Enhancing the Security of Caesar Cipher Substitution Method using a transposition technique for more Secure Communication

K.Arul Jothy,
Final Year, Department of Computer Science and Engineering,
JCT College of Engineering and Technology, Coimbatore, India,
aruljothy22@gmail.com

K.Sivakumar,
Assistant Professor, Department of Computer Science and Engineering,
JCT College of Engineering and Technology, Coimbatore, India,
sivakumar.karuppan@gmail.com

R.Tharani,
Assistant Professor, Department of Computer Science and Engineering,
JCT College of Engineering and Technology, Coimbatore, India,
tharani.r@jct.ac.in

ABSTRACT In recent years there is drastic progress in Internet world. Sensitive information can be shared through internet but this information sharing is susceptible to certain attacks. Cryptography was introduced to solve this problem. Cryptography is an art and the science of creating the secret code. Substitution and the transposition are the two technique use for encoding and decoding the text. So when we these two technique individually it is easy to track. This can be overcome by combining these two techniques. So the Caesar cipher from substitution and the keyed transposition and the columnar technique from the transposition can be used. So by combining these two techniques the fundamental weakness can be overcome and the cipher text becomes very hard to track.

Key words: Caesar cipher, Columnar method, Transposition technique, Encryption, Decryption

I. INTRODUCTION

- We are living in the information age. We need to keep track of our information about every aspect of our lives.
- And the computer becomes the most essential part of all human lives. So the computer based transaction had become more popular among all now a days.
- Computer based system have three valuable components. They are
  - i) Hardware
  - ii) Software
  - iii) Data
- Securities of these components are evaluated in terms of vulnerability, threats, attacks and control.
- An assault on system security that derives from an intelligent threat; that is an intelligent act that is a deliberated attempt to evade security services and violates the security policy of a system.
- So the security for the sensitive information through internet had become more important.
- So but still we are left with a difficult job of protecting network from variety of attacks.
- And because of lots of efforts network support staff came up with the solution to the problem named "CRYPTOGRAPHY"
- Cryptography is the process of encrypting and decrypting the information from sender to receiver through the network.
- The information is encrypted and decrypted with the help of secret key.

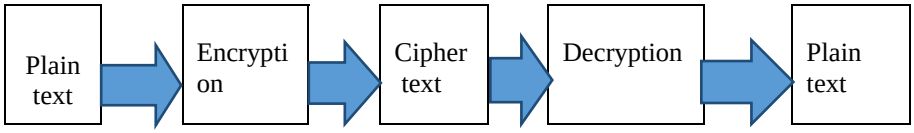


Fig.1 Encryption and Decryption

- The two ways in which the text can be encrypted and decrypted is
  a. Substitution method
  b. Transposition method
- Substitution method replaces one character by another character. The character can be replaced by number also and vice versa. e.g: Monoalphabetic ciphers, Caesar cipher, play fair etc….
- Transposition method means does not substitute one symbol by another; instead it changes the location of the symbols. e.g: keyless transposition, keyed transposition.
- Here the plain text along with key value is encrypted to obtain the cipher text and the cipher text is transmitted through the insecure channel and the text is decrypted in the receiver side by using the key value to obtain the original plain text.

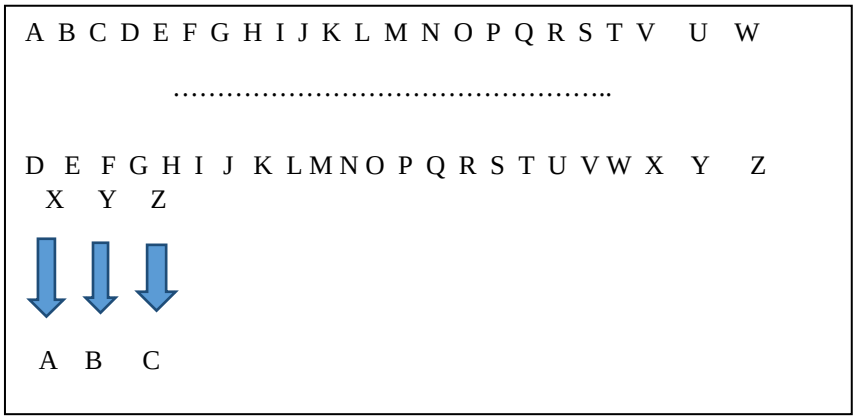
1.1 CAESAR CIPHER

- Caesar cipher is the simplest technique. It is also called as the shift cipher.
- In this method the single character is replaced by another character by using the secret key.

