Enhancing The Security of Caesar Cipher Using Double Substitution Method

Shahid Bashir Dar
Research Scholar, Department of Computer Science and Engineering
Bells Institute of Management and Technology
Shimla(HP), India
darshahid9@gmail.com

Abstract— Cryptography comes from the Greek words for "secret writing". The plain text is encrypted into the corresponding cipher text, using an algorithm and a key. Substitution and Transposition are two techniques used for converting data into non-readable form. Caesar Cipher is an example of substitution technique. In this paper we have proposed a cipher that uses basic encryption techniques of substitution and transposition. A single columnar transposition followed by a double substitution is applied on a Caesar cipher in order to make it a stronger and a more secure cipher.

Keywords- cryptography, substitution, transposition, Caesar cipher, key.

I. INTRODUCTION

The development of internet has put a lot of burden on a cryptanalyst to develop suitable encryption techniques that could secure the data over internet. In this age of information, it is impossible to imagine without internet. A huge amount of data is interchanged over internet, sensitive information like credit card information, confidential data, banking transactions, needs to be protected demanding a highest degree of security. The messages to be encrypted, known as the plaintext, are transformed by a function that is parameterized by a key [1]. The cipher text is transmitted to the intended receiver(s) where the reverse of encryption process is done to get the original plaintext.

Encryption process can be categorized into: substitution ciphers and transposition ciphers. In a substitution cipher each letter or a group of letters is replaced by another letter or group of letters to disguise it [1].Caesar cipher, Hill cipher, mono-alphabetic cipher are some examples of the substitution cipher. Whereas, in transposition ciphers, letters are reordered in such a way to create confusion to the intruder. Rail fence cipher, Columnar cipher are some examples of the transposition cipher.

II. CAESAR CIPHER AND ITS CRYPTANALYSIS

The Caesar cipher is of oldest and simplest known cipher. It is one of the types of substitution cipher, in which each letter in the message or plaintext is shifted a certain number of places down the alphabet. For example, with a shift of 2, A would be replace by C, B would be replaced by D, C would be replace by E, and so on.

The encryption for the given plaintext with as shift (key) of 2 can be done as:

Plaintext: defend the wall of china

Cipher text: fghgpf vjg ycnn qh ejkpc

Decryption is simply done using an offset of -2 to get the original plaintext.

We translate all the 26 characters to numbers, 'a'=0, 'b'=1,'c'=2…'z'=25. The Caesar cipher encryption function, E(x), can be now represented as:

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

Where 'k' is the key (the shift) applied to each character 'x'. The Caesar cipher decryption function, D(x), will be

$$D(x) = (x – k) \bmod 26$$

III. ALGORITHM

The proposed algorithm that is used for encryption and decryption of the data provides a new Caesar cipher which is stronger more secure than the original one.

A. Encryption

1) First take the plaintext to be encrypted from the sender.
2) Write the plaintext in a rectangular way, row by row. Order of columns is determined by key K1.
3) Read off the message column by column, we get cipher text CT1.
4) Use key K2 to shift each of the character of cipher text CT1.we get cipher text CT2.
5) Repeat step 4 for cipher text CT2.

6) Output of step 5 is our required cipher text CT.

B. Decryption

It follows all the steps of encryption process but in the reverse order to get the original plaintext.

1) It takes cipher text, keys K1 and K2. The number of rows is also known to the receiver.
2) Use key K2 to decrypt the cipher text.
3) The output of step 2 is again decrypted with key K2.
4) Arrange the output of step 3 in a rectangular way, column by column using key K1 and the number of rows.
5) Read off the message row by row.
6) Output of step 5 is our required plaintext.

IV. EXAMPLE

A. Encryption

1) Suppose the plaintext is

HELLOCRYPTOGRAPHY

2) Suppose 3 4 1 2 5 be the key K1. We arrange plaintext rectangular way

Key K1:	**3**	**4**	**1**	**2**	**5**
Plaintext:	**H**	**E**	**L**	**L**	**O**
	C	**R**	**Y**	**P**	**T**
	O	**G**	**R**	**A**	**P**
	H	**Y**			

3) Read off message column by column, we get cipher text CT1.

CT1: LYRLPAHCOHERGYOTP

4) We use key K2 = 3 to shift charecters of cipher text CT1.

CT2: OBUOSDKFRKHUJBRWS

5) Repeat step 4 for cipher text CT2.

CT: REXRVGNIUNKXMEUZV

6) Our final encrypted message will be CT: REXRVGNIUNKXMEUZV.

B. Decryption

1) Use key K2=3 to decrypt cipher text CT.

OBUOSDKFRKHUJBRWS

2) Again use key K2=3 to decrypt the output of step 1.

LYRLPAHCOHERGYOTP

3) Arrange output of step 2 in rectangular format, column by column, using key K1= 3 4 1 2 5.

Key K1:	**3**	**4**	**1**	**2**	**5**
	H	**E**	**L**	**L**	**O**
	C	**R**	**Y**	**P**	**T**
	O	**G**	**R**	**A**	**P**
	H	**Y**			

4) Read off the message row by row, we get the original plain text.

HELLOCRYPTOGRAPHY

5) Our required plain text is: HELLOCRYPTOGRAPHY

V. ADVANTAGES

The proposed Caesar cipher employing a double substitution method has following advantages over the simple Caesar cipher.

- It uses very less structured permutation.
- It is more difficult to crypt-analyze.
- Brute force attack is not possible.
- It is simple to perform double substitution.
- Overcomes the limitations of simple Caesar cipher.

VI. DISADVANTAGES

- It is difficult to implement as simple Caesar cipher.
- It makes use of two keys as compared to the simple Caesar cipher.

REFERENCES

[1] Andrew S.Tanenbaum"Computer Networks", Fourth Edition, PEARSON.
[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] http://practicalcryptography.com/ciphers/caesar-cipher/.