Volume 3, Issue 3, March 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

# Enhancing Security of One Time Pad Cipher by Double Columnar Transposition Method

**Sonia Dhull, Vinod Saroha**
*SES, BPS Mahila Vishwavidhyalaya*
*India*

***Abstract— Cryptography is an art and science of converting original message into nonreadable form means 'secret writing'. Two techniques are used for converting data into nonreadable form: 1) Transposition technique 2) Substitution technique. One Time Pad is an example of substitution method. As One Time Pad has various limitations so this talk will present a perspective on combination of techniques substitution and transposition. A double columnar transposition method is applied on One Time Pad in order to overcome limitations of One time Pad cipher and provide much more secure and strong cipher.***

***Keywords— substitution, transposition, cryptography, One Time Pad cipher, cryptanalysis.***

## I. INTRODUCTION

With the era of computer, need of automated tools became essential and the collection of tools designed to protect data and to protect data from hacker is known as Computer Security[1]. The use of networks and communication facilities for carrying data between users and computer to computer is done. So Network Security measures are needed to protect data during transmission[1].

For Network Security came the concept of **Cryptography**- meaning is 'Secret Writing'-is the most effective and strongest tool for controlling against many types of security attacks. A well designed data cannot be modified, read or fabricated (it is a process to send data to receiver after arranging in the same manner after hacking it by Hacker)[2]. So Encryption is the process to change data in a form that cannot be get easily. Symmetric and Asymmetric are the two types of encryption. In symmetric encryption techniques we use the same key for both encryption and decryption purpose. In symmetric method, there are two techniques (substitution and transposition) are used. Substitution technique maps the plaintext elements into cipher text elements and Transposition technique change the position of plaintext elements systematically into ciphertext elements[1].

## II. ONE TIME PAD AND ITS CRYPTANALYSIS

Army Signal Corp. Officer, Joseph Mauborgne, proposed an improvement to Vernam Cipher that was the ultimate in security[5]. He suggested that we use a random key that is as long as the message means the key need not to be repeated. In additional key must be use once for encryption and decryption of a single message and then that key is discarded. So this technique is called as One Time Pad and there is relationship between key and plaintext and it is unbreakable. In this as advance of vignere cipher scheme we Can use 27 character in which 27th character is SPACE, so in this key will be as long as message. So table of Vignere cipher must be expanded to 27*27.

If in case it is known that a given ciphertext is One time pad cipher, then brute force cryptanalysis is easily performed: Try all the 27 keys. There are some weak points about One Time Pad which enables us to use brute force attack[4].

1. The encryption and decryption algorithm is known.
2. Only 2 keys are to try.
3. The language of the plaintext is known and easily recognizable.
4. Need of absolute synchronization between sender and receiver.
5. Need for an unlimited numbers of keys.
6. Generating a large number of random keys is no problem but printing, distributing, storing and accounting for such keys are problems.

## III. ALGORITHM

There is an algorithm which is used to encrypt and decrypt the data which enhance the more security of One Time Pad cipher than original One Time Pad.

A. Encryption Algorithm-

1) We take a message or plaintext from user which we have to encrypt.
2) Then decide the $key_1$, using which we get the characters after finding out the values in One Time Pad 27th characters tableau.
3) Encrypt the message by replacing each letter using decided $key_1$.

 

4) Now write the encrypted message or output of the step3 in rectangle way, row by row. The number of rows depends on the amount of data.
5) Now the order of column becomes the $key_2$ to this algorithm, which is decided by sender for encryption and also known by receiver.
6) Read off the message column by column.
7) Output of step 6 is again written in rectangle form, as above done.
8) After placing the data so, we again read it column by column and we get out our result.
9) Finally we get the secure cipher text (Encrypted data) to forward securely.

B. Decryption algorithm-

An algorithm used in reverse order to get the plaintext is known as decryption algorithm.

1) It takes cipher text, $key_1$, $key_2$ as input which is also known by receiver.
2) Arrange the cipher text in rectangle form: column by column using order of key2.
3) Now read off the data row by row.
4) Repeat the step 2 and 3 using output of step 3 as input.
5) Now decrypt the output of step 4 with $key_1$: using one time pad tableau.
6) Finally we get the original message.

