Assignment NO - 2

Aim :- Write a Java/C/C++/python program to perform encryption and decryption using the method of transposition technique

Theory -

Transposition cipher is a cryptographic algorithm In this algorithm the order of alphabets in the plaintext is rearranged from a cipher tex

for example -

consider transposition cipher is column nar transposition cipher where each character in the plantext is written horizontally with specified alphabet width. the ciphar is written vertically which creates an entirely different cipher text

consider the plantest hello world and let us apply the simple columner transposition technique as shown below

h	e	l	l
o	w	o	r
l	d		

The plain text character are placed horizontaly and the cipher text is created with vertical format as holewdlolr. Also the receiver has to use the same table to decrypt the cipher text to plain text to plain text.

Transposition Techniques -

There are different transposition techniques used to encrypt and decrypt the message for this programe we used Columnar transposition tenchniques.

1 Rail fence transposition Cipher

The Rail fence Cipher is a form of transposition cipher that gets its name from the way in which it is encoded. In the rail fence cipher the plaintext is written downwards on succesive rails of an imaginary fence then mouing up when we get to the bottom the message is them read off in row

for example.

using three row's rails and a message in them read off in rows using rails and a message of 'WE ARE DISCOVREDFIFE AT ONCE the cipher writes out

```
W...  E....  C..  R     L  T  F
F     R      D ..  S     O  E  E
F     E      A . O . C ... A T ..V.. D.. E.. N.
```

Then reads off

WECRI TEERD SOEEFEAO CA IVDEN

2 Columnar transposition. In a columnar transposition 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. Both the width of the rows and the rows and the permutation of the columns are usually defined by a keyword

For example
the word ZEBRAS is of length 6 (so the rows are length 6) and the permutation is defined by the alphabetical order of the letters in the keyword ID. In this case the order would be " 6 3 2 4 1 5 "

In a Regular columnar transposition cipher any spare space are filled with nulls in an irregular columnar transposition cipher the space are left blank then he can write the message out in columns again then reorder the columns.

3) Double transposition.

A single columnar transposition could be attacked by guess positive column lengths writing the message out in its columns (but in the wrong order as the key is not yet known) and then looking anagrams this is simply a columnar transposition applied twice. the same key can be used for both transposition or two different keys can be used

4] Book cipher / Running key cipher.

The Running key cipher has the same internal working as the vigenere cipher. the difference lies in ~~to~~ how to key is chosen the running key cipher is a poly-alphabetic substituation the book cipher is a homophonic substitution. the cipher can still be broken through as there are stastical patterns in both the key and the plaintext which can be exploited. If the key for the running key cipher comes from a stastically random source then it becomes a 'one time pad' cipher the 'key' for a running key cipher is a long piece of text.

Algorithm -

Step-1 write all the characters of plain text message row by row in a rectangle of predefined size

Step. 2 Read the message in a columnar manner. i.e column by column.

Step 3 The resultant message is ciphertext

Conclusion -

In this program I learn about c language perform encryption and decryption using the method of transposition technique.