A new Divide and Shuffle Based algorithm of Encryption for Text Message

Dr. S. Muthusundari

R.M.D. Engineering College, Department of Computer Science & Engineering, S. Muthusundari, PO Box 601 206, Kavaraipettai, Chennai, India.

**ARTICLE INFO**

**Article history:**
Received 16 April 2015
Accepted 12 June 2015
Available online 10 July 2015

**Keywords:**
cipher text, reverse, divide, shuffle, security

**ABSTRACT**

In today’s situation, data is transmitted over network needs protection form hackers. Security plays a crucial part in transmissions. Encryption and decryption algorithms take a vital role in providing the data security against the attacks. Encryption of data is an important topic for research, as secure and efficient algorithms are needed in order to optimize encryption and decryption of data[1]. This paper proposes a new encryption algorithm, which uses reverse concept of the text message to encrypt and to decrypt the message which uses divide and shuffle methods. This algorithm provides high security in transmission over network.

© 2015 AENSI Publisher All rights reserved.


**INTRODUCTION**

The data transmission between sender and receiver over the network needs to be protected from unauthorized parties. Data integrity, authentication, and secrecy of exchanged data should be made while they are in transmission. The data should be effectively encrypted at the sender side and only the intend receiver should be able to interpret the cipher text message. Proper keys should be used to encrypt and decrypt the text messages. The original message of the sender called as the plain text is converted into an unreadable form, called as cipher text. The cipher text is transmitted over the network to the receiver, who decrypts it into original message using the same private key [2].

There are several reasons for using encryption (examples are given below, and the crypto system that one should use is the one best suited for one's particular purpose and which satisfies the requirements of the following.

- Ease-of-use
- Reliability
- Security

**Related Work:**

S.P Padia et al (2012) have proposed a new plain text based transposition method. Earlier they developed few transposition techniques[10]. In this paper they have attempted to enhance those techniques and made them more advanced. In the old technique such as rail fence, they are key based to encrypt the plain text. They have exposed already in the journal paper, the reverse transposition technique and Odd-Even transposition technique (The IUP journal of Computer sciences, Vol. V, No. 4, 2011) are in which key is depend on the plaintext so that sender or receiver can easily understand and easily decrypt the cipher text into plaintext but these techniques does not provide any limitation for the generation of key value. And it does not provide any idea about the digits, characters and special character. There is no provision to recapture blank spaces of the words of the plaintext.

Yashpalsingh Rajput et al (2014) have proposed an Improved Cryptographic Technique for the encryption of text message using double encryption. This work proposes an improved scheme for the encryption of the plain text message for its security[6]. All the conventional encryption techniques are very weak and brute force attack and traditional cryptanalysis can be used to easily determine the plain text from encrypted text. In this work of encryption technique, a new combined concept of conventional ceaser cipher algorithm with hill cipher algorithm is used to make encryption technique a much more secure and stronger than the earlier concept. The decryption process is very difficult. The proposed system is divided into two phases. In first phase, to encrypt a new substitution approach is used as first encrypted text. The encryption is done using variable length key which depends on the string length. In the second phase, the hill cipher technique is applied on the first encrypted
text to produce new encrypted text or cipher text. Based on the decryption key, the receiver can generate the original text message.

Bhagat et al (2013) have proposed a Reverse Encryption Algorithm: A Technique for Encryption & Decryption. This paper has proposed a new encryption algorithm, called Reverse Encryption Algorithm (REA). This proposed algorithm is very simple and has very fast approach. REA encryption algorithm provides a secured encryption and cost benefits method.

Himanshu Gupta and Vinod kumar sharma (2013) have proposed a Multiphase Encryption: A New Concept in Modern Cryptography. The conventional methods of encryption can only dealt with maintaining the data security [4]. The information could be accessed by the unauthorized user to lead malicious purpose. Therefore, it is necessary to apply effective encryption/ decryption methods to enhance data security. The multiple encryption techniques of present time cannot provide sufficient security. In this research paper, the new encryption technique named as —Multiphase Encryption is proposed. In this encryption technique, original data is encrypted several times with different strong encryption algorithms at each time. This encryption technique enhances the complexity in encryption algorithm at a great extent.

