ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 1, January 2017

Enhancing the Security of Caesar Cipher Using Different Shift Key

Muzafar Ahmad Wani[1], Ummer Akbar[2]

M. Tech Student, Dept. of CSE, BITS, Pilani, Rajasthan, India[1]

Software Engineer, Capgemini, Pune, India[1]

M. Tech Student, Dept. of CSE, BIMT,Mehli, Shimla, H.P, India[2]

Software Engineer, Mindstack, Bangalore, India[2]

ABSTRACT: Cryptography is the science of information security. The word is derived from the Greek "kryptos" meaning hidden. At the sender side the original text called plain text is encrypted into the corresponding cipher text, using an algorithm and the key. At the receiver side the encrypted text is decrypted into the plain text. The two techniques used in converting text into non-readable form are transposition and substitution. Caesar cipher is an example of transposition and substitution. This paper proposes a cipher that uses transposition followed by substitution with different key for each alphabet in order to make stronger and more secure cipher to frequency attacks.

KEYWORDS: cipher, cryptography, frequency analysis, key, Substitution and transposition

I. INTRODUCTION

In today's world, one cannot imagine life without Internet. Internet is used everywhere whether it is college, university bank, government office or any private sector. 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. What the cryptanalyst need to do is to develop suitable encryption techniques that could secure the data over internet. The messages to be encrypted, known as the plaintext, are transformed by a function that is parameterized by a key. 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 .Caesar cipher, Hill cipher, mono-alphabetic cipher are some examples of the substitution cipher. Whereas, in transposition cipher, letters are reordered in such a way that creates confusion to the intruder. Rail fence cipher, Columnar cipher are some examples of the transposition.].

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 3, "A" would be replace by "D", "B" would be replaced by "E", "C" would be replace by "F", and so on.

The encryption for the given plaintext with as shift (key) of 3 can be done as:

Plaintext: helloword
Cipher text: khoorzrug
Decryption is simply done using an offset of -3 to get the original plaintext.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 1, January 2017

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
$D(x) = (x – k) \bmod 26$

In this basic algorithm "letter frequency analysis" problem occurs, this is because similar alphabets are replaced by same alphabet e.g.
The encryption of plaintext with shift (key) of 4 can be done as:
Plaintext : " INFORMATION"
Cipher text: " MRJSVQEXMSR"
Here it is clear both "I" are transformed to " M".

The solution to this problem is to find a way of encryption to transform similar alphabet to different alphabets , so that frequency count would not be a clue for attackers. The proposed algorithm is the solution of above said problem.
.

III. PROPOSED ALGORITHM

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

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.

5) Use key K =K2 (the shift) + P (position of alphabet in plaintext) to shift each of the character of cipher text CT1.we get cipher text CT2
That is $E(x) =(x+ (K2+p)) \bmod 26$

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 and "P" position of alphabets to decrypt the cipher text.
$E(x) =(x-(K2+P)) \bmod 26;$
.
3) Arrange the output of step 2 in a rectangular way, column by column using key K1 and the number of rows.

4) Read off the message row by row.

5) Output of step 4 is our required plaintext

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 1, January 2017

IV. EXAMPLE

A. ENCRYPTION

1) Suppose the plaintext is
Protectmefromfrequecyanalysis

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

Key K1 :	**4**	**2**	**5**	**3**	**1**
Plaintext:	**P**	**R**	**O**	**T**	**E**
	C	**T**	**M**	**E**	**F**
	R	**O**	**M**	**F**	**R**
	E	**Q**	**U**	**E**	**N**
	C	**Y**	**A**	**N**	**A**
	L	**Y**	**S**	**I**	**S**

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

CT1: EFRNASRTOQYYTEFENIPCRECLOMMUAS

4) Use key k=K2+p to shift characters of cipher text CT1, where key K2 = 4 and "p" position of each alphabet
i.e. For E
x=4;
p=1;
K2=4;
E ("E") = (4+ (4+1)) mod26
= 9
This means "E" is converted to "I"
Similarly other alphabets can be converted and result would be CT2

CT2:IKXUIBBEADMNJVWWHDLZPDCMQPQZGZ

Our final encrypted message will be CT2:

Decryption

1) Use key k=K2+p to shift characters of cipher text CT2, where key K2 = 4 and "p" position of each alphabet
i.e. for "J
X=9;
K2=4;
P=1;
D (J) = (9-(4+1)) mod26
=4
=E
Similarly other alphabet can be converted and gets
CT1: EFRNASRTOQYYTEFENIPCRECLOMMUAS

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

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 1, January 2017

Key K1: **4 2 5 3 1**

P	**R**	**O**	**T**	**E**
C	**T**	**M**	**E**	**F**
R	**O**	**M**	**F**	**R**
E	**Q**	**U**	**E**	**N**
C	**Y**	**A**	**N**	**A**
L	**Y**	**S**	**I**	**S**

3) Read off the message row by row, we get the original plain text.
Protect me from frequency analysis

4) Our required plain text is:
Protect me from frequency analysis

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.
- Frequency analysis attack is not possible.
- Overcomes the limitations of simple Caesar cipher

VI. DISADVANTAGES

- It is difficult to implement as simple Caesar cipher.
- It is difficult to count the position of alphabet.
- Message should be reached to destination in orde

REFERENCES

[1] Andrew S.Tanenbaum"Computer Networks", Fourth Edition, PEARSON.
[2] AtulKahate(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/.