Modified Ceaser Cipher and Rail fence Technique to Enhance Security

Baljit Saini,
Lecturer, Computer Department, K.D.Polytechnic, Patan, Gujrat, India.

Abstract: Cryptography is the art to secure messages by encoding them. Cryptography techniques are used to secure messages. Information security is important in transmission and data storage. The Caesar cipher is one of the earliest known Substitution ciphers. In Ceaser Cipher each letter in the plaintext is shifted a certain number of places down the alphabet. Rail Fence Cipher transposition Technique involves writing plain text as a sequence of diagonals and then reading it row by row to produce cipher text. In this paper I experimented on the well known techniques Ceaser Cipher and rail fence to induce some strength to these encryption techniques. Proposed method showed that it is better in terms of providing more security to any given text message. In our experiments Caesar Ciphers and rail fence techniques are used as representatives of Classical Techniques. In this paper, Author modified the traditional Caesar cipher and fixed the key size as two. Another thing alphabet index is checked add alphabet index into key and take its modulus. After that we will apply rail fence algorithm on index value to again encrypt the message.

Keyword: *Plain Text, Cipher Text, Key*

I. INTRODUCTION

In this information age we need information at every aspect of our lives. Information is like an asset. [1]Information needs to be secured from unauthorized access. Information also needs protection from unauthorized change. In today's era information is distributed due to internet and networking. People can share information from distance. When transmitting information from one place to secrecy of information should be maintained. Sensitive information like bank password, Bank account number, credit card number etc is transferred from internet multiple times. At that time some mechanism or technique is required to secure information.

A. Cryptography

Cryptography [2] word has a Greek Meaning that is Secret Writing. Cryptography techniques are used to secure data. In Cryptography plain text is transferred to cipher text using encryption technique, this process is called encryption. And converting cipher text to plain text by using decryption technique, this process is called decryption.

II. CRYPTOGRAPHY TECHNIQUES

- Substitution Techniques
- Transposition Techniques

A. Substitution Techniques

In substitution techniques plain text characters are replaced by other numbers, symbols and characters.

Caesar Cipher technique

Caesar Cipher technique is one of the examples of substitution techniques. Caesar cipher was proposed by Julius Caesar. In Caesar Cipher plaintext is replaced with some fixed alphabets.

Example
Plaintext- MORNING
Cipher text-PRUQLQJ

TABLE 1-Caesar Cipher Table

Alphabet	Position
A	D
B	E
C	F
D	G
E	H
F	I
G	J
H	K
I	L
J	M
K	N
L	O
M	P
N	Q
O	R
P	S
Q	T
R	U
S	V
T	W
U	X
V	Y
W	Z
X	A
Y	B
Z	C

B. Transposition Techniques

[3]A transposition cipher involves the rearranging of the letters in the plaintext to encrypt the message. This is in contrast to a substitution cipher, in which the plaintext letters are replaced by letters from another alphabet (or by different letters from the same alphabet).

Rail Fence Cipher

[4]The Rail Fence Cipher is a type of transposition cipher. In rail fence cipher technique following steps are used

1. Write down the plain text message as a sequence of diagonals
2. Read the plain text written in step 1 as a sequence of rows

Example
Plaintext- MORNING
Cipher text- MRIGONN

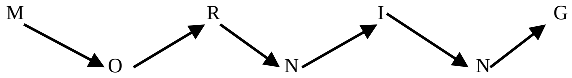

Fig.1Example of Rail Fence Algorithm

III. PROPOSED ALGORITHM

A. Encryption Algorithm

First Level Encryption
Step 1
In the proposed algorithm plaintext and encryption key is required. Encryption key will be an integer number and it is based on position of alphabet in alphabet table.

TABLE 2-Alphabet Position Table

Alphabet	Position
A	0
B	1
C	2
D	3
E	4
F	5
G	6
H	7
I	8
J	9
K	10
L	11
M	12
N	13
O	14
P	15
Q	16
R	17
S	18
T	19
U	20
V	21
W	22
X	23
Y	24
Z	25

Step 2
If there is repeated word in the text put X before and after repeated alphabet and then makes Cipher text.
Step 3

$$C1=(P+2)\,\%26 \tag{1}$$

C1:-Cipher text generated using modified ceaser cipher algorithm
P: Plaintext position in alphabet table

Second Level Encryption
Step 4
Arrange the text as a sequence of diagonals. Read the text started from row 1 left to right then from row 2 left to right.

