Assignment No 2

Title:

Write a Java/C/C++/Python program to perform encryption and decryption using the method of

Transposition technique.

Theory:

Transposition Cypher:

Transposition Cipher is a cryptographic algorithm where the order of alphabets in the plaintext is rearranged to form a cipher text. In this process, the actual plain text alphabets are not included.

Transposition Techniques

1. Rail Fence Transposition
2. Columnar Transposition
3. Improved Columnar Transposition
4. Book Cipher/Running Key Cipher

Columnar transposition:

Example

A simple example for a transposition cipher is **columnar transposition cipher** where each character in the plain text is written horizontally with specified alphabet width. The cipher is written vertically, which creates an entirely different cipher text.

Consider the plain text **hello world**, and let us apply the simple columnar transposition technique as shown below

h	e	l	l
o	w	o	r
l	d		

The plain text characters are placed horizontally and the cipher text is created with vertical format as **: holewdlo lr.** Now, the receiver has to use the same table to decrypt the cipher text to plain text.

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 spaces are filled with nulls or left blank or placed by a character (Example: _).
5. Finally, the message is read off in columns, in the order specified by the keyword.

Encryption

Given text = Geeks for Geeks

Keyword = HACK **Length of Keyword** = 4 (no of rows) **Order of Alphabets in HACK** = 3124

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

Print Characters of column 1,2,3,4

Encrypted Text = e kefGsGsrekoe_

Decryption

1. To decipher it, the recipient has to work out the column lengths by dividing the message length by the key length.

2. Then, write the message out in columns again, then re-order the columns by reforming the key word.

Implementation:

- Install anaconda navigator.
- Launch Jupiter notebook
- And run python code.

Python code :

```
import math
plaintext="transposition technique using python"
key=8
ciphertext=['']*key
for colum in range(key):
    pointer=colum
    while pointer<len(plaintext):
     ciphertext[colum]+=plaintext[pointer]
     # print(ciphertext)
     pointer+=key

cipher=' '.join(ciphertext)
print(cipher)

nC = math.ceil(len(cipher) / key)
print(nC )
nR = key
numOfShadedBoxes = (nC * nR) - len(cipher)
pt = [''] * nC
col=0
row=0
for sym in cipher:
   pt[col]+=sym
   col+=1
   if (col == nC) or (col == nC - 1 and row >= nR- numOfShadedBoxes):
       col=0
       row=row+1

print(''.join(pt))
```