Ernastuti (2014) proposed a Perfect Shuffle algorithm for cryptography. This paper proposes the new algorithm based on perfect shuffle technique. It is called Perfect Shuffle Crypto Algorithm (PSCA) which is classified as a transposition or permutation technique in the crypto system [5]. The PSCA is an asymmetry key encryption, uses a pair of keys, that are a public key for encrypting data, and a corresponding private secret key for decrypting. PSCA is very fast and simple for technical support. For the linear plaintext length of N=2n, it will take O (N log N) to complete both encryption and decryption process. The PSCA is provided a secure, especially for cipher text-only attack. It is enabling to apply PSCA as a basic algorithm alternative to develop or create a crypto algorithm which employs the layered scheme.

**Proposed Methodology:**
The proposed encryption algorithm has the following features.

**A. Algorithm:**

1. Get the plain text from the sender
2. Reverse the plain text as cipher text

**Fig. 1:** Encryption algorithm.

**B. Working principle of encryption process:**
The original message: welcome
1. Plain text: welcome
2. Reverse the plain text : emoclew

**Cipher Text: emoclew**

**C. Encryption Block diagram:**

**D. Decryption Algorithm:**
The decryption algorithm performs the reverse operations of encryption such that P = D (K, C). It is done in three steps. The procedures are as follows,

1. Get the cipher text from the sender
2. To find the Mid value = n/2
3. If n is even then
   3 a) divide the list in to two halves as 1 to mid value and mid + 1 to n.
   b) Each divided list of its own array element shuffle in its position.

**Fig. 2:** Encryption Block Diagram.
4. If n is odd then
   a) divide the list into two halves as 1 to mid -1 and mid + 1 to n
   b) repeat step 3 b)
   c) and keep the mid value as in its position
5. Original plain text

Fig. 3: Decryption Algorithm.

E. Working principle of Decryption Process
1. Get the cipher text from the sender
   cipher text: e m o c l e w
2. To find the mid value: n = 7
   Mid value = 7/2 = 3.5, hence consider mid = 4
3. n is not even so step 4 will function.
4. n is odd then
   a) divide the list into two halves as 1 to mid -1 and mid + 1 to n
   
5 Original Plain Text: welcome

Fig. 4: Decryption Block Diagram

G. Case Study I:
Encryption Process

Plain text:  ashwin

Cipher text:  n i w h s a

Decryption process

1. the cipher text:  n i w h s a

2. find the mid value: n= 6
   Mid = 6/2 = 3

3. N is even. 3 a) divide the list into two halves
   n i w h s a

3 b) shuffle by its own array

   n   i    w     h      s      a

Plain Text :  a   s   h   w   i   n

RESULTS AND DISCUSSIONS

To study the effectiveness of this proposed algorithm compares with respect to encryption using Double encryption [1] and Multiphase [2] encryption algorithm. We have used programming language C to implement both the algorithms. The implementation results show that the performance of the proposed algorithm is achieving better than the encryption algorithm using Double and Multiphase encryption algorithm.

A few case studies have been carried out to get an average of this study; the result is given in the table 1 with respect to time taken to encrypt & decrypt process. Based on the analysis of the result, the proposed algorithm is ensured its performance.

Table 1: Comparison with respect to time taken to encrypt & Decrypt

<table>
<thead>
<tr>
<th>Sno</th>
<th>Data</th>
<th>Time taken to encrypt &amp; Decrypt in seconds</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Double encryption</td>
</tr>
<tr>
<td>1</td>
<td>100</td>
<td>23</td>
</tr>
<tr>
<td>2</td>
<td>250</td>
<td>42</td>
</tr>
<tr>
<td>3</td>
<td>350</td>
<td>48</td>
</tr>
<tr>
<td>4</td>
<td>500</td>
<td>65</td>
</tr>
<tr>
<td>5</td>
<td>750</td>
<td>76</td>
</tr>
</tbody>
</table>

Fig. 5: Performance with respect to encrypt & Decrypt data.

Conclusion:

In this paper we have presented an implementation of reverse and shuffle algorithm for secured message communication. The main objective was to evaluate the performance of this algorithm in terms of data size. The results have shown that the proposed encryption algorithm was very effective in complexity and security. It was achieved the
effectiveness to encrypt the message from the case study. The computing time also minimum with respect to Double and Multiphase encryption from table 1.

The Encryption algorithm, presented above, is a simple, direct method using reverse and shuffle technique. Consequently, it is reliable fast and suitable for high speed encryption applications. The n value checking of cipher text transmission gives strength to this encryption algorithm. The combination of reverse, divide and shuffle makes the decryption process very reliable and secrecy.

REFERENCES


