TCET
DEPARTMENT OF INFORMATION TECHNOLOGY (IT)
(Accredited by NBA for 3 years, 4th Cycle Accreditation w.e.f. 1st July 2022)
Choice Based Credit Grading System (CBCGS)
Under TCET Autonomy

# Cryptography & Network Security

## TE IT

## Experiment No 2

## Implementation of Rail Fence Cipher

**Aim**: To write a Python program to implement Rail Fence Cipher (Transposition Cipher Technique).

**Learning Objectives**:

- To understand the transposition technique.
- To describe Rail Fence Cipher algorithm and encrypt the plain text.

**Theory**:

**Transposition Techniques:**

Substitution techniques focus on substituting a plain-text alphabet with a cipher-text alphabet. Transposition techniques differ from substitution techniques in the way that they do not simply replace one alphabet with another, but they also perform some permutation over the plain text.

**Algorithm of Rail Fence Cipher**:

The rail fence cipher (also called a zigzag cipher) is a form of transposition cipher. It derives its name from the way in which it is encoded. It uses a simple algorithm as shown in fig. 1

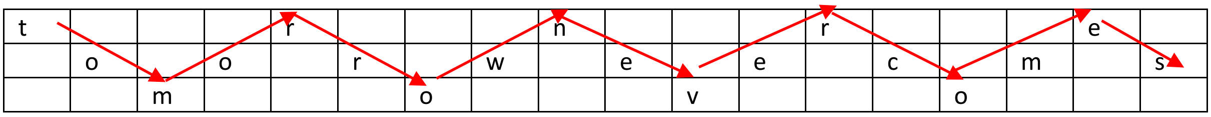
1. Write down the plain-text message as a sequence of diagonals.
2. Read the plain text written in *Step* 1 as a sequence of rows.

***Fig. 1 Rail-fence technique***

Encryption Process:

1. In the rail fence cipher, the plain text is written downwards and diagonally on successive rails of an imaginary fence.
2. When we reach the bottom rail, we traverse upwards moving diagonally, after reaching the top rail, the direction is changed again. Thus the alphabet of the message is written in a zig-zag manner.
3. After each alphabet has been written, the individual rows are combined to obtain the cipher text.

For example, if the message is “tomorrow never comes” and the number of rails = 3 then the cipher is prepared as:



| | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| t | | | | r | | | | n | | | | r | | | | e | |
| | o | | o | | r | | w | | e | | e | | c | | m | | s |
| | | m | | | | o | | | | v | | | | o | | | |

**The cipher text is:** “trnreoorweecmsmovo”

## Decryption:

As we’ve seen earlier, the number of columns in the rail fence cipher remains equal to the length of the plain-text message. And the key corresponds to the number of rails.

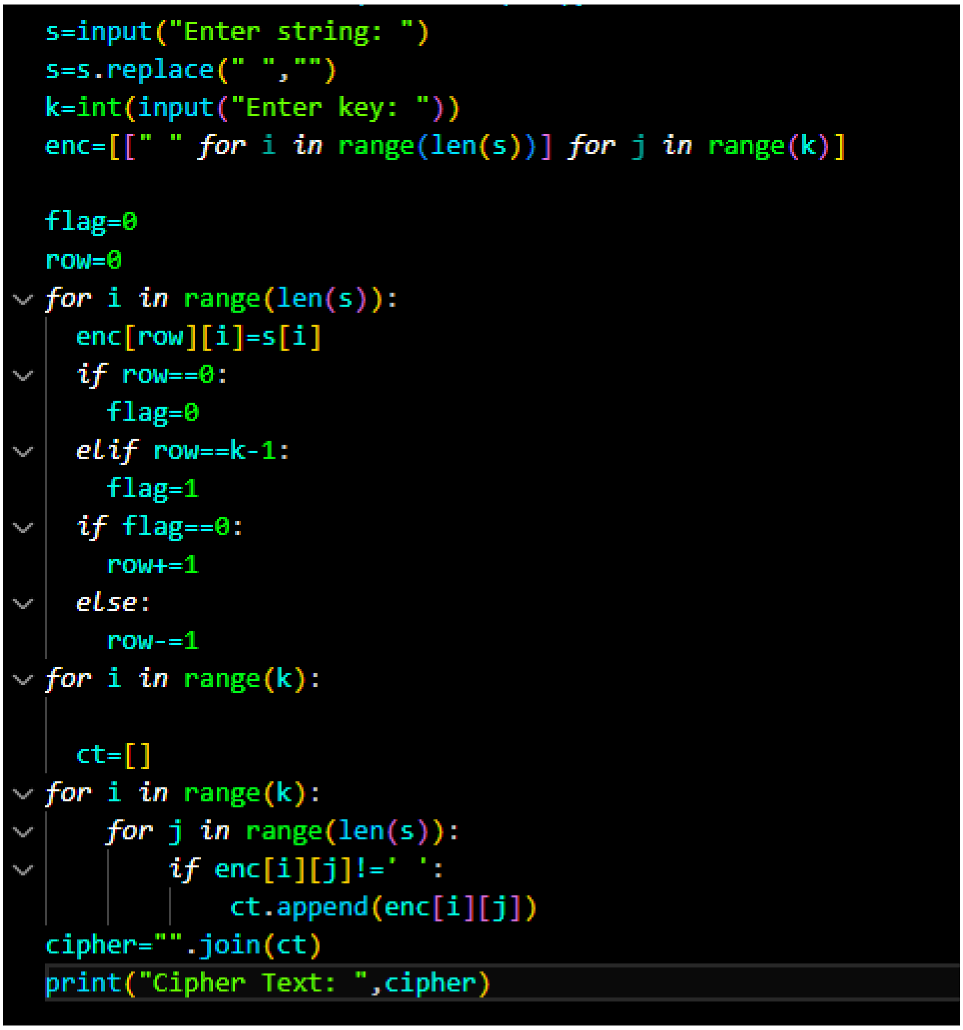
Hence, the rail matrix can be constructed accordingly. Once we’ve got the matrix we can figure out the spots where texts should be placed (using the same way of moving diagonally up and down alternatively).

