An Improved RSA based on Double Even Magic Square of order 32

Shahla Uthman Umar-college of science- University of Kirkuk
Shahla_umar@uokirkuk.edu.iq
Shahla_aothman@yahoo.com

[Abstract]

Because of the computers systems discovery and the use of computer networks between countries, security is very important to transfer confidential information over the networks; traditional cryptographic systems such as Rivest-Shamir-Adlemen (RSA) are depend on guesswork as well as mathematics. Information theory illustrates that conventional cryptographic systems cannot be regarded fully secure unless the private key; which it is used once only; is at least as long as the plain text. And another limitation is using ASCII value to represent the plaintext, So the repetition of characters in the plain text will appear in the cipher text therefore we have given approach to generate magic square of order 32 which cannot be easily traced and use this square in the cryptography which it is used to improve efficiency through providing an additional level of security to encryption. Through of the characteristics of magic squares, and it’s some complex conditions (non-repetition property), these squares generates a huge numbers of non-duplicate random numbers which can be used to represent the numerals rather than ASCII values as well as the magic square is also used to generate the keys for public key encryption algorithms.

[Keywords: Magic Square, RSA, Public Key Cryptosystem, Encryption algorithm, key.]

تحسين خوارزمية التشفير RSA باستخدام المربعات السحرية الفردية المزدوجة ذات المرتبة 32

Web Site: www.kujss.com  Email: kirkukjournsci@yahoo.com, kirkukjournsci@gmail.com
الملخص

بسبب اكتشاف أنظمة الحواسيب واستخدام شبكات الحاسوب بين البلدان، فإن البيانات مهددة من قِبَل

العوامل المتنوعة، وأكثر أنظمة التشفير التقليدية مثل (RSA) تعتمد على التخمين بالإضافة إلى

الرياضيات. توضح نظرية المعلومات أن أنظمة التشفير التقليدية لا يمكن اعتبارها آمنة تمامًا إلا إذا كان المفتاح الخاص

والتي يتم استخدامها مرة واحدة فقط على الأقل بطول النص السري، ومن الفقود الأخرى في هذه الطرق هو استخدام

قيمة (ASCII) لتمثيل النص الاصلي، وبالتالي فإن تكرار الأحرف في النص الاصلي سوف تظهر في النص المشفر

لذلك اقترحنا طريقة جديدة لتوليد المربعات السريعة ذات المرتبة 32 والتي لا يمكن تتبعها والتنبيه بقينها بسهولة.

والمربعة هذه المربعات في التشفير والذي يستخدم لتحسين كفاءة التشفير من خلال توفير مستوى إضافي من الأمان.

من خلال خصائص المربعات السحرية، وبعض شروطها المعقدة (مثل خاصية عدم التكرار للقيم)، هذه المربعات تولد

أعدادًا كبيرة من الأرقام العشوائية غير المكررة والتي يمكن استخدامها لتمثيل الأرقام بدلاً من القيم

المربعة السحرية تستخدم أيضاً لتوليد مفاتيح خوارزميات التشفير بال}@{

الأعمال المفتاحية: - المربع السحري، نظام التشفير بالمفتاح العام، خوارزمية التشفر، [ ]

المفتاح

1. Introduction

Cryptography pointed completely on encryption, which is the process of transforming original information (plaintext) into unreadable text (cipher text), while

Web Site: www.kujss.com Email: kirkukjoursci@yahoo.com,
kirkukjoursci@gmail.com
decryption is the inverse, Converting from the unreadable cipher text back to plaintext. In cipher, there are two algorithms, the encryption and the reversing decryption [1].

There are two kinds of cryptosystems, symmetric and asymmetric. In asymmetric systems there are two keys, the first one (public key) is used to encrypt a message while the second one (private key) is used to decrypt it, therefore these systems increase the security of communication [1]. An example of asymmetric systems is RSA. The security of several cryptographic systems relates with the creation of unexpected elements like the secret key in the DES algorithms, the key stream in the one-time pad and the prime P, and Q in the RSA encryption. In every these instances, the keys made must be sufficient in size and the arbitrary. However, RSA is not completely secure or secure against chosen cipher text attacks. If all variables are selected in such a way that it's impossible to compute the private key (d) from the public key (n, e), or choosing P, Q are incredibly large. Even if the above variables were selected carefully, none of the computational problems are completely guaranteed enough [2]. To encrypt the clear message characters, their ASCII values are taken which is possible that the same cipher text is produced for the characters which occur in several positions in the plaintext. To eliminate this problem, this paper attempts to improve a method with "doubly even magic squares (DEMS)" of order 32 (32 ×32) which equals to 1024 different values and dividing this magic square to different corresponding ASCII tables (each table is 128 ASCII characters). Thus, instead of taking the ASCII values of the characters to encrypt, different numerals representing the location of ASCII values in the magic square are taken and also using the same magic square to select two prime numbers (P and Q) which is used to generate the public key (e, n) then these numerals are encrypted using "RSA cryptosystem".