## IV. EXAMPLE

Encryption

1) Suppose the original message is
**THIS IS AN EXAMLE OF ENCRYTION**.

2) Suppose the $key_1$ is DCBHIGEDCBIHGHEADCBAACEDCBAHAICB.

**3)** Encrypt the data using $key_1$ and tableau:
WJJZHOWCCOHLCHQPOGAOFBIQESYWTQQO.

4) Suppose the $key_2$ is 4 3 1 2 5 6 7 which is number of column and also specify their order. It can be anything according to the sender.

5) Now arrange the output of step 3 in rectangle format

| Key: | **4** | **3** | **1** | **2** | **5** | **6** | **7** |
|---|---|---|---|---|---|---|---|
| Plaintext: | W | J | J | Z | H | O | W |
| | C | C | O | H | L | C | H |
| | Q | P | O | G | A | O | F |
| | B | I | Q | E | S | Y | W |
| | T | Q | Q | O | | | |

6) Read column by column according to the order and
The cipher text is: JOOQQZHGEOJCPIQWCQBTHLASOCOYWHFW.

7) Now write the above cipher in rectangle form

| Key: | **4** | **3** | **1** | **2** | **5** | **6** | **7** |
|---|---|---|---|---|---|---|---|
| Plaintext: | J | O | O | Q | Q | G | H |
| | G | E | O | J | C | P | I |
| | Q | W | C | Q | B | T | H |
| | L | A | S | O | C | O | Y |
| | W | H | F | W | | | |

8) Read the data column wise again.
The cipher is: OOCSFQJQOWOEWAHJGQLWQCBCZPTOHIHY.

9) Finally we get our secure output.

*Decryption*

1) Arrange the cipher in rectangle form: column by column, receiver knows the $key_2$ and number of rows.
First apply $k_2$ on it-

| Key: | 4 | 3 | 1 | 2 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|
| Plaintext: | J | O | O | Q | Q | Z | H |
| | G | E | O | J | C | P | I |
| | Q | W | C | Q | B | T | H |
| | L | A | S | O | C | O | Y |
| | W | H | F | W | | | |

2) Read row by row:
JOOQQZHGEOJCPIQWCQBTHLASOCOYWHFW.

3) Again arrange the output in rectangle form column by column:
Key: 4 3 1 2 5 6 7

 

Plaintext: W J J Z H O W
C C O H L C H
Q P O G A O F
B I Q E S Y W
T Q Q O

4) Read row wise, the data is
WJJZHOWCCOHLCHQPOGAOFBIQESYWTQQO.

5) Using $key_1$ and tableau again we get the same data.
**THIS IS AN EXAMPLE OF ENCRYTION**

6) This is original message which is sent by sender.

## V. APPLICATION

This One Time Pad which is enhanced using Double Columnar Transposition Technique has various advantages over simple One Time Pad technique-

- There is no chance to cryptanalyze.
- Brute force attack on it is impossible.
- Result is not easy to reconstruct.
- Also overcome the limitation of simple One Time Pad.
-

## VI. DISADVANTAGE

- Use of Double Transposition technique makes it a complex method.
- Also difficult to implement.

## CONCLUSIONS

One Time Pad is already a strongest Substitution technique and used for high security data. It is a substitution technique in which only letter replaced by any other letter. Transposition techniques are mainly used with other technique to improve the level of security. Only use of Substitution technique replaces the letter by any other letter and only use of Transposition technique changes the place of letters but use of both techniques simultaneously improve the level of security and provide more secure data. The above described method is the combination of both techniques and provides much more secure data than only use of single Substitution technique.

## ACKNOWLEDGMENT

Author would like to give sincere gratitude especially to Mr. Vinod Saroha for his guidance and support to pursue this work.

## REFERENCES

[1] William Stalling "Network Security Essentials (Applications and Standards)", Pearson Education, 2004.
[2] Charles P.Pfleeger "Security in Computing", 4th edition, Pearson Education.
[3] Stallings W (1999), *Cryptography and Network Security*, 2nd edition, Prentice Hall.
[4] William Stallings (2003), *Cryptography and Network Security*, 3rd edition, Pearson Education.
[5] http://en.wikipedia.org/wiki/Cryptography.

 