Then, we fill the ciphertext row-wise. After filling it, we traverse the matrix in a zig-zag manner to obtain the original text.

### Results:

Encrypt and Decrypt your full name using Rail Fence Cipher.

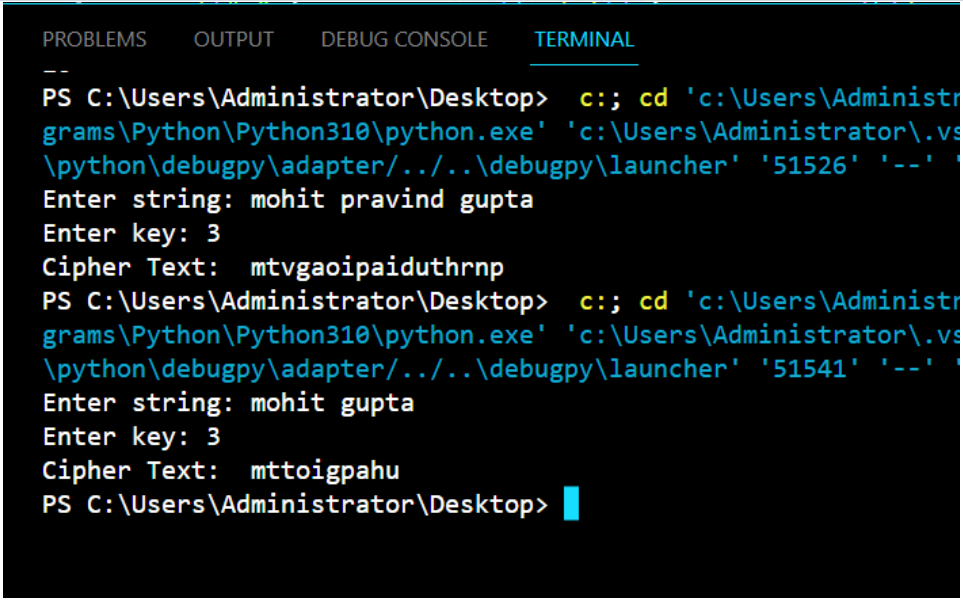
### Outputs:



```
s=input("Enter string: ")
s=s.replace(" ","")
k=int(input("Enter key: "))
enc=[[" " for i in range(len(s))] for j in range(k)]

flag=0
row=0
for i in range(len(s)):
  enc[row][i]=s[i]
  if row==0:
    flag=0
  elif row==k-1:
    flag=1
  if flag==0:
    row+=1
  else:
    row-=1
for i in range(k):

  ct=[]
for i in range(k):
    for j in range(len(s)):
        if enc[i][j]!=' ':
            ct.append(enc[i][j])
cipher="".join(ct)
print("Cipher Text: ",cipher)
```



```
--
PS C:\Users\Administrator\Desktop>  c:; cd 'c:\Users\Administr
grams\Python\Python310\python.exe' 'c:\Users\Administrator\.vs
\python\debugpy\adapter/../..\debugpy\launcher' '51526' '--' '
Enter string: mohit pravind gupta
Enter key: 3
Cipher Text:  mtvgaoipaiduthrnp
PS C:\Users\Administrator\Desktop>  c:; cd 'c:\Users\Administr
grams\Python\Python310\python.exe' 'c:\Users\Administrator\.vs
\python\debugpy\adapter/../..\debugpy\launcher' '51541' '--' '
Enter string: mohit gupta
Enter key: 3
Cipher Text:  mttoigpahu
PS C:\Users\Administrator\Desktop>
```

## Conclusion:

The Rail Fence Cipher employs diagonal writing across virtual rails, forming a zig-zag pattern. By mastering this transposition technique, one gains practical knowledge of encryption methods and the manipulation of character order, enhancing their cryptographic understanding. Experimenting with Rail Fence Cipher offers insight into encryption concepts through its unique approach.

## Practical Learning Outcomes:

| After performing the practical, the learner is able to: | Marked √ |
|---|---|
| i. To understand the transposition technique.<br>ii. To describe Rail Fence Cipher algorithm and encrypt the plain text. | |

| Outcome | PLO 1 | PLO 2 | PLO 3 | Performance | Attendance | Total Score | IT DEPARTMENT- TCET |
|---|---|---|---|---|---|---|---|
| Weight | 20 | 20 | 20 | 20 | 20 | 100 | Date of Performance: ________<br>Date of Correction: ____________<br>Roll No: __________<br>Marks: ______/100<br>Signature of Faculty: |
| Score | | | | | | | |