Volume 2, Issue 10, October 2012 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 Caesar Cipher by Double Columnar Transposition Method

Mr. Vinod Saroha
CSE,SES,BPSMV
India

Suman Mor
CSE,SES,BPSMV
India

Anurag Dagar
CSE,SES,BPSMV
India

Abstract - Cryptography is an art and science of converting original message into nonreadable form.There are two techniques for converting data into nonreadable form:1)Transposition technique 2)Substitution technique.Caesar cipher is an example of substitution method.As Caesar cipher 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 Caesar cipher in order to overcome all limitation of Caesar cipher and provide much more secure and strong cipher.

Keywords— substitution,transposition,cryptography,Caesar cipher,cryptanalysis.

I. INTRODUCTION

In today's information age,it is impossible to imagine without internet.This modern era is dominated by paperless offices,E-mail messages,E-cash transactions and virtual departmental stores.Due to this there is a great need of interchanging of data through internet.Various sensitive information like banking transactions,credit information, confidential data is transfered over internet.To protect this type of data there is a great need of security.We convert our data in a nonreadable form at sender side and convert that data in readable form again at receiver end.The art and science of creating nonreadable data or cipher so that only intended person is only able to read the data is called Cryptography[2]. Encryption is a process by which we convert our data in nonreadable form.Decryption is reverse of encryption process[3].Plaintext is the intended original message.Cipher text is the coded message.There are two techniques of encryption:Substitution Technique and Transposition Technique[4].

In substitution technique,the letters of plain text are replaced by other letters or any number or by symbols. Example Caesar cipher,hill cipher,monoalphabetic cipher etc[4].

In transposition technique,some sort of permutation is performed on plaintext.Example:rail fence method,columnar method etc[4].

II. CAESAR CIPHER AND ITS CRYPTANALYSIS

Caesar cipher is one of the simplest type of substitution method.In this letters of alphabets are replaced by letters three places further down the alphabet.But in general,this shift may be of any places[4]. Using the Caesar cipher,the message "RETURN TO ROME" is encrypted as "UHWXUA WR URPH".So attacker is not able to read the message if he intercepts the message[3].

If in case it is known that a given ciphertext is Caesar cipher,then brute force cryptanalysis is easily performed:Try all the 25 keys.There are some weakpoints about Caesar cipher which enables us to use brute force attack[4].

1.The encryption and decryption algorithm is known.
2.Only 25 keys are to try.
3.The language of the plaintext is known and easily recognizible..

III. ALGORITHM

There is an algorithm which is used to encrypt and decrypt the data which provides more secure Caesar cipher than original Caesar cipher.

A. Encryption

1) First,we take a message or plain text from user which have to encrypt.
2) Decide the key_1(places) with the help of which characters are to be shifted.
3) Decrypt the message by replacing each letter by decided key_1.
4) Now write this encrypted message or output of step 3 in rectangle way,row by row.The number of rows depends on amount of data.

5) The order of column becomes the key(key_2) to this algorithm,which is decided by sender and also known to receiver.
6) Read off the message column by column and we can permute the order of column.
7) The output of step 6 is write in rectangle form again,row by row as above told.
8) After placing data in rectangle form then it is read off column by column,we get our result.
9) Finally we get the secure cipher text(encrypted message).

B. Decryption

The algorithm which runs in reverse order to get the original data is known as decryption.

1) It takes the cipher text,key_1 and key_2.The number of rows is also known to receiver.
2) Arrange the cipher in rectangle form:column by column using key_2 and number of rows.
3) Read the message row by row.
4) Repeat the step 2 and 3 with the output of step 3 as input.
5) Now decrypt the message with key_1.
6) Finally we get our original data(plain text).

IV. EXAMPLE

A. *Encryption*

1) Suppose the original message is

THISISANEXAMLEOFENCRYTION.

2) Suppose the key_1 is 4.
3) Decrypt the data by 4 places:

XLMWMWERIBEQPISJIRGVCXMSR

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: **X L M W M W E**
R I B E Q P I
S J I R G V C
X M S R

6) Read column by column according to the order and
The cipher text is:
MBISWERRLIJMXRSXMQGWPVEIC
7) Now write the above cipher in rectangle form

Key : **4 3 1 2 5 6 7**

Plaintext: M B I S W E R
R L I J M X R
S X M Q G W P
V E I C

8) Read the data columnwise again.
The cipher is:
IIMISJQCBLXEMRSVWMGEXWRRP
9) Finally we get our secure output
IIMI SJQCBLXEMRSVWMGEXWRRP

B. *Decryption*

1) Arrange the cipher in rectangle form:column by column,receiver knows the key and number of rows.

Key : **4 3 1 2 5 6 7**

Plaintext: M B I S W E R

R L I J M X R

S X M Q G W P

V E I C

2) Read row by row:
MBISWERRLIJMXRSXMQGWPVEIC
3) Again arrange the output in rectangle form column by column:

Key : 4 3 1 2 5 6 7

Plaintext: X L M W M W E

R I B E Q P I

S J I R G V C

X M S R

4) Read row wise,the data is
XLMWMWERIBEQPISJIRGVCXMSR
5) Using key_1,which is 4, decrypt the above cipher and we get
THISISANEXAMPLEOFENCRYTION
6) This is original message which is sent by sender.

V. APPLICATION

This Caesar cipher which is secured by "Double Transposition Columnar" has various advantages over simple Caesar cipher.

- In this double transposition method is applied which provide much less structured permutation.
- It is more difficult to cryptanalyze.
- The result is not easily reconstructed.
- Brute force attack is not possible.
- Overcome all the limitations of Caesar cipher.

.

VI. DISADVANTAGE

- Complex method by performing two stage of columnar transposition method.
- Difficult to implement as simple Caesar cipher.

VII. CONCLUSION

Caesar cipher is simplest type of cipher and mostly used.Transposition method is mostly combined with other techniques.Both substitution method and transposition method encryption are easily performed with the power of computers. The combination of these two classic techniques provides more secure and strong cipher.The final cipher text is so strong that is very difficult to break.Substitution method only replace the letter with any other letter and transposition method only change position of characters.The above described method is the combination of both the transposition and substitution method which provides much more secure cipher.

Acknowledgment

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

REFERENCES

[1] William Stalling"Network Security Essentials(Applications and Standards)",Pearson Education,2004
[2] Atul Kahate (2009), *Cryptography and Network Security,* 2nd edition, McGraw-Hill.
[3] Stallings W (1999), *Cryptography and Network Security,* 2nd edition, Prentice Hall.
[4] William Stallings (2003), *Cryptography and Network Security,* 3rd edition, Pearson Education .