Encryption:
C= E (P + K) MOD 26
Where,
C= cipher text
E= encryption
P= plain text
K= Secret key

Decryption:
P= D(C-K) MOD 26
Where,
C= cipher text
D= decryption
P= plain text
K= Secret key

Table I. Caesar Cipher technique



THE KEY VALUE USED IS: 03

EXAMPLE: HAPPY

Encryption

C= E (P + K) MOD 26

C =E (H +3) MOD 26

C=E(7+3)MOD 26

C=E(10)MOD 26

C= 10 MOD 26

C=10

C=K

Therefore the encrypted text of happy is **KDSSB**

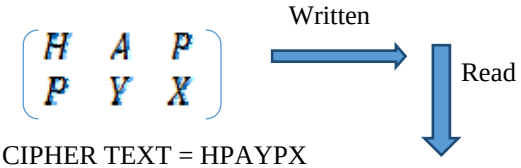
After this the decryption is done in the reverse order to obtain the original text HAPPY.

1.2 COLUMNAR METHOD

- A transposition cipher rearranges the characters in the plain text to form the cipher text.
- So, cipher text is obtained by applying permutation on plain text. The key used to decrypt the message is the inverse of the original key.
- So here the number of column and the row is fixed based on the key value chosen by the sender and the receiver during encryption.
- Then during the encryption the character are written by row by row and the cipher text is obtained by reading the character column by column.
- Then during the decryption process based on the key value the characters are separated and then characters are written column by column and characters are read by row by row.
- So the space left empty at last in the matrix is filled by the dummy variable called bogus letter.

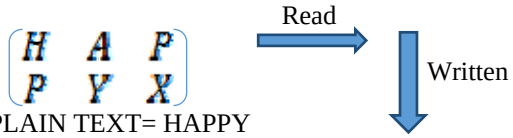
EXAMPLE: HAPPY

Encryption:



CIPHER TEXT = HPAYPX

Decryption:



PLAIN TEXT= HAPPY

1.3 KEYED TRANSPOSITION

- Here the sender and the receiver have to agree to divide the text into group of required number of character.
- And the divided number of character must be equal in their size. In case of inequality of size of character then the bogus letter must be added to make all the group of equal size.
- For the arrangement of key the sender and receiver can use some technique based on their wish.
- Key generation : Secret key value is 3

Table II. Keyed Transposition technique

ENCRYPTION DECRYPTION

1	2	3
3	1	2

EXAMPLE: HAPPY

Segregated into 3 character based on key: HAP PYX

Encrypted text is APHYXP

- Then the reverse operation is performed to obtain the original plain text.

II. PROPOSED WORK

In proposed work we will combine Caesar Cipher, Columnar method, Keyed transposition techniques for making the communication more secure.

Algorithm: (The key value must be agreed before the transaction take place)

ENCRYPTION:

STEP I: Take the plain text as input and remove the spaces between words.

STEP II: Encrypt by using Caesar cipher.

STEP III: Then encrypt by using columnar method.

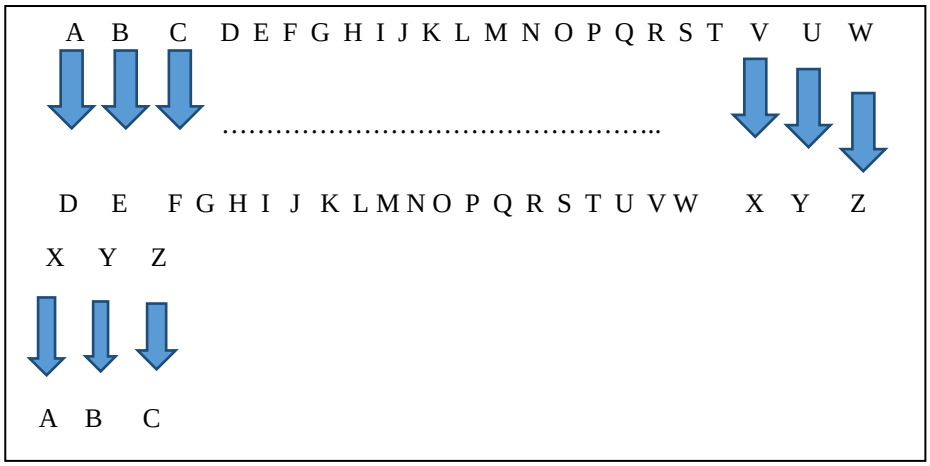
STEP IV: Then finally encrypt by using keyed transaction method and here the key value is based on the number of row in columnar based on my length of string.

STEP V: After implementing the above specified encryption technique, cipher text is sent to the intended recipient.