Example:

Plaintext-MORNING

Cipher text
C1(M)=(12+2)%26=14=O
C1(O)=(14+2)%26=16=Q
C1(R) = (17+2)%26=19=T
C1(N)= (13+2)%26=15=P
C1(I)=(8+2)%26=10=K
C1(X)=(23+2)%26=25=Z
C1(N)=(13+2)%26=15=P
C1(X)=(23+2)%26=25=Z
C1(G)=(6+2)%26=8=I
C1=OQTPKZPZI
In this example N is repeated. So X is inserted before and after repeated N.

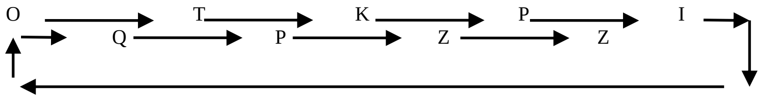

Fig.2Example of Proposed Encryption Algorithm

C=OTKPIQPZZ

C: Ciphertext

B. Decryption Algorithm

First Level Decryption

Step 1

- Read Cipher text C.
- Arrange cipher text as a sequence in two rows
- Read them as diagonals.

Second Level Decryption

Step 2

- Get integer values corresponding to alphabet from the Table2.
- Apply formula given below to get Plain text. Here C1 is Cipher text obtained from step 2

$$P=(C1-2)\,\%26 \tag{2}$$

- If there is alphabet X before and after any character. Ignore X and read the Alphabet from the table corresponding to the number obtained by the formula.

- Now we get Plain text

Example

Step 1

Read Cipher text

C= OTKPIQPZZ

Arrange Cipher text in two rows

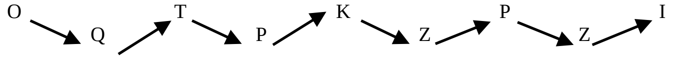

Fig.2Example of Proposed Decryption Algorithm Level 1

Read Cipher text rows as diagonals

C1=OQTPKZPZI

Step 2

- Get integer values corresponding to alphabet from the Table2

TABLE 3- Example of Proposed Decryption Algorithm Level 2

O	**Q**	**T**	**P**	**K**	**Z**	**P**	**Z**	**I**
14	**16**	**19**	**15**	**10**	**25**	**15**	**25**	**8**

- Apply formula (2)

  Get corresponding alphabet from the Table2.

  P(O)=(14-2)%26=12=M

  P(Q)=(16-2)%26=14=O

  P(T)=(19-2)%26=17=R

  P(P)=(15-2)%26=13=N

  P(K)=(10-2)%26=8=I

  P(Z)=(25-2)%26=23=X

  P(P)=(15-2)%26=13=N

  P(Z)=(25-2)%26=23=X

  P(I)=(8-2)%26=6=G

- Ignore X if it exists before and after any alphabet in the text. Then Read text.
- Plaintext=MORNING

CONCLUSIONS

Caesar cipher and Rail fence techniques are simple cipher techniques to encrypt data. The modified Caesar cipher and rail fence technique can encrypt data strongly. In the proposed algorithm both substitution and transposition methods are used to encrypt data. Cipher text generated by proposed algorithm will be difficult to break Combination .

References

[1] Atul Kahate (2009), *Cryptography and Network Security*, 2nd edition, McGraw-Hill.
[2] Stallings W (2014), *Cryptography and Network Security Principles and Practice*,6th edition, Pearson Education.
[3] William Stallings (2003), *Cryptography and Network Security*, 3rd edition, Pearson Education
[4] http://www.cs.trincoll.edu/~crypto/historical/railfence.html
[5] M. S. Hwang and C. Y. Liu, \Authenticated encryption schemes: current status and key issues," International Journal of Network Security, vol. 1, no. 2, pp. 61-73, 2005.