10)

On converting (3.8) and (3.9), in their binary form, and comparing the corresponding strings, we notice that the two ciphertexts differ by 271 bits (out of 512 bits). This shows that the strength of the cipher is expected to be up to the mark.
CRYPTANALYSIS

The different types of cryptanalytic attacks which are generally considered in the literature of Cryptography are

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

The key matrices K and L, involved in this analysis, contain 16 decimal numbers each. The constants d and e, which are chosen at our will in the construction of the involutory matrices A and B, are two more decimal numbers. In view of these facts, the total length of the keys is 34 decimal numbers, that is 272 binary bits. Hence the size of the key space is

\[ 2^{272} = \left(10^3\right)^{27.2} = 10^{81.6}. \]

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

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

As this number is very large, we can firmly say that this cipher cannot be broken by the brute force attack.

Let us now consider the known plaintext attack. In this we know as many pairs of the plaintext and the ciphertext as we desire. In the development of this cipher as we have an iterative process, which involves a pair of keys, functions mix() and substitute(), and XOR operation, at the end of the iteration process, the relation between the plaintext and the ciphertext can be viewed as shown below

\[ C = \Psi \left( M \left( (A \Psi \left( M \left( \ldots \Psi \left( M \left( (A \Psi \left( (A \oplus B) \mod 256 \right) \oplus B \right) \mod 256 \right) \ldots \right) \mod 256 \right) \right) \right) \right) \]  

In writing (4.1), the function mix() and the function substitute() are represented as M and \( \Psi \) for simplicity and elegance. Here we notice that the equation (4.1) cannot be written in the form

\[ C = F(A, B, M, \Psi) P \]  

where F is a function, depending upon K,L,M and \( \Psi \). This amounts to that we cannot find a direct relation between C and P as we could do in the case of the classical Hill cipher. Thus this cipher cannot be broken by the known plaintext attack.

The last two cases of cryptanalysis, namely chosen plaintext attack and chosen ciphertext attack are very complicated, and hence we leave them at the present stage.

In the light of the above discussion we conclude that this cipher is a strong one.

COMPUTATIONS AND CONCLUSIONS

In this investigation, we have developed a block cipher, called modern advanced Hill cipher, which includes a pair of keys, XOR operation and functions mix() and substitute(). In this cipher the computations are carried out by writing programs for encryption and decryption in Java.

The plaintext (3.1) is divided into 6 blocks, wherein each block is containing 64 characters. Nevertheless, as the last block is containing only 26 characters, it is supplemented with 38 blank characters so that it becomes a complete block. On using the encryption algorithm the ciphertext corresponding to the entire plaintext (3.1) is obtained in the form
The avalanche effect and the cryptanalysis, considered in sections 3 and 4, clearly indicate that the cipher is a strong one and it cannot be broken by any cryptanalytic attack. This generalization of the advanced Hill cipher is markedly an interesting one, and it can be applied comfortably for the transmission of information in a secured manner.

REFERENCES


© JGRCS 2011, All Rights Reserved