A Cryptosystem Design with Recursive Key Generation Techniques

S.G.Srikantaswamy¹, H.D.Phaneendra², ¹*

¹National Institute of Engineering, Mysore, Karnataka, India
²Department of Computer Science and Engineering, NIE, Mysore, Karnataka, India

Abstract

Communication is a basic process of exchanging information. It involves sender, receiver and the channel. Information security is a very important aspect now a day. The introduction of internet and distributed system made the information security issue more challenging and complex. Cryptography plays a crucial role in providing security to data transmitted over the internetwork. Encryption is the most widely used technique used to scramble the data that is being transmitted over the network from sender to a receiver. The encryption algorithms are available practically and provide the security for user data and information. This paper presents an advanced encryption technique which combines the features of substitution and transposition. Five different key values being used in this algorithms and each key value is used to substitute the corresponding plaintext characters in association with addition operation. Each key value is twice as that of the previous one. The basic key value is a fixed one defined by the user. The transposition technique is employed by left shifting each bit of the data. The shifted data is complemented to alter the each bit of the cipher text that is being generated. The effort of the algorithm is to make the cryptanalysis difficult and to make the algorithm stronger.

© 2011 Published by Elsevier Ltd. Selection and/or peer-review under responsibility of ICCTSD 2011

Keywords: Cryptosystem; Information Security; Plaintext; Cipher text; Encryption; Decryption; Key; Cipher; Substitution; Transposition.

1. Introduction

Encryption is a technique of scrambling the original data to be transmitted. Decryption is a process of converting the scrambled data to original format. The original data is referred as plaintext and the scrambled data is called cipher text. The nonlinearity property play a important role in block cipher design[1]. The role of key is very important in encrypting and decrypting the data to be transmitted [2]. Many encryption and decryption algorithms are widely available and being used for encrypting and decrypting the data [6, 7]. Many encryption algorithm incorporates both substitution and transposition techniques [3, 4, 5]. Substitution cipher involves the replacing one or more characters in a message with one or more other entities may be other characters, symbols and numbers. There are several types of substitution ciphers available in the field of network security [6]. Mono alphabetic substitution involves replacing each character or letter in the given message with another character of the alphabet. Polyalphabetic substitution involves the following features:

- A set of related monoalphabetic substitution rules is used.
- A key determines which particular rule is chosen for a given transformation.

The best known such algorithm is referred to as the vigenere cipher [6]. Here, an encryption algorithm which incorporates the techniques of both substitution and transposition technique with effective key generation technique is proposed. To encrypt a message, a key value K is assumed. The first character of the message is added with the key value. The resultant value is then right shifted once. The right shifted value is then complemented. The resultant complemented value is the

The organization of the paper is as follows: Section 2 provides the complete encryption process details. Section 3 gives encryption algorithm details. Section 4 gives encryption and decryption results. Section 5 provides the features of the proposed scheme and Section 6 provides conclusions drawn from the analysis carried out on the above desired encryption and decryption algorithm. Section 7 contains references.

### 2. Encryption process

Consider a plaintext message say “ENCRYPTION”. Let the key be \( K \). Now the different versions of key values are derived using recursion method. Consider the first character of the plaintext message \( P[0] \). Let the key value used to substitute the first character be \( K[0] \), initial value to be assumed. For the subsequent plaintext characters \( P[i] \), the key value to be used is \( K[i] \), where \( 1 \leq i \leq n \). The first plaintext character is added with key value \( K[0] \). The initial key value is selected by the communicating entities. The key value is added to plaintext character. The resultant value is right shifted once. The shifted value of the plaintext is complemented to obtain the final ciphertext value for corresponding value of the plaintext. Now for the next plaintext character say \( P[1] \), the key value used will be \( K[1]=K[0]+K[0] \). For the subsequent plaintext characters, the key value is used \( K[i]=K[i-1]+K[i-1] \). The above procedure is repeated to obtain \( C_2 \). Similarly to obtain \( C_3 \) from \( P_3 \), the key value used will be \( K[3]=K[2]+K[2] \), for \( C_4 \), key \( K[4]=K[3]+K[3] \), and finally for \( C_i \), key \( K[i]=K[i-1]+K[i-1] \).

