NAME: PRERNA SUNIL JADHAV
SAP ID: 60004220127
BATCH: C2-2
BRANCH: COMPUTER ENGINEERING
COURSE: INFORMATION SECURITY LABORATORY.
COURSE CODE: DJ19CEL603

EXPERIMENT 04

AIM: Study and Implement Simple Columnar Transposition cipher.

THEORY: Given a plaintext message and a ~~Retri~~ numeric key, cipher / de-cipher the given text using columnar Transposition cipher. It is a form of transposition just like Rail fence cipher. It involves writing the plaintext out in rows, then reading the ciphertext off in columns one by one.

Encryption: In a transposition cipher, the order of the alphabets is re-arranged to obtain the cipher text.

1) The message is written out in rows of a fixed length, and then read out again column by column and the columns are chosen in some scrambled order.

2) Width of the rows and the permutation of the columns are usually defined by a keyword.

3) For example, the word HACK is of length 4 (so the rows are of length 4), and the permutation is defined by the alphabetical order of the letters in the keyword. In this case, the order would be "3 1 2 4".
4) Any spare space are filled with nulls or left blank or placed by a ex character (Example: _)
5) Finally, the message is read off in column in the order specified by keyword.

H	A	C	K
3	1	2	4
G	e	e	k
s	_	f	o
r	_	G	e
e	k	s	_

Print character of columns 1,2,3,4

Encrypted text: eketGsGsrekoe_

Decryption: To decipher it, the receipient has to work out the column length by dividing the message length by key length.
Then, write the message out in columns again, then re-order the columns by reforming the keyword.

CONCLUSION: It is simple and efficient encryption method that has been widely used in various applications, including data protection and military communication etc.
Hence, we studied and implemented columnar Transposition.

Name:	Prerna Sunil Jadhav
Sap Id:	60004220127
Class:	T. Y. B. Tech (Computer Engineering)
Course:	Information Security Laboratory
Course Code:	DJ19CEL603
Experiment No.:	04

AIM: Study and Implement Simple Columnar Transposition Cipher.

CODE:

```
def ColTT_Enc(plain_text, key):
    matrix = []
    for i in range(key):
        matrix.append([])
    for i in range(len(plain_text)):
        matrix[i % key].append(plain_text[i])
    for i in matrix:
        print(i)
    cypher_text = ''
    for i in matrix:
        for char in i:
            cypher_text += char
    print("Cipher text of Columnar Transposition is " + cypher_text)
    return cypher_text


def ColTT_Dec(cypher_text, key):
    matrix = []
    for i in range(key):
        matrix.append([])
    count = int(len(cypher_text)/key)
    length = 0
    extra = int(len(cypher_text) % key)
    for charlist in matrix:
        for j in range(count):
            charlist.append(cypher_text[length])
            length = length+1
        if (extra != 0):
            charlist.append(cypher_text[length])
            length = length+1
            extra = extra-1
    for i in matrix:
        print(i)
    plain_text = ''
```

```
    for i in range(key+1):
        for charlist in matrix:
            if i > len(charlist)-1:
                continue
            plain_text = plain_text + charlist[i]
    print("Decrypted text of Columnar Transposition is " + plain_text)

string = input("Enter a string:")
col = int(input("Enter column number:"))
c2 = ColTT_Enc(string, col)
ColTT_Dec(c2, col)
```

OUTPUT:

```
PS C:\Users\Jadhav\Documents\BTech\Docs\6th Sem\IS\Code> & C:/msys64/mingw64/bin/python.exe "c:/Users/Jadhav/Doc
uments/BTech/Docs/6th Sem/IS/Code/Exp4/Simple_Columnar_Transposition.py"
Enter a string:Hi this is prerna jadhav
Enter column number:5
['H', 'i', ' ', 'n', 'd']
['i', 's', 'p', 'a', 'h']
[' ', ' ', 'r', ' ', 'a']
['t', 'i', 'e', 'j', 'v']
['h', 's', 'r', 'a']
Cipher text of Columnar Transposition is Hi ndispah  r atiejvhsra
['H', 'i', ' ', 'n', 'd']
['i', 's', 'p', 'a', 'h']
[' ', ' ', 'r', ' ', 'a']
['t', 'i', 'e', 'j', 'v']
['h', 's', 'r', 'a']
Decrypted text of Columnar Transposition is Hi this is prerna jadhav
```