

Experiment No: 4

Aim: To study and implementation of Transposition Cipher.

Introduction: In this Transposition Cipher method of cryptography, positions of alphabets in plaintext is shifted according to key and give a permutation of the plaintext.

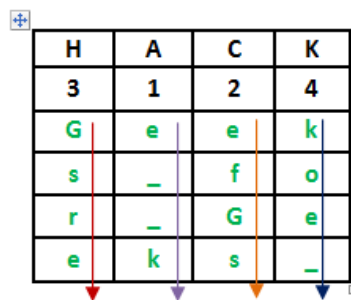
Encryption

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 kefGsGsrekeoe_

This is how the Transposition cipher can be implemented and is implemented below. We can add any dummy letters in the end of the matrix. Here we have taken ‘_’(Underscore) as a dummy letter.

Program (Source Code):

```
#include<iostream>
#include<string>
using namespace std;

int encry(string key, string pt)
{
    int row;
    int col = key.length();
    if(pt.length() % key.length() == 0)
    {
        row=pt.length() / key.length();
    }
    else
    {
        row=(pt.length() / key.length()) + 1;
    }

    char mat[row][col];
    for(int i=0; i<row; i++)
    {
```

```

        for(int j=0; j<col; j++)
        {
            //blank space in the matrix is replaced by '_'
            mat[i][j] = '_';
        }
    }

    int k=0;
    for(int i=0; i<row; i++)
    {
        for(int j=0; j<col; j++)
        {
            if(k<pt.length())
            {
                mat[i][j] = pt[k++];
            }
        }
    }

    int arr[col];
    int temp = 1;
    string alpha = "abcdefghijklmnopqrstuvwxyz";
    for(int i=0; i<alpha.length(), temp <= col; i++)
    {
        for(int j=0; j<col; j++)
        {
            if(alpha[i] == key[j])
            {
                arr[j] = temp;
                temp++;
            }
        }
    }

    int tra=1;
    for(int i=0; i<col; i++)
    {
        for(int j=0; j<col; j++)
        {
            if(arr[j] == tra)
            {
                for(int i=0; i<row; i++)
                {
                    cout<<mat[i][j];
                }
                tra++;
            }
        }
    }

```

```

        return 0;
    }

int decry(string key, string pt)
{
    int row;
    int col = key.length();
    if(pt.length() % key.length() == 0)
    {
        row=pt.length() / key.length();
    }
    else
    {
        row=(pt.length() / key.length()) + 1;
    }

    char mat[row][col];

    int arr[col];
    int temp = 1;
    string alpha = "abcdefghijklmnopqrstuvwxyz";
    for(int i=0; i<alpha.length(), temp <= col; i++)
    {
        for(int j=0; j<col; j++)
        {
            if(alpha[i] == key[j])
            {
                arr[j] = temp;
                temp++;
            }
        }
    }

    int tra=1,z=0;
    for(int i=0; i<col; i++)
    {
        for(int j=0; j<col; j++)
        {
            if(arr[j] == tra)
            {
                for(int i=0; i<row; i++)
                {
                    mat[i][j] = pt[z++];
                }
                tra++;
            }
        }
    }

    int k=0;