2. Related Work

Web Site: www.kujss.com Email: kirkukjoursci@yahoo.com, kirkukjoursci@gmail.com
As the intruder has the chance of finding the public key value (e), then finding the decryption key (d) value directly and decrypts the cipher text, "Amare Anagaw Aycle and Vuda Sreenivasarao" [3] suggested an efficient representation of RSA algorithm by applying mathematical logics on two public keys rather than sending the public key (e) in RAS algorithm. While "Gopinath Ganapathy and K Mani" [4] suggested a new layer of security to public key algorithm by providing more security to the cryptosystem using magic squares idea. In July 2012 Sonia Goyat[5] proposed a new algorithm by applying the genetic algorithm to cryptography and alter the algorithm to generate more powerful keys and also the random values, which it is used to generate keys, are unique. Then A new algorithm "Modified Subset-Sum cryptosystem over RSA" was presented by Sonal Sharma, Saroj Hiranwal, Prashant Sharma[6] which it is secured against Shamir attacks on RSA as well as various sorts of Mathematical attacks. And in January of the same year Prasant Sharma, Amit Kumar Gupta et al [7] studied the rapidity of RSA public key cryptosystem to decline the time taken for finding factor for a huge number. They suggested a new algorithm and its output was compared with "Fermats factorization Algorithm and trial division algorithm".

3. Proposed Methodology

The Improved RSA based on Double Even Magic Square (DEMS) is:-

Step 1:- Generate Doubly Even Magic Square of order 32 (32 × 32 ) which contains totally 1024 values and divide it to eight different quadrants each consists of 128 characters. Each different quadrant corresponds to one ASCII set (128 characters).

Step 2:- For every letter in the plain text, the numerals corresponding to its position in different quadrants of magic square are taken then these numerals are encrypted and decrypted using RSA public key cryptosystem.
Step 3:-Use the same magic square to select two prime numbers P and Q which is used to find the public key in RSA, from the range (1-1024) two numbers are selected randomly and then from this limit any two prime number (p and q) are selected which cannot be trace because of their randomness. (figure 1)

3.1. Construction of Magic Square

Web Site: www.kujss.com Email: kirkukjoursci@yahoo.com, kirkukjoursci@gmail.com
"A magic square" of order n is a square array or an array of \( n^2 \) numbers which fulfils the condition that the sum of the elements of each row and column, as well as the main diagonals, is the same number which it is called the magic. Generally, the entries are thought of as the natural numbers 1, 2, ..., \( n^2 \), where each number is used exactly once. Magic Squares utilized to generate a huge number of random keys. The number of magic squares of order 4 (4x4) using the numbers from 1 to 16 and magic constant (34) is 880 magic square, magic squares of order 6 (6x6) or above require a huge amount of calculations where normal computer cannot be resolved, according to some estimates the number exceeds \((1.7745 \times 10^{19})\) through rotate rows and columns. The use of magic squares in data encryption gives more security because of the difficulty of magic squares analysis using frequency analysis, Or by using the principle of guesswork and the trial and error to decode the text [8]. "The magic constants for normal magic squares of orders \( n = 3, 4, 5, 6, 7, 8 \ldots \) are 15, 34, 65, 111, 175, 265... respectively".

\[
\text{Sum} = n \left( \frac{n^2 + 1}{2} \right)
\]

Magic squares are classified into three types: odd, doubly even and singly even [9]

3.2. Construction of Doubly Even Magic Squares

A doubly even magic square is a square matrix of order n, where n is divisible by four only, while a singly even magic square is a square matrix of order n, where n is even but not divisible by four. [9]

"A (4×4) magic square is a doubly even magic square, and one of the three types of magic square. The other two types are":

