An Overview on Disrupted Transposition Cipher for Security Enhancement

B. Mahalakshmi
Assistant Professor
Vardhaman College of Engineering

Ch. Sravan Kumar
Assistant Professor
Vardhaman College of Engineering

ABSTRACT

Cryptographic plays a significant role in the internet world. Cryptography comes from the Greek words "secret communication" in the presence of third parties. Cryptographic techniques are used to protect information like substitution and transposition. Caesar cipher is one of the simplest and most extensively known substitution techniques. In Caesar cipher each letter in the plaintext is replaced by a letter in some fixed number of positions down the alphabet. Zigzag cipher is a form of transposition cipher. It derives its name from the way in which it is encoded. In a Disrupted transposition cipher certain positions in a grid are blanked out, and not used when filling in the plaintext. This breaks up regular patterns and makes the cryptanalyst's job more difficult. Caesar Substitution Cipher, Zigzag Cipher and Disrupted Transposition Cipher Techniques are used independently then cipher text acquired is easy to break. To reduce the drawback of substitution and transposition techniques, in this paper we proposed combination of substitution and transposition techniques in order to provide to secure cipher text.

Keywords

Cryptography, Substitution, Transposition, Caesar Cipher, Zigzag Cipher, Disrupted Transposition Cipher, Cipher Text.

1. INTRODUCTION

In the modern era security plays a very important Role. Information also needs protection from unauthorized change [1]. In this information age we need information at every aspect of our lives. Information needs to be secured from unauthorized access. When transmitting information from one place to another, secrecy of information should also be maintained. Sensitive information like bank password, Bank account number, credit card number etc is transmitted through an unsecure medium called internet.

To protect the information exchanged, here we are proposing a zigzag technique that rearranges the plaintext into cipher text. The cipher text obtained is not a secure, so to provide a higher level of security we use a disrupted transposition technique that provides a certain positions on a grid are blanked out based on the key positions that are arranged in row wise and read in column wise. The above two techniques represent the transposition cipher, to get a more secure cipher text, intermediate cipher text is applied into a Caesar cipher. To get the plain text first we apply the final cipher text into Caesar Cipher then we will get the second intermediate Cipher text and that second Intermediate cipher text is applied into disrupted transposition cipher then we will get first intermediate cipher text. By applying a zigzag transposition technique on a first intermediate cipher text, we will get the original plain text.

2. TRANSPOSITION CIPHER

2.1 Simple Transposition Cipher

A transposition cipher is one that does not alter any letters of the original message. A very different kind of mapping is achieved by performing some sort of permutation on the plaintext letters, according to a secret key, so that anyone who knows the key can put the letters back in their proper order and read the message. [1,2]

The Simple transposition cipher is made by just writing the message backward

Example:

CRYPTOGRAPHY AND NETWORK SECURITY

becomes

YTIRUCES KROWTEN DNA YHPARGOTPYRC

The main drawback with simple transposition cipher is backward writing it is too easy to recognize.

2.1 Rail Fence Cipher

Rail Fence cipher is a form of transposition cipher, in which letters of the plaintext are written alternating between rows and the rows are then read sequentially to give the cipher. In a depth-two rail fence (two rows) the message "CRYPTOGRAPHY AND NETWORK SECURITY"

```
C   Y   T   G   A   H   A   D   E   W   R   S   C   R   T
  R   P   O   R   P   Y   N   N   T   O   K   E   U   I   Y
```

Now the cipher is

CYTGAHADEWRSCRTRPORPYNNTOKEUIY

2.2 Disrupted Transposition Cipher

The disrupted transposition cipher is a further complication to the normal transposition technique. Instead of filling the matrix row by row, the rows are all filled in irregular fashion. This results in a very complex transposition of the characters.

First, we determine the exact number of rows and columns to fill. Next we fill a row until we reach the first alphabet sequence from the keyword sequence. If the first digit is at the 8th place, we will only fill that row up to that position. We continue the next row until the second position and so on based on the given example. If we have reached the end position of the last line we continue by filling the remaining empty places at each line. In our example the difference between the two areas is visible by the lower and upper case characters.[3].

