Abstract:

In the past few years use of internet has grown dramatically. Lots of sensitive data is being stored and transferred on-line via Internet. This leads to the need of securing data. Many data security techniques arise due to this among which are cryptographic techniques. Cryptography is art of converting plain text(P.T.) into Cipher Text(C.T.) our proposed work is combination of such two techniques Ceaser Cipher and Rail Fence Algorithm with some modification in Rail Fence algorithm. When both of these techniques considered individual, it is easy to crack the cipher text obtained. But with combination of ceaser Cipher with modified Rail Fence algorithm provides more security to data being transferred, making cipher to crack typical.

Keywords: Modified Rail fence, Ceaser Cipher, Data security, and cipher.

Introduction: Security to data being transferred on-line is very important as it includes critical data like bank transaction, military information, conversation between different nations, etc. For providing this security cryptography is being used. Cryptography is converting the plain text into cipher text using some keys so that no one other than intended users can read and understand the information. There are mainly two techniques namely Symmetric Key cryptography and asymmetric key cryptography. In symmetric key cryptography encryption and decryption keys are same, whereas in asymmetric key cryptography both these keys are different. These keys are known to both sender and receiver. Encryption process goes as:

![Encryption Diagram](image-url)
Decryption process is converting the cipher text back into Plain Text.

Current Work:

**Ceaser cipher:** Ceaser cipher Technique is Substitution technique in which letter are replaced by some another letter by adding or subtracting certain value(key) to the current letter. A general rule for encryption using Ceaser cipher technique is:

\[ C.T = (P.T.+\text{key})\mod 26 \]

Ex.

P.T.: RAM IS HERE

Key: 3

Encryption:

<table>
<thead>
<tr>
<th>Letter</th>
<th>Key</th>
<th>Cipher Letter</th>
</tr>
</thead>
<tbody>
<tr>
<td>R</td>
<td>+3</td>
<td>U</td>
</tr>
<tr>
<td>A</td>
<td>+3</td>
<td>D</td>
</tr>
<tr>
<td>M</td>
<td>+3</td>
<td>P</td>
</tr>
<tr>
<td>I</td>
<td>+3</td>
<td>L</td>
</tr>
<tr>
<td>S</td>
<td>+3</td>
<td>V</td>
</tr>
<tr>
<td>H</td>
<td>+3</td>
<td>K</td>
</tr>
<tr>
<td>E</td>
<td>+3</td>
<td>H</td>
</tr>
<tr>
<td>R</td>
<td>+3</td>
<td>U</td>
</tr>
<tr>
<td>E</td>
<td>+3</td>
<td>H</td>
</tr>
</tbody>
</table>

Encrypted key is:

UDPLVKHUH

Decryption:

<table>
<thead>
<tr>
<th>Cipher Letter</th>
<th>Key</th>
<th>Letter</th>
</tr>
</thead>
<tbody>
<tr>
<td>U</td>
<td>-3</td>
<td>R</td>
</tr>
<tr>
<td>D</td>
<td>-3</td>
<td>A</td>
</tr>
<tr>
<td>P</td>
<td>-3</td>
<td>M</td>
</tr>
<tr>
<td>L</td>
<td>-3</td>
<td>I</td>
</tr>
<tr>
<td>V</td>
<td>-3</td>
<td>S</td>
</tr>
<tr>
<td>K</td>
<td>-3</td>
<td>H</td>
</tr>
</tbody>
</table>
Decrypted code is:

RAMISHERE

**Rail Fence Cipher:** Rail Fence Cipher technique is a transposition technique in which position of letters is interchanged using some key.

In rail fence cipher technique letter are placed in zigzag format in different no. of lines based on key, and then read line by line, making cipher text.

Ex.

P.T.: RAM IS HERE

Key: 2

Now read the code line by line and get cipher text:

C.T.: RMSEAIHR

For decryption key is known to receiver, so write the code in two lines and read code diagonally, as shown below:

P.T.: RAMISHERE

**Problem with existing work:**

Ceaser Cipher is vulnerable to Brute-force attack, which is to trying each possible key to break the code. If attacker breaks one code he can easily break the remaining code using that key. Which is quite easy is to do when used in alone.

Similarly it is also easy to break the Rail-Fence Algorithm if attacker comes to know about the key used, by splitting the code into different number of lines and reading the code into zigzag pattern.
Proposed Work:

Proposed work is combination of both ceaser cipher and some modification in rail fence algorithm. New work in this approach is that when splitting the code in zigzag pattern, a numeric row will be introduced between continuous two lines, as shown below. So here we will be using two keys one for ceaser cipher and one for rail fence cipher, which will make code more secure.

Ex.

P.t.: RAM IS HERE.