- \[ \text{odd} \] (where \( n=3, 5, 7, 9, 11 \), etc.)
In this paper we focused only on the implementation of doubly even magic square of order 32 (32 × 32) and their affect to enhance the public-key cryptosystem (RSA), to construct "doubly even magic squares", starting with the simplest (8×8). In 8 by 8 grids, in first step we write the numbers 1 through 64 from left to right (figure 2.a). Then "flip" the numbers in the diagonals (the red lines). That is to say, exchange 64 & 1, 55 & 10, ..., and 57 & 8 and 50 & 15 and so on, and we will have a magic square constant= 260 (figure 2.b). In the second step we divide 8 by 8 square into 4 blocks (each block is 4 by 4) then replace and flip the elements in the secondary diagnose of block 1 with the elements in the secondary diagnose of block 4 (gray cells) and replace and flip the elements in the main diagnose of block 2 with the elements in the main diagnose of block 3 (yellow cells)(figure 2.c)
With the same approach we construct a doubly even magic square of order 32 (Figure 3)
3.2. Algorithm of generating of Doubly Even magic square:

Figure 3: Doubly Even Magic Square of order 32
4. Experiments and Results

Web Site: www.kujss.com   Email: kirkukjoursci@yahoo.com, kirkukjoursci@gmail.com
1. Magic Square of order 4 is first generated using the proposed algorithm which satisfies the double even magic squares requirements with magic constant (34) (figure):

\[
\begin{array}{cccc}
16 & 2 & 3 & 13 \\
5 & 11 & 10 & 8 \\
9 & 7 & 6 & 12 \\
4 & 14 & 15 & 1 \\
\end{array}
\]

Figure 3: Double even magic square of order 4

2. with the same way, we construct magic square of order 8, 16, 32 with magic constant 260, 2056, 16400 respectively (figure 4) (figure 5) (magic square of order 32 shown in figure 3) :-

\[
\begin{array}{cccccccc}
64 & 2 & 3 & 61 & 60 & 6 & 7 & 57 \\
9 & 55 & 54 & 12 & 13 & 51 & 50 & 16 \\
17 & 47 & 46 & 20 & 21 & 43 & 42 & 24 \\
40 & 26 & 27 & 37 & 36 & 30 & 31 & 33 \\
32 & 34 & 35 & 29 & 28 & 38 & 39 & 25 \\
41 & 23 & 22 & 44 & 45 & 19 & 18 & 48 \\
56 & 10 & 11 & 53 & 52 & 14 & 15 & 49 \\
8 & 58 & 59 & 5 & 4 & 62 & 63 & 1 \\
\end{array}
\]