```

```

        for(int i=0; i<row; i++)
        {
            for(int j=0; j<col; j++)
            {
                if(mat[i][j] != '_')
                {
                    cout<<mat[i][j];
                }
            }
        }

        return 0;
    }

int main()
{
    string key;
    cout<<"Enter a key using small alphabets only(transposition cipher)"<<endl;
    getline(cin>>ws, key);
    string pt;
    cout<<"Enter plaintext"<<endl;
    getline(cin>>ws, pt);

    int choice;
    cout<<"Press 1 to encipher the text"<<endl;
    cout<<"Press 2 to decipher the text"<<endl;
    cin>>choice;

    switch(choice)
    {
    case 1:
        cout<<"Encrypted output:"<<endl;
        encry(key, pt);
        break;

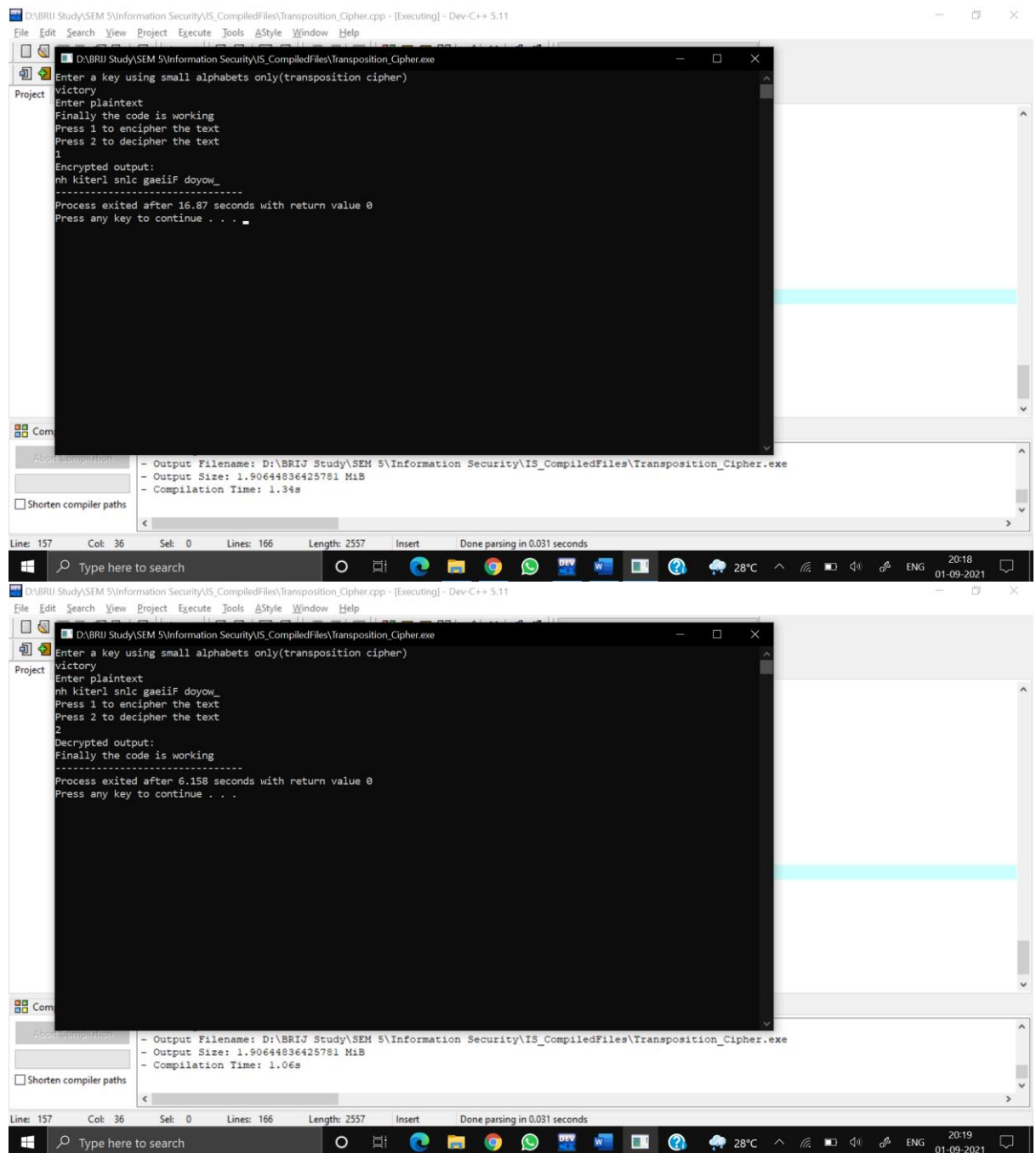
    case 2:
        cout<<"Decrypted output:"<<endl;
        decry(key, pt);
        break;

    default:
        cout<<"Try again next time"<<endl;
    }

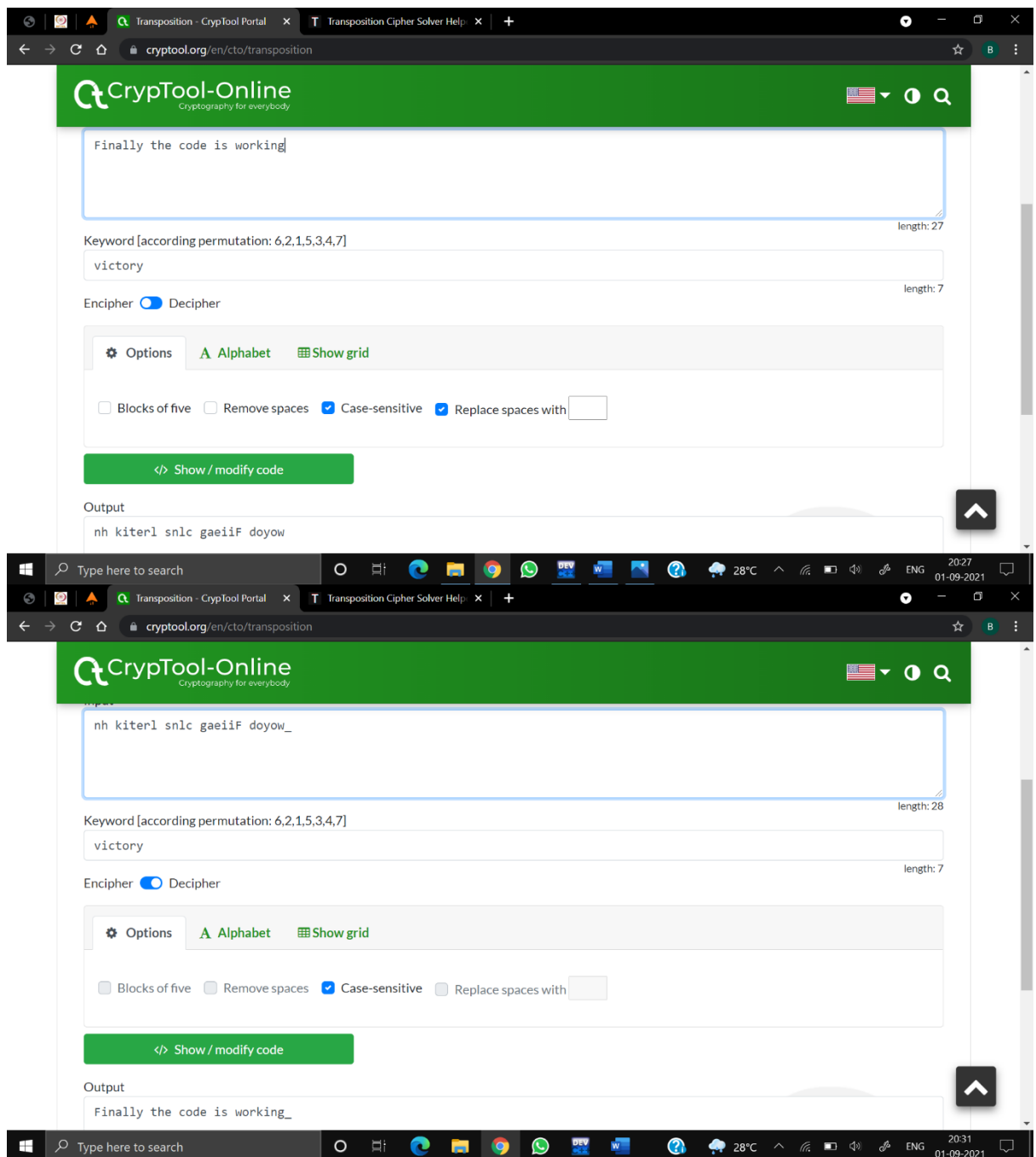
    return 0;
}