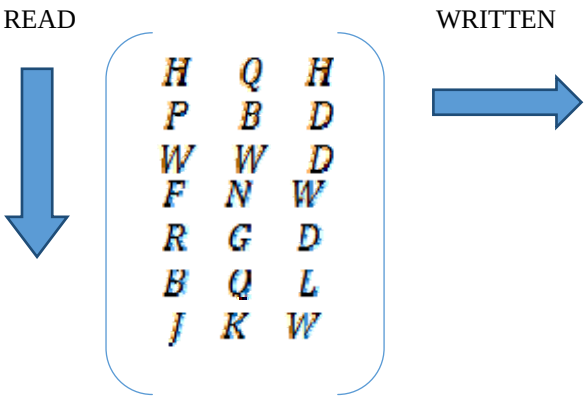
DECRYPTION:

STEP I: Take the cipher text as input from the sender.
STEP II: Then decrypt by using keyed transaction method.
STEP III: Then decrypt by using columnar method.
STEP IV: Then finally decrypt by using Caesar cipher.
STEP V: After implementing the above specified technique the plain text is obtained.
EXAMPLE:
"ENEMY ATTACK TODAY NIGHT"
The fixed key value is: 03
ENCRYPTION:
STEP I: The plain text is **"ENEMY ATTACK TODAY NIGHT"**
STEP II: CAESAR CIPHER
C= E (P+K)
K= key value =03

Table III. Caesar cipher technique



Here the values are assigned to letters A –Z from 0 TO 25. So the above table is arranged based on key value.
The result is: "HQHPB DWWDFN WRGDB QLJKW"
STEP III: COLUMNAR METHOD
INPUT: "HQHPB DWWDFN WRGDB QLJKW"
KEYVALUE =03
So, the text is segregated as set of three characters
"HQH PBD WWD FNW RGD BQL JKW"



The result is:
"HPWFRBJ QBWNGQL HDDWDLW"
STEP IV: KEYED TRANSACTION METHOD

Note:

> Here the number of row in columnar is 7. So I am choosing key value for this transaction as 7. And one kind of arrangement is made for the even number and another for the odd number .So the kind of arrangement must be discussed by the sender and the receiver.

INPUT: “HPWFRBJ QBWNGQL HDDWDLW”

Table IV. Keyed transposition technique-Encryption

ENCRYPTION DECRYPTION

1	2	3	4	5	6	7
2	4	6	7	5	3	1

HPWFRBJ QBWNGQL HDDWDLW

The result: “JHBPRWF LQQBGWN WHLDDDW”

STEP V: The obtained cipher text is:”JHBPRWF LQQBGWN WHLDDDW”

DECRYPTION:

STEP I: KEYED TRANSACTION METHOD

The input cipher text is:”JHBPRWF LQQBGWN WHLDDDW”

Table V. Keyed transposition technique-Decryption

ENCRYPTION DECRYPTION

1	2	3	4	5	6	7
2	4	6	7	5	3	1

The result is: “HPWFRBJ QBWNGQL HDDWDLW”

STEP II: COLUMNAR METHOD

Input is: “HPWFRBJ QBWNGQL HDDWDLW”

READ WRITTEN

H	Q	H
P	B	D
W	W	D
F	N	W
R	G	D
B	Q	L
J	K	W

The result is:

“HQH PBD WWD FNW RGD BQL JKW”

STEP III: CAESAR CIPHER

Decryption:
P= D(C-K) MOD 26
Conversion sample for cipher text HQH
P=D(H-3) MOD 26
P=D(7-3) MOD 26
P=D(4)MOD 26
P= 4
P=E

The result is:**“ENEMY ATTACK TODAY NIGHT”**

STEP IV: The obtained plain text is **“ENEMY ATTACK TODAY NIGHT”**

III APPLICATION

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

- It is more difficult to cryptanalyze.
- The result cannot be easily reconstructed.
- Overcome all the limitations of Caesar cipher.
- The combinations of substitution and transposition technique together increase the complexity of attack.

IV CONCLUSION

- Caesar cipher is the simplest substitution method.
- It is also the weakest cipher.
- It's only advantage lies in the fact that it is not complex and can be understood easily.
- This advantage leads to the problem of easy detection.
- For overcoming this problem Caesar cipher is combined with transposition techniques.
- Transposition technique used here is Columnar and keyed transposition.
- The above proposed method is a combination of transposition and substitution hence it will provide better security for text.
- However, the used algorithms can be improved to get better results.
- Security provided by this algorithm can be enhanced further by using it with one or more different encryption algorithms or by using asymmetric key approach instead of symmetric key.

V ACKNOWLEDGMENT

We would like to give our sincere gratitude to our guide Mr. K .Sivakumar who encouraged and guided us throughout this paper.

VI REFERENCES

[1] AtulKahate (2009), Cryptography and Network Security, 2nd edition, McGraw-Hill.
[2] Stallings, W. (2006), Cryptography and Network Security 4/E., Pearson Education India.
[3] Behrouz A Fourouzan, DebdeepMukhopadhyay (2010), Cryptography and Network, 2nd edition, McGraw-Hill.
[4] Goyal, Kashish, and SupriyaKinger. "Modified Caesar Cipher for Better Security Enhancement." International Journal of Computer Applications (0975–8887) Volume (2013).