Key: 2

Will be encoded as:

\[
\begin{array}{c}
R \\
M \\
S \\
E \\
E \\
1 \\
3 \\
5 \\
7 \\
9 \\
7 \\
5 \\
3 \\
A \\
I \\
H \\
R
\end{array}
\]

C.T.: RMSEE13579753AIHR

This is more complicated to break than simple rail fence algorithm. Hacker will be more confused with numeric data in between.

When this modified algorithm will be combined with Ceaser Cipher algorithm it will be providing much security then individual of each.

Encryption Algorithm:

- Take the Plain Text (P.T.) as input
- Define the encryption key ‘K1’ for Ceaser Cipher and ‘K2’ for modified Rail Fence Cipher techniques
- Determine the numerical value to be inserted in between the rows of Rail Fence Cipher, and the range of numerical data
- Apply the key ‘K1’ on Plain Text to retrieve cipher text C.T.1
- Take C.T.1 as input for modified Rail Fence technique and divide it in various rows based on key value ‘K2’.
- At alternate rows insert the numerical value in the increasing order.
- Read the text line by line, to retrieve final encrypted method.
Decryption Algorithm:

- Take the Cipher Text
- Split the Cipher Text in different rows according to key value k2
- Delete all the numerical rows
- Read the text in zigzag pattern starting from left corner
- On this decrypted code apply key value k1 as done in Caesar cipher to decrypt the code
- Read the final Plain Text

Pictorial representation of proposed work:

![Diagram showing the decryption process](image)

Example:

P.T.: ATTACK WILL BE DONE AT 3 PM

Key1: 5

Key2: 2

Key3: odd numbers from 1 to 9

Step 1: encode using Caesar cipher

<table>
<thead>
<tr>
<th>A</th>
<th>+ 5</th>
<th>= F</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>+ 5</td>
<td>= Y</td>
</tr>
<tr>
<td>T</td>
<td>+ 5</td>
<td>= Y</td>
</tr>
<tr>
<td>A</td>
<td>+ 5</td>
<td>= F</td>
</tr>
<tr>
<td>C</td>
<td>+ 5</td>
<td>= H</td>
</tr>
<tr>
<td>K</td>
<td>+ 5</td>
<td>= P</td>
</tr>
<tr>
<td>W + 5 = C</td>
<td></td>
<td></td>
</tr>
<tr>
<td>I + 5 = N</td>
<td></td>
<td></td>
</tr>
<tr>
<td>L + 5 = Q</td>
<td></td>
<td></td>
</tr>
<tr>
<td>L + 5 = Q</td>
<td></td>
<td></td>
</tr>
<tr>
<td>B + 5 = G</td>
<td></td>
<td></td>
</tr>
<tr>
<td>E + 5 = J</td>
<td></td>
<td></td>
</tr>
<tr>
<td>D + 5 = I</td>
<td></td>
<td></td>
</tr>
<tr>
<td>O + 5 = T</td>
<td></td>
<td></td>
</tr>
<tr>
<td>N + 5 = S</td>
<td></td>
<td></td>
</tr>
<tr>
<td>E + 5 = J</td>
<td></td>
<td></td>
</tr>
<tr>
<td>A + 5 = F</td>
<td></td>
<td></td>
</tr>
<tr>
<td>T + 5 = Y</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3 + 5 = 8</td>
<td></td>
<td></td>
</tr>
<tr>
<td>P + 5 = U</td>
<td></td>
<td></td>
</tr>
<tr>
<td>M + 5 = R</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

So C.T.1 is: FYYFPCNQQGJITSJFY8UR

Step2: encrypt the code using modified Rail fence cipher algorithm as:

\[
\begin{array}{llllll}
F & Y & H & C & N & U \\
1 & 3 & 5 & 7 & 9 & 7 \\
Y & F & P & N
\end{array}
\]

\[
\begin{array}{llllll}
Q & G & I & S & R & U \\
3 & 1 & 3 & 5 & 7 & 7 \\
Q & J & T & J
\end{array}
\]

So new Cipher Text (C.T. 2) is:

FYHCQGISF8R1357975313579753135YFPNQJTJYU

**Conclusion:** Individually both these are simplest type cipher algorithm and are being used mostly. When substitution technique combined with transposition technique provides much more security against attacks like Brute Force attack. As
in this approach encryption consist of both ceaser Cipher And Modified Rail Fence Algorithm which contains Numerical key also which is being inserted between the data which is being encrypted, so it will provide great security to data being transferred making code to break typical specially in the case if data is alphanumeric.

References:

1. Anupama Mishra, Enhancing Security of Ceaser Cipher using Different Methods, Vol. 02, IJRET.
4. Randhir Kumar, Integration of Ceaser Cipher with Redefence cipher for Enhancing Data Security, Vol. 02, IJSRD.

Corresponding Author:
Navaneethan C*,
Email: navaneethan.c@vit.ac.in