```

Output (Program):



Output (Cryptool):



Cryptanalysis:

The process of attempting to discover X or K or both is known as cryptanalysis. The strategy used by the cryptanalysis depends on the nature of the encryption scheme and the information available to the cryptanalyst. There are various types of cryptanalytic attacks based on the amount of information known to the cryptanalyst. Cipher text only – A copy of cipher text alone is known to the cryptanalyst. Known plaintext – The cryptanalyst has a copy of the cipher text and the corresponding plaintext. Chosen plaintext – The cryptanalysts gain temporary access to the encryption machine. They cannot open it to find the key, however; they can encrypt a large number of suitably chosen plaintexts and try to use the resulting cipher texts to deduce the key. Chosen cipher text – The cryptanalyst obtains temporary access to the decryption machine,

uses it to decrypt several strings of symbols, and tries to use the results to deduce the key.

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. The Columnar Transposition was used for serious purposes all over the world, until the beginning of the second half of the 20th century. To break the ciphertext, an attacker should try to create the tables of different sizes, enter the encrypted message down into the columns, and for each table look for anagrams appearing in rows. Cryptanalysts observed a significant improvement in crypto security when transposition technique is performed. They also noted that re-encrypting the cipher text using same transposition cipher creates better security.

Applications:

- 1) Probably one of the oldest known implementations of the transposition cipher was the Spartan Scytale (also commonly spelled as Skytale).
- 2) In ancient Greece (around 475 B.C.), the Spartan army commanders created a Scytale, a device they designed for sending secret messages.

References:

1. <https://www.geeksforgeeks.org/columnar-transposition-cipher/>
2. <https://www.youtube.com/watch?v=Q9s6PwcVzDU>
3. https://en.wikipedia.org/wiki/Transposition_cipher
4. https://www.google.com/url?sa=i&url=https%3A%2F%2Fwww.geeksforgeeks.org%2Fcolumnar-transposition-cipher%2F&psig=AOvVaw2dbvJNw4-on72wu_CaihD2&ust=1630595344751000&source=images&cd=vfe&ved=0CAsQjRxqFwoTCKC4wpWH3vICFQAAAAAdAAAAABAD