19/11/2020 **Mohd. Aftab Alam**
02013302717

EXPERIMENT 6

Aim: Write a program to perform Encryption/Decryption using Transposition Technique.

Theory:
In cryptography, a transposition cipher is a method of encryption by which the positions held by units of plaintext (which are commonly characters or groups of characters) are shifted according to a regular system, so that the ciphertext constitutes a permutation of the plaintext. That is, the order of the units is changed. Mathematically a bijective function is used on the characters' positions to encrypt and an inverse function to decrypt.

Algorithm:

Encryption:

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 e.g., 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.
5. Finally, the message is read off in columns, in the order specified by the keyword.

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.

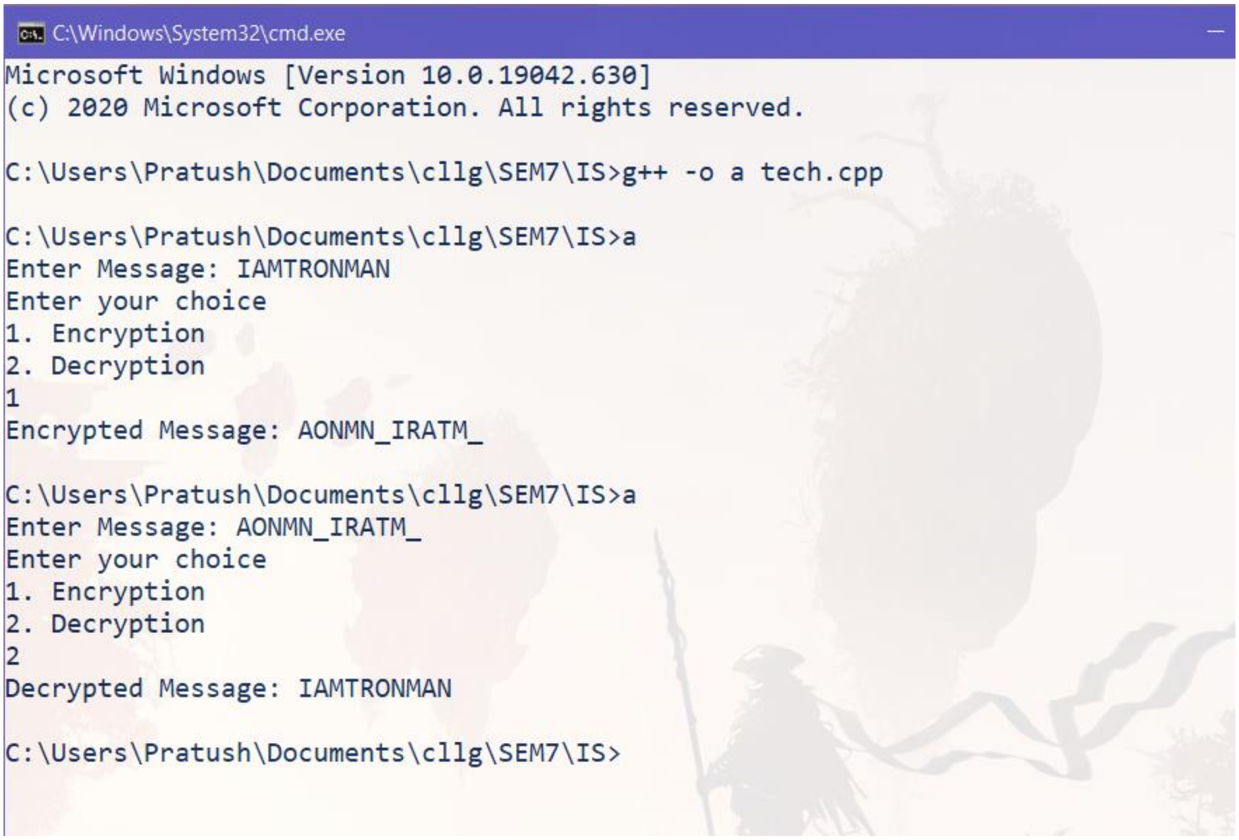
Code:

```
#include<bits/stdc++.h>
using namespace std;

string const key = "HACK";
map<int,int> keyMap;
void setPermutationOrder() {
        for(int i=0; i < key.length(); i++) {
                keyMap[key[i]] = i;
        }
}
string encryptMessage(string msg){
        int row,col,j;
        string cipher = "";
        col = key.length();
        row = msg.length()/col;
        if (msg.length() % col)
                row += 1;
        char matrix[row][col];
        for (int i=0,k=0; i < row; i++) {
                for (int j=0; j<col; ) {
```

```
                if(msg[k] == '\0') {
                    matrix[i][j] = '_';
                    j++;
                }
                if( isalpha(msg[k]) || msg[k]==' ') {
                    matrix[i][j] = msg[k];
                    j++;
                }
                k++;
            }
        }
        for (map<int,int>::iterator ii = keyMap.begin(); ii!=keyMap.end(); ++ii) {
            j=ii->second;
            for (int i=0; i<row; i++) {
                if( isalpha(matrix[i][j]) || matrix[i][j]==' ' || matrix[i][j]=='_')
                    cipher += matrix[i][j];
            }
        }
        return cipher;
}
string decryptMessage(string cipher) {
        int col = key.length();
        int row = cipher.length()/col;
        char cipherMat[row][col];
        for (int j=0,k=0; j<col; j++)
            for (int i=0; i<row; i++)
                cipherMat[i][j] = cipher[k++];
        int index = 0;
        for( map<int,int>::iterator ii=keyMap.begin(); ii!=keyMap.end(); ++ii)
            ii->second = index++;
        char decCipher[row][col];
        map<int,int>::iterator ii=keyMap.begin();
        int k = 0;
        for (int l=0,j; key[l]!='\0'; k++) {
            j = keyMap[key[l++]];
            for (int i=0; i<row; i++) {
                decCipher[i][k]=cipherMat[i][j];
            }
        }
        string msg = "";
        for (int i=0; i<row; i++) {
            for(int j=0; j<col; j++) {
                if(decCipher[i][j] != '_')
                    msg += decCipher[i][j];
            }
        }
        return msg;
}
int main(void) {
        string msg;
   int ch;
   printf("Enter Message: ");getline(cin,msg);
          setPermutationOrder();
   cout<<"Enter your choice \n1. Encryption \n2. Decryption \n";
   cin>>ch;
   if(ch==1){
             cout << "Encrypted Message: " << encryptMessage(msg)<<endl;
   }
   else if(ch==2){
      cout << "Decrypted Message: " << decryptMessage(msg)<<endl;
   }
          return 0;
}
```

Output:



```
Microsoft Windows [Version 10.0.19042.630]
(c) 2020 Microsoft Corporation. All rights reserved.

C:\Users\Pratush\Documents\cllg\SEM7\IS>g++ -o a tech.cpp

C:\Users\Pratush\Documents\cllg\SEM7\IS>a
Enter Message: IAMTRONMAN
Enter your choice
1. Encryption
2. Decryption
1
Encrypted Message: AONMN_IRATM_

C:\Users\Pratush\Documents\cllg\SEM7\IS>a
Enter Message: AONMN_IRATM_
Enter your choice
1. Encryption
2. Decryption
2
Decrypted Message: IAMTRONMAN

C:\Users\Pratush\Documents\cllg\SEM7\IS>
```