Figure 4: Double even magic square of order 8
<table>
<thead>
<tr>
<th>256</th>
<th>2</th>
<th>3</th>
<th>253</th>
<th>252</th>
<th>6</th>
<th>7</th>
<th>249</th>
<th>248</th>
<th>10</th>
<th>11</th>
<th>245</th>
<th>244</th>
<th>14</th>
<th>15</th>
<th>241</th>
</tr>
</thead>
<tbody>
<tr>
<td>17</td>
<td>239</td>
<td>238</td>
<td>20</td>
<td>21</td>
<td>235</td>
<td>234</td>
<td>24</td>
<td>25</td>
<td>231</td>
<td>230</td>
<td>28</td>
<td>29</td>
<td>227</td>
<td>226</td>
<td>32</td>
</tr>
<tr>
<td>33</td>
<td>223</td>
<td>222</td>
<td>36</td>
<td>37</td>
<td>219</td>
<td>218</td>
<td>40</td>
<td>41</td>
<td>215</td>
<td>214</td>
<td>44</td>
<td>45</td>
<td>211</td>
<td>210</td>
<td>48</td>
</tr>
<tr>
<td>208</td>
<td>50</td>
<td>51</td>
<td>205</td>
<td>204</td>
<td>54</td>
<td>55</td>
<td>201</td>
<td>200</td>
<td>58</td>
<td>59</td>
<td>197</td>
<td>196</td>
<td>62</td>
<td>63</td>
<td>193</td>
</tr>
<tr>
<td>192</td>
<td>66</td>
<td>67</td>
<td>189</td>
<td>188</td>
<td>70</td>
<td>71</td>
<td>185</td>
<td>184</td>
<td>74</td>
<td>75</td>
<td>181</td>
<td>180</td>
<td>78</td>
<td>79</td>
<td>177</td>
</tr>
<tr>
<td>81</td>
<td>175</td>
<td>174</td>
<td>84</td>
<td>85</td>
<td>171</td>
<td>170</td>
<td>88</td>
<td>89</td>
<td>167</td>
<td>166</td>
<td>92</td>
<td>93</td>
<td>163</td>
<td>162</td>
<td>96</td>
</tr>
<tr>
<td>97</td>
<td>159</td>
<td>158</td>
<td>100</td>
<td>101</td>
<td>155</td>
<td>154</td>
<td>104</td>
<td>105</td>
<td>151</td>
<td>150</td>
<td>108</td>
<td>109</td>
<td>147</td>
<td>146</td>
<td>112</td>
</tr>
<tr>
<td>144</td>
<td>114</td>
<td>115</td>
<td>141</td>
<td>140</td>
<td>118</td>
<td>119</td>
<td>137</td>
<td>136</td>
<td>122</td>
<td>123</td>
<td>133</td>
<td>132</td>
<td>126</td>
<td>127</td>
<td>129</td>
</tr>
<tr>
<td>128</td>
<td>130</td>
<td>131</td>
<td>125</td>
<td>124</td>
<td>134</td>
<td>135</td>
<td>121</td>
<td>120</td>
<td>138</td>
<td>139</td>
<td>117</td>
<td>116</td>
<td>142</td>
<td>143</td>
<td>113</td>
</tr>
<tr>
<td>145</td>
<td>111</td>
<td>110</td>
<td>148</td>
<td>149</td>
<td>107</td>
<td>106</td>
<td>152</td>
<td>153</td>
<td>103</td>
<td>102</td>
<td>156</td>
<td>157</td>
<td>99</td>
<td>98</td>
<td>160</td>
</tr>
<tr>
<td>161</td>
<td>95</td>
<td>94</td>
<td>164</td>
<td>165</td>
<td>91</td>
<td>90</td>
<td>168</td>
<td>169</td>
<td>87</td>
<td>86</td>
<td>172</td>
<td>173</td>
<td>83</td>
<td>82</td>
<td>176</td>
</tr>
<tr>
<td>80</td>
<td>178</td>
<td>179</td>
<td>77</td>
<td>76</td>
<td>182</td>
<td>183</td>
<td>73</td>
<td>72</td>
<td>186</td>
<td>187</td>
<td>69</td>
<td>68</td>
<td>190</td>
<td>191</td>
<td>65</td>
</tr>
<tr>
<td>64</td>
<td>194</td>
<td>195</td>
<td>61</td>
<td>60</td>
<td>198</td>
<td>199</td>
<td>57</td>
<td>56</td>
<td>202</td>
<td>203</td>
<td>53</td>
<td>52</td>
<td>206</td>
<td>207</td>
<td>49</td>
</tr>
<tr>
<td>209</td>
<td>47</td>
<td>46</td>
<td>212</td>
<td>213</td>
<td>43</td>
<td>42</td>
<td>216</td>
<td>217</td>
<td>39</td>
<td>38</td>
<td>220</td>
<td>221</td>
<td>35</td>
<td>34</td>
<td>224</td>
</tr>
<tr>
<td>225</td>
<td>31</td>
<td>30</td>
<td>228</td>
<td>229</td>
<td>27</td>
<td>26</td>
<td>232</td>
<td>233</td>
<td>23</td>
<td>22</td>
<td>236</td>
<td>237</td>
<td>19</td>
<td>18</td>
<td>240</td>
</tr>
<tr>
<td>16</td>
<td>242</td>
<td>243</td>
<td>13</td>
<td>12</td>
<td>246</td>
<td>247</td>
<td>9</td>
<td>8</td>
<td>250</td>
<td>251</td>
<td>5</td>
<td>4</td>
<td>254</td>
<td>255</td>
<td>1</td>
</tr>
</tbody>
</table>

Figure 5: Double even magic square of order 16
It is so difficult to determine the number of unique magic squares of different orders, but the number of unique magic squares of order n=1, 2, ... are 1, 0, 1, 880, 275305224. The 880 squares of order 4 were enumerated by "Frénicle de Bessy" in 1693, and are illustrated in Berlekamp (1982). "R. Schroeppel" in 1973 calculate the number of (5×5) magic squares[13], while the number of (6×6) squares is not identified, but "Pinn and Wieczerkowski (1998)" estimated it to be (1.7745(16)×1019) [14].

5. Example on RSA with double even Magic Square

RSA is implemented to illustrate the effect of using magic squares to enhance the security of public key encryption schemes. The secret key in the system consists of two prime numbers (P and Q) and an exponent (d) while the public key consists of the modulus N = P.Q and an exponent (e) where d = e⁻¹ mod (P-1) (Q-1). The user calculates C = Mᵉ mod (n) for encryption and M = Cᵈ mod (n) is done for decryption (for any message [11],[12].