The plain text:

"We confirm the delivery of the documents later"

We use the key BIRTHDAY

On the matrix1: after filling the first area

On the matrix2: we see the same matrix

filled completely:

Matrix 1:

2	**5**	**6**	**7**	**4**	**3**	**1**	**8**
B	**I**	**R**	**T**	**H**	**D**	**A**	**Y**
W	**E**	**C**	**O**	**N**	**F**	**I**	
R							
M	**T**	**H**	**E**	**D**	**E**		
L	**I**	**V**	**E**	**R**			
Y	**O**						
F	**T**	**H**					
E	**D**	**O**	**C**				
U	**M**	**E**	**N**	**T**	**S**	**L**	**A**

Matrix2:

2	**5**	**6**	**7**	**4**	**3**	**1**	**8**
B	**I**	**R**	**T**	**H**	**D**	**A**	**Y**
W	**E**	**C**	**O**	**N**	**F**	**I**	**t**
R	**E**	**r**					
M	**T**	**H**	**E**	**D**	**E**		
L	**I**	**V**	**E**	**R**			
Y	**O**						
F	**T**	**H**					
E	**D**	**O**	**C**				
U	**M**	**E**	**N**	**T**	**S**	**L**	**A**

Once the matrix is filled we read it off by the columns, according to the keyword sequence.

The Cipher Text:

ILWRMLYFEUFESNDRTEETIOTDMCRHVHOEOEE CNTA

3. SUBSTITUTION CIPHER:

In cryptography a **substitution cipher** is a process of make secret code by which piece of plaintext are replaced with unreadable code according to a fixed system; the "piece" may be only one letter (the most common), combine of two letters, three letters, mixtures of the above, and so forth. The recipient decrypts the text by performing the inverse substitution.

3.1 Caesar Cipher

In cryptography, a Caesar cipher also known as a Caesar shift cipher or shift cipher, is one of the simplest and most extensively known encryption techniques. It is a type of replacement cipher in which every letter in the plaintext is replaced by a letter some fixed number of positions added down the alphabet. For example, with a shift of 4, A would be replaced by E; B would become F, and so on. The method is named after Julius Caesar.

Example: In Caesar cipher first we translate all of our characters to numbers, 'a'=0,'b'=1,'c'=2,…,'z'=25. We can now represent the Caesar cipher encryption function, e(x) where x is the character we are encrypting, as;

$e (x) = (x + k)(\bmod 26)$

Where k is the key (the shift) applied to each letter. After applying this function the result is a number which must then be translated back into a letter. The decryption functions is :

$e (x)=(x – k) (\bmod 26)$

4. PROPOSED WORK

4.1 Encryption Algorithm

Step 1. First select the plaintext to be encrypted from the sender.

Step 2. Write down the plaintext as a sequence of diagonals (zigzag) in a depth=2(two rows) or depth=3 (three rows), etc. Using the depth as key k1 and the order of elements, as key K2. Using the key k2 read the message, we get cipher text CT1.

Step 3. Select the key K3 as password

Step 4. A table is drawn with column equal to the number of alphabet in the K3 with rows that are sufficient to accommodate all the characters of the plaintext.

Step 5. The password is arranged in such a way as to its occurrence in the alphabet i.e the alphabet closest to letter 'a' is assigned the first position in whatever column it is.

Step 6: The positions of the alphabet is used to write the CT1 in a row wise until we reach the first alphabet in the corresponding column. This process is continued till all the k3 positions have been exhausted, and if the CT1 includes some of the left characters then we use the blanks of the table in a row wise to fill left characters of CT1 in lower case, then we get cipher text CT2.

Step 7. Then apply the cipher text CT2 into Caesar cipher with key K4 finally we get the cipher text (CT3) as required Cipher text.

4.2 Decryption Algorithm

Step 1. First Cipher text CT3 is decrypt using Key K4 we can get Cipher text CT2.

Step 2. Arrange the output of step 1 in a column wise based on the Key K3.

Step 3. Read the message row by row until we encounter the first alphabetic position in k3, this process is continued until all the characters according to k3 are read out. Then we read lower case characters in row wise, we get cipher text CT1

Step 4. Result of step 3 is arranged in row wise based on the Key K2(sequence) and K1(depth).

Step 5. Read off the message in to diagonals finally we get plain Text.

Example: Encryption Process

Step 1. Let the Plain Text to be encrypted is "we confirm the delivery of the documents later".

Step 2. Write the plaintext down as a sequence of diagonals using K1 (depth=3) and K2 (2,1,3).

```
2W      N       M        D     V        O
1  E  O  F  R    T  E    E  I  E  Y  F
3    C      I        H        L        R        etc.
```

Step 3. Now read rows in key (K2) sequence, we get cipher text **(CT1)** "EOFRTEEIEYFHDCMNSAEWNMDVOEUTTCIHLRTOE LR".

