Practical No.4

Aim: To implement Rail fence cipher of transposition Techniques.

Date :

Practical No. 4

Aim : To implement Rail Fence cipher of transposition Techniques.

Theory :

The rail fence cipher (something called zigzag cipher) is a transposition cipher that jumbles up the order of the letters of a message using a basic algorithm.

The rail fence cipher works by writing your message on alternate lines across the pages, and then reading off each line in turn.

For example, let's consider the plaintext "This is a secret message".

plaintext : THIS IS A SECRET MESSAGE

To encode this message we will first write over two lines (the "rails of the fence") as follows :

Rail fence Encoding

T		I		I		A		E		R		T		E		S	
	H		S		S		S		C		E		M		S		A

G	
	E

Note that all white spaces have been removed from the plain text.

The cipher is then read off by writing the top row first, followed by the bottom row :

ciphertext : TIIAERIESGHSSSCEMSAE

Conclusion :

The concept of transposition stream ciphers, Railfence cipher has been studied successfully.

Date :

program:

```
def encryptRailFence(text, key):
    rail = [['\n' for i in range(len(text))]
                  for j in range(key)]
    dir_down = False
    row, col = 0,0

    for i in range(len(text)):
        if (row == 0) or (row == key-1):
            dir_down = not dir_down
        rail[row][col] = text[i]
        col += 1

        if dir_down:
            row += 1
        else:
            row -= 1
    result = []
    for i in range(key):
        for j in range(len(text)):
            if rail[i][j] != '\n':
                result.append(rail[i][j])
    return("".join(result))

def decryptRailFence(cipher, key):
    rail = [['\n' for i in range(len(cipher))]
                  for j in range(key)]
    dir_down = None
    row, col = 0,0

    for i in range(len(cipher)):
        if row == 0:
```

output :

```
main.py                                                    Save    Run    Shell

def encryptRailFence(text, key):
    rail = [['\n' for i in range(len(text))]
                  for j in range(key)]
    dir_down = False
    row, col = 0, 0

    for i in range(len(text)):
        if (row == 0) or (row == key - 1):
            dir_down = not dir_down

        rail[row][col] = text[i]
        col += 1

        if dir_down:
            row += 1
        else:
            row -= 1
    result = []
    for i in range(key):
        for j in range(len(text)):
            if rail[i][j] != '\n':
                result.append(rail[i][j])
    return("" .join(result))

def decryptRailFence(cipher, key):
```

```
tiaeitesjhisscemsae
thisisasecretmessage
>
```

Date :

```
        dir_down = True
    if row == key - 1:
        dir_down = False

    rail[row][col] = '*'
    col += 1

    if dir_down:
        row += 1
    else:
        row -= 1

index = 0
for i in range(key):
    for j in range(len(cipher)):
        if ((rail[i][j] == '*') and
        (index < len(cipher))):
            rail[i][j] = cipher[index]
            index += 1

result = []
row, col = 0, 0
for i in range(len(cipher)):
    if row == 0:
        dir_down = True
    if row == key - 1:
        dir_down = False
    if (rail[row][col] != '*'):
        result.append(rail[row][col])
        col += 1
    if dir_down:
        row += 1
```

Page No.

conclusion:

The concept of transposition Stream cipher, Rail fence has been studied successfully.

Date :

```
        else:
            row -= 1
    return ("".join(result))

if __name__ == "__main__":
    print(encryptRailFence("thisisasecretmessage", 2))
    print(decryptRailFence("tiiaetegsssrcesae", 2))
```

Conclusion:

The concept of transposition stream cipher, Rail fence cipher has been studied successfully.

Date :

Viva Questions:

(1) what is Transposition Technique?

→ Transposition technique is a method of encryption plain text into cipher text by performing permutation over the plain text.

(2) Explain how Rail fence work?

→ The rail fence cipher works by writing your message on alternate line like zig zag pattern across the page and then reading off each line in turn.

(3) What is disadvantages of Rail fence?

→ The main disadvantages of rail fence cipher technique are lack of security, limited effectiveness and vulnerability to attack. Attacker can easily break the encryption by launching attacks.