**U18CO018**

**Shekhaliya Shubham**

**CNS**

**Lab Assignment 2**

- Implement columnar transposition cipher.

Code:

```
#include <bits/stdc++.h>

using namespace std;

string encryption(string plainText, string key) {

    int n = plainText.length();

    int col = key.length();
    int row = ceil(n*1.0/col);

    char matrix[row][col];

    int p = 0;
    for(int i = 0;i<row;i++) {
        for(int j = 0;j<col;j++) {
            matrix[i][j] = (p>=n) ? '_' : plainText[p++];
        }
    }

    map<int, vector<int>> map;

    for(int i = 0;i<key.length();i++) {
        map[key[i]].emplace_back(i);
    }

    string cipherText = "";

    for(auto it : map) {
        for(auto j: it.second) {
            for(int i = 0;i<row;i++) {
                cipherText += matrix[i][j];
```

```
            }
        }
    }

    return cipherText;
}

string decryption(string cipherText, string key) {
    int n = cipherText.length();
    int col = key.length();
    int row = ceil(n*1.0/col);

    char matrix[row][col];

    map<int, vector<int>> map;

    for(int i = 0;i<key.length();i++) {
        map[key[i]].emplace_back(i);
    }

    int p = 0;
    for(auto it : map) {
        for(auto j: it.second) {
            for(int i = 0;i<row;i++) {
                matrix[i][j] = cipherText[p++];
            }
        }
    }

    string plainText = "";
    for(int i = 0;i<row;i++) {
        for(int j = 0;j<col;j++) {
            if(matrix[i][j] == '_') {
                i = row;
                break;
            }
            plainText += matrix[i][j];
        }
    }

    return plainText;
}

string readFrom(string filename)
{
    ifstream file;
    string input = "", result = "";
    file.open(filename);
```

```
    while (!file.eof())
    {
        getline(file, input);
        result += input + "\n";
    }
    file.close();
    return result.substr(0, result.length() - 1);
}

void writeTo(string filename, string message)
{
    ofstream file;
    file.open(filename);
    file << message;
    file.close();
}

int main() {

    string key = "";

    int ch = 0;

    while(true) {

        cout<<"1. Encryption\n";
        cout<<"2. Decryption\n";

        cin>>ch;

        if(ch == 1) {

            string plainText = readFrom("input.txt");
            cout<<"Enter the key"<<endl;
            cin>>key;

            string cipherText = encryption(plainText, key);
            writeTo("output1.txt", cipherText);

            cout<<"plain Text :: \n";
            cout<<plainText<<"\n\n";

            cout<<"cipher Text :: \n";
            cout<<cipherText<<"\n\n";

        } else if (ch == 2) {

            string cipherText = readFrom("output1.txt");
```

```
            cout<<"Enter the key"<<endl;
            cin>>key;

            string plainText = decryption(cipherText, key);
            writeTo("output2.txt", plainText);

            cout<<"cipher Text :: \n";
            cout<<cipherText<<"\n\n";

            cout<<"plain Text :: \n";
            cout<<plainText<<"\n\n";

        } else {
            break;
        }
    }

    return 0;
}
```

```
E:\Asem7\CNS\Assignment2>g++ a.cpp

E:\Asem7\CNS\Assignment2>a.exe
1. Encryption
2. Decryption
1
Enter the key
SECUREKEY
plain Text ::
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

cipher Text ::
 arirtn  tdsnioh sardnestctur l_nrtteeenhiltihccspraeiry  xtenp_yys sdy enyfx oa fesctlmthost n_t oiaothp
up rltrcsio r
trsathe_p,pc  pw s  tancg rhcoa, en att_rhnnioryhoboehmrrot a ueapceufi_Ig ihm ocseiaw  rua
td soeeipo tcpao hcbti  tcmao ce ggthi tmoa_oasp fiiohnl(eyeoh)fra shtt iex_

1. Encryption
2. Decryption
2
Enter the key
SECUREKEY
cipher Text ::
 arirtn  tdsnioh sardnestctur l_nrtteeenhiltihccspraeiry  xtenp_yys sdy enyfx oa fesctlmthost n_t oiaothp
up rltrcsio r
trsathe_p,pc  pw s  tancg rhcoa, en att_rhnnioryhoboehmrrot a ueapceufi_Ig ihm ocseiaw  rua
td soeeipo tcpao hcbti  tcmao ce ggthi tmoa_oasp fiiohnl(eyeoh)fra shtt iex_

plain Text ::
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

1. Encryption
2. Decryption
3

E:\Asem7\CNS\Assignment2>
```

Plain Text :