Step 4. Using disrupted transposition cipher arranges the cipher text **(CT1)** in row wise based on the Key K3 (Birthday), we get cipher text (**CT2).**

2	**5**	**6**	**7**	**4**	**3**	**1**	**8**
B	**I**	**R**	**T**	**H**	**D**	**A**	**Y**
E	**O**	**F**	**R**	**T**	**E**	**E**	**E**
I	**L**	**R**					
E	**Y**	**F**	**H**	**D**	**C**		
M	**N**	**S**	**A**	**E**			
W	**N**						
M	**D**	**V**					
O	**E**	**U**	**T**				
T	**C**	**I**	**H**	**L**	**R**	**T**	**O**

Step 5. Read the message column wise based on the Key K3 alphabetical order. "ETEIEMWMOTECR TDELOYNNDECFFSVUIRHATHOELR”

Step 6. Using Caesar cipher with K4 to convert CT2 into CT3 Using Key k4=3 can get final cipher text

“HWHLHPZPRWHFUWGHORBQQGHFIIVYXLUKDWK RHOU”

Example: Decryption Process

Step 1. Use key k4=3 to decrypt Cipher text CT3: “HWHLHPZPRWHFUWGHORBQQGHFIIVYXLUKDWK RHOU”

Apply e (x)=(x-k4) mod 26

we get cipher text CT2 "ETEIEMWMOTECR TDELOYNNDECFFSVUIRHATHOELR”

Step 2. Arrange output of step 2 in column wise base on the key K3(birthday) and read it on row wise.

CT2="ETEIEMWMOTECRTDELOYNNDECFFSVUIRHA THOELR”

2	**5**	**6**	**7**	**4**	**3**	**1**	**8**
B	**I**	**R**	**T**	**H**	**D**	**A**	**Y**
E	**O**	**F**	**R**	**T**	**E**	**E**	**E**
I	**L**	**R**					
E	**Y**	**F**	**H**	**D**	**C**		
M	**N**	**S**	**A**	**E**			
W	**N**						
M	**D**	**V**					
O	**E**	**U**	**T**				
T	**C**	**I**	**H**	**L**	**R**	**T**	**O**

We get CT1= “EOFRTEEIEYFHDCMNSAEWNMDVOEUTTCIHLRTOE LR”

Step 3. First count the number of letters in CT1 and find the depth of zigzag algorithm and put the cross marks and fill the result of step 2.Read the message in a diagonal way we get plain text.
“We confirm the delivery of the documents later”.

X X X X X X x X X X

X X X X X X X X X X X X X X X X X X X

X X X x x X X X X x

2 W N M D V O E U T T

1 E O F R T E E I E Y F H D C M N S A E

3 C I H L R T O E L R

Advantages of the Proposed Algorithm:

1. The proposed algorithm is more difficult to crypt-analyze.
2. Brute Force attack is not possible.
3. It Overcome the limitations of substitution and transposition ciphers.
4. Apply the transposition and substitution cipher combine together to provide more security.

Disadvantages of the Proposed Algorithm:

It makes use of multiple keys so that key transformation is more difficult. To overcome this problem we can make use of public key cryptography.

5. CONCLUSION

Caesar Cipher and Rail Fence are simplest and easily understandable substitution techniques. This is the advantage of these techniques. This advantage leads to security problems. To overcome this problem Caesar Cipher and Rail Fence are combined with Disrupted transposition cipher. The above proposed technique is a combination of substitution and transposition methods which provides greater level of security to any stream of data.

6. REFERENCES

[1] William Stallings 2009 cryptography and network security

[2] *https://books.google.co.in/books?isbn=0486320316*

[3] Jawad Ahmad Dar **“**Humanizing the Security of Rail Fence Cipher Using Double Transposition and Substitution Techniques” IJSR, 2012.

[4] Rail Fence Cipher, Route Cipher, Columnar transposition Cipher retrieved from http://en.wikipedia.org/Transposition

[5] Mu. Annalakshmi, A. Padmapriya, Zigzag Ciphers: A Novel Transposition Method.

[6] Network Security and Cryptography by Atul Kahate.

[7] Ajit Singh, Aarti Nandal, Swati Malik "Implementation of Caesar Cipher with Rail Fence for Enhancing Data Security" in December 2012.

[8] https://en.wikipedia.org/wiki/Caesar_cipher.

[9] Mr. Vinod Saroha, Suman Mor, Anurag Dagar, "Enhancing Security of Caesar Cipher by Double Columnar Transposition Method" in October 2012.