### 3. Encryption algorithm

Step 1: Start
Step 2: Input the plaintext message \( P_i \), \( 1 \leq i \leq n \).
Step 3: Declare the key value \( K[0] \).
Step 4: Generate different key values \( K_i \), \( 1 \leq i \leq n \)
- \( K[i]=K[i-1]+K[i-1] \)
- \( K[0]= \text{say 25} \)
- \( K[1]=K[0]+K[0] \)
- Etc...
Step 5: Add corresponding Key to plaintext
Step 6: Right shift the result of step 5 once
Step 7: Complement the result of step 6
Step 8: Transmit the Ciphertext

### 4. Encryption and decryption results

#### 4.1 Encryption

<table>
<thead>
<tr>
<th>P</th>
<th>A.V</th>
<th>K</th>
<th>C1</th>
<th>C2</th>
<th>C</th>
</tr>
</thead>
<tbody>
<tr>
<td>E</td>
<td>69</td>
<td>25</td>
<td>94</td>
<td>47</td>
<td>65488</td>
</tr>
<tr>
<td>N</td>
<td>78</td>
<td>50</td>
<td>128</td>
<td>64</td>
<td>65471</td>
</tr>
<tr>
<td>C</td>
<td>67</td>
<td>100</td>
<td>167</td>
<td>83</td>
<td>65452</td>
</tr>
<tr>
<td>R</td>
<td>82</td>
<td>200</td>
<td>282</td>
<td>141</td>
<td>65394</td>
</tr>
<tr>
<td>Y</td>
<td>89</td>
<td>400</td>
<td>489</td>
<td>244</td>
<td>65291</td>
</tr>
<tr>
<td>P</td>
<td>80</td>
<td>800</td>
<td>880</td>
<td>440</td>
<td>65095</td>
</tr>
<tr>
<td>T</td>
<td>84</td>
<td>1600</td>
<td>1684</td>
<td>842</td>
<td>64693</td>
</tr>
<tr>
<td>I</td>
<td>73</td>
<td>3200</td>
<td>3273</td>
<td>1636</td>
<td>63899</td>
</tr>
<tr>
<td>O</td>
<td>79</td>
<td>6400</td>
<td>6479</td>
<td>3239</td>
<td>62296</td>
</tr>
<tr>
<td>N</td>
<td>78</td>
<td>12800</td>
<td>12878</td>
<td>6039</td>
<td>59496</td>
</tr>
</tbody>
</table>

\[ P=\text{Plaintext, A.V= Ascii decimal eqt.of} \ P. \]
\[ K=\text{Key Value, C1=}P+K, \ C2= C1 \text{ Right shifted once, } C= \text{Ciphertext = One’s Complement of} \ C2 \]
4.2 Decryption

<table>
<thead>
<tr>
<th>C</th>
<th>P3</th>
<th>P2</th>
<th>P1</th>
<th>P</th>
</tr>
</thead>
<tbody>
<tr>
<td>65488</td>
<td>47</td>
<td>94</td>
<td>69</td>
<td>E</td>
</tr>
<tr>
<td>65471</td>
<td>64</td>
<td>128</td>
<td>78</td>
<td>N</td>
</tr>
<tr>
<td>65452</td>
<td>83</td>
<td>167</td>
<td>67</td>
<td>C</td>
</tr>
<tr>
<td>65394</td>
<td>141</td>
<td>282</td>
<td>82</td>
<td>R</td>
</tr>
<tr>
<td>65291</td>
<td>244</td>
<td>489</td>
<td>89</td>
<td>Y</td>
</tr>
<tr>
<td>65095</td>
<td>440</td>
<td>880</td>
<td>80</td>
<td>P</td>
</tr>
<tr>
<td>64693</td>
<td>842</td>
<td>1684</td>
<td>84</td>
<td>T</td>
</tr>
<tr>
<td>63899</td>
<td>1636</td>
<td>3273</td>
<td>73</td>
<td>I</td>
</tr>
<tr>
<td>62296</td>
<td>3239</td>
<td>6479</td>
<td>79</td>
<td>O</td>
</tr>
<tr>
<td>59496</td>
<td>6039</td>
<td>12878</td>
<td>78</td>
<td>N</td>
</tr>
</tbody>
</table>

C=Ascii.eqt.of ciphertext
P3=One’s complement of C
P2=P3 left shifted once
P1=P2-K
P= Original transmitted Plaintext character

5. Features of the proposed scheme

i. More security
ii. Simple coding
iii. Good Encryption Speed
iv. Easy to Analyze
v. Fast Response.

6. Conclusion

The Secured communication is a very important aspect of data communication. The securing data is more important in data communications over internet-works. Active attacks involve both modification and fabrication of messages. The goal of the encryption algorithm designing is to frustrate the hackers and makes the cryptanalysis difficult. The key value play more important role in encryption process. The processing speed, coding factors also plays a very important role. Using different key values for encrypting consecutive characters of plaintext hides the relationship between the ciphertext and plaintext. Altering each value of the ciphertext generated to get the final ciphertext make the cryptanalysis still more complex. The algorithm provides appreciable data security and requires minimum coding and involves less processing delay. The key length can be extended to improve security but it reduces the speed. The working of the algorithm can be demonstrated for any length of data.

7. References