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

Cipher Text:

arirtn  tdsnioh sardnestctur l_nrtteeenhiltihccspraeiry  xtenp_yys sdy enyfx oa fesctlmthost n_t oiaothp

up rltrcsio r

trsathe_p,pc  pw s  tancg rhcoa, en att_rhnnioryhoboehmrrot a ueapceufi_lg ihm ocseiaw rua

td soeeipo tcpao hcbti  tcmao ce ggthi tmoa_oasp fiiohnl(eyeoh)fra shtt iex_

- Implement rail fence transposition cipher

Code:

```
#include <bits/stdc++.h>

using namespace std;

string encryption(string plainText, int key) {

    int n = key;
    vector<vector<char>> matrix(n);

    int k = 0;
    int f = 1;
    for(char c : plainText) {
        matrix[k].emplace_back(c);
        if(k + 1 == n) {
            f = -1;
        } else if (k == 0) {
            f = 1;
        }
        k += f;
    }

    string cipherText = "";

    for(auto vi : matrix) {
        for(auto c : vi) {
            cipherText += c;
        }
    }

    return cipherText;
}

string decryption(string cipherText, int key) {

    int row = key;
    int col = cipherText.length();
    vector<vector<char>> matrix(row, vector<char>(col, '_'));
    bool down = false;
```

```
    int j = 0;
    for (int i = 0; i < col; i++)
    {
        if (j == 0 || j == row - 1)
            down = !down;
        matrix[j][i] = '*';
        down ? j++ : j--;
    }
    int k = 0;
    for (int i = 0; i < row; i++)
    {
        for (j = 0; j < col; j++)
        {
            if (matrix[i][j] == '*' && k < col)
            {
                matrix[i][j] = cipherText[k++];
            }
        }
    }

    j = 0;
    down = false;
    string plainText = "";
    for (int i = 0; i < col; i++)
    {
        if (j == 0 || j == row - 1)
            down = !down;
        plainText += matrix[j][i];
        down ? j++ : j--;
    }
    return plainText;
}

string readFrom(string filename)
{
    ifstream file;
    string input = "", result = "";
    file.open(filename);
    while (!file.eof())
    {
        getline(file, input);
        result += input + "\n";
    }
    file.close();
    return result.substr(0, result.length() - 1);
}

void writeTo(string filename, string message)
```

```
{
    ofstream file;
    file.open(filename);
    file << message;
    file.close();
}

int main() {

    int key = 0;

    int ch = 0;

    while(true) {

        cout<<"1. Encryption\n";
        cout<<"2. Decryption\n";

        cin>>ch;
        if(ch == 1) {

            string plainText = readFrom("input.txt");
            cout<<"Enter the key"<<endl;
            cin>>key;

            string cipherText = encryption(plainText, key);
            writeTo("output3.txt", cipherText);

            cout<<"plain Text :: \n";
            cout<<plainText<<"\n\n";

            cout<<"cipher Text :: \n";
            cout<<cipherText<<"\n\n";

        } else if (ch == 2) {

            string cipherText = readFrom("output3.txt");
            cout<<"Enter the key"<<endl;
            cin>>key;

            string plainText = decryption(cipherText, key);
            writeTo("output4.txt", plainText);

            cout<<"cipher Text :: \n";
            cout<<cipherText<<"\n\n";

            cout<<"plain Text :: \n";
            cout<<plainText<<"\n\n";
```

```
        } else {
            break;
        }
    }

    return 0;
}
```

```
E:\Asem7\CNS\Assignment2>g++ b.cpp

E:\Asem7\CNS\Assignment2>a.exe
1. Encryption
2. Decryption
1
Enter the key
5
plain Text ::
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

cipher Text ::
Io p ihnnco
 fecocrocrsageyohrnsuolntg,asonc stoeco ihpsshyuo txihcm hesru hes h cn rgsss teetose mt fpat pry nsoir ed ribh  inebn pnth  myat gpfat)eidcit u t
t  hecttaran  ixcyahtaiipeam fytywtetol isli waeolrco sorc
rfeodoalre,htcpx iu etotenerprth op hidta(rnar aatr amaittpiht

1. Encryption
2. Decryption
2
Enter the key
5
cipher Text ::
Io p ihnnco
 fecocrocrsageyohrnsuolntg,asonc stoeco ihpsshyuo txihcm hesru hes h cn rgsss teetose mt fpat pry nsoir ed ribh  inebn pnth  myat gpfat)eidcit u t
t  hecttaran  ixcyahtaiipeam fytywtetol isli waeolrco sorc
rfeodoalre,htcpx iu etotenerprth op hidta(rnar aatr amaittpiht

plain Text ::
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

1. Encryption
2. Decryption
3

E:\Asem7\CNS\Assignment2>
```

Plain Text :

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

Cipher Text:

Io p ihnnco

fecocrocrsageyohrnsuolntg,asonc stoeco ihpsshyuo txihcm hesru hes h cn rgsss teetose mt fpat pry nsoir ed ribh inebn pnth myat gpfat)eidcit u t

t hecttaran ixcyahtaiipeam fytywtetol isli waeolrco sorc

rfeodoalre,htcpx iu etotenerprth op hidta(rnar aatr amaittpiht