In this paper, the modulus of N, M, and C should have a length of 512-1024 bits in order to prevent the known attacks. Using the above algorithm, we construct a "doubly even magic square" of order 32 which contains 1024 different (non repetition) values, as the characters set consists of 128 ASCII values, the magic square is divided logically into different 8 matrices each one with 128 values corresponding to individual ASCII character, for getting more realization of the proposed matter, we take an example, assume P=13, Q=17 and the public key (e) =11, then N=221, and (P-1).(Q-1)=192 .now the secret key(d) = 35 . To encrypt the message (A CAR), the ASCII values of A, C and R are 65, 67 and 82 respectively, so to encrypt A which appears in first and third position in the plain text, the numerals which appear at 65th position of first matrices and at 65th position of third matrices( figure 3 which is divided logically into 8 matrice) are taken respectively, Thus Nᵖ(A)=959 and 831, Nᵖ(C)=68 and Nᵖ(R) =942. And the cipher C(A)=959¹¹ mod 221=82, C(C)=68¹¹ mod 221=204, C(A)=831¹¹ mod 221=77, C(R)=942¹¹ mod 221=167 similarly we use this

Web Site: www.kujss.com Email: kirkukjoursci@yahoo.com, kirkukjoursci@gmail.com
substitution for every repeated character in the plaintext, therefore for each repeated character A, B, C,... (which appears more than once in the plain text), different cipher texts are generated.

6. The comparison between ordinary RSA algorithm and proposed RSA with Double Even Magic Square:

To illustrate the result of RSA algorithm with magic square, the plain text (MESSAGE) is first encrypted using existing RSA (if p=19, q=23, n=437, (p-1).(q-1)=396, e=13 then d=61) and the output is shown in Table 1. It is clear that the characters (E and S) appear twice in the plaintext, therefore in the ordinary RSA, the cipher text of them is the same (425), while in the suggested (RSA with DEMS), the cipher text value of the first (E) which is (397) is differ from the second (E) which it is (298) and the same thing with any repeated characters in the plaintext. This methodology is implemented in C#

Table 1. Comparison of cipher text

<table>
<thead>
<tr>
<th>Plain text</th>
<th>ASCII value</th>
<th>Cipher text</th>
<th>Plain text</th>
<th>MS value</th>
<th>Cipher text</th>
</tr>
</thead>
<tbody>
<tr>
<td>M</td>
<td>77</td>
<td>248</td>
<td>M</td>
<td>947</td>
<td>62</td>
</tr>
<tr>
<td>E</td>
<td>69</td>
<td>69</td>
<td>E</td>
<td>955</td>
<td>397</td>
</tr>
<tr>
<td>S</td>
<td>83</td>
<td>425</td>
<td>S</td>
<td>84</td>
<td>350</td>
</tr>
<tr>
<td>S</td>
<td>83</td>
<td>425</td>
<td>S</td>
<td>212</td>
<td>90</td>
</tr>
<tr>
<td>A</td>
<td>65</td>
<td>122</td>
<td>A</td>
<td>959</td>
<td>348</td>
</tr>
<tr>
<td>G</td>
<td>71</td>
<td>211</td>
<td>G</td>
<td>72</td>
<td>124</td>
</tr>
<tr>
<td>E</td>
<td>69</td>
<td>69</td>
<td>E</td>
<td>827</td>
<td>298</td>
</tr>
</tbody>
</table>
7. Conclusion

This work prevents any hacker from getting the plain text in a readable form even if they obtained the keys because of using the numerical values of magic square rather than the ASCII values of characters (rather than of unique ASCII table, 8 tables with various set of values are used). It is unsolved problem to determine the number of magic squares of order 32 which is used in this paper. The security aspect of RSA is improved because there are no duplicated values in Magic Squares. In the ordinary RSA, the same cipher text values are generated whenever the same characters are repeated in the plain text, while in the proposed (RSA with DEMS) different values are produced in the cipher text for each occurrence of the same character in the plain text. It plays an important role in increasing the randomness and security of the algorithm. One of the issues in the proposed work is additional time needed for the construction of Magic squares initially.

REFERENCES
Web Site: www.kujss.com  Email: kirkukjoursci@yahoo.com, kirkukjoursci@gmail.com


Department of Physics and Astronomy, University of Manitoba, Winnipeg, Manitoba, Canada R3T 2N2, 19 July 2012