U18CO018

Shekhaliya Shubham

CNS

Assignment 1

Implement a menu driven program for Caesar Cipher with following functions:

a. Encrypt given plain text.
b. Decrypt given cipher text.
c. Find encryption key using brute force attack.
d. Find encryption key using frequency analysis attack.

Code:

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

using namespace std;

string encrypt(string plainText, int key)
{
    string cipherText = "";

    for (int i = 0; i < plainText.length(); i++)
    {
        if (isupper(plainText[i]))
            cipherText += char(int(plainText[i] + key - 'A') % 26 + 'A');
        else if (islower(plainText[i]))
            cipherText += char(int(plainText[i] + key - 'a') % 26 + 'a');
        else if (plainText[i] >= '0' && plainText[i] <= '9')
            cipherText += char(int(plainText[i] + key - '0') % 10 + '0');
        else
            cipherText += plainText[i];
    }

    return cipherText;
}

string decrypt(string cipherText, int key)
{
    string plainText = "";

    for (int i = 0; i < cipherText.length(); i++)
```

```
    {

        if (isupper(cipherText[i]))
            plainText += (cipherText[i] - 'A' - key + 26) % 26 + 'A';
        else if (islower(cipherText[i]))
            plainText += (cipherText[i] - 'a' - key + 26) % 26 + 'a';
        else if (cipherText[i] >= '0' && cipherText[i] <= '9')
            plainText += (cipherText[i] - '0' - key + 26) % 26 + '0';
        else
            plainText += cipherText[i];
    }

    return plainText;
}

void findEncryptionKeyUsingBruteForce(string plainText, string cipherText)
{
    int flag = -1;

    for (int key = 0; key < 26; key++)
    {
        string text = decrypt(cipherText, key);
        if (plainText == text)
        {
            flag = key;
            break;
        }
    }

    if (flag != 0)
        cout << "The key is: " << flag << endl;
    else
        cout << "Key not found" << endl;
}

void findEncryptionKeyUsingFrequencyAnalysis(string text)
{
    string freq = "etaoinshrdlcumwfgypbvkjxqz";

    vector<int> frequency(26);

    for (int i = 0; i < text.length(); i++)
    {
        if (text[i] >= 'a' && text[i] <= 'z')
            frequency[text[i] - 'a']++;
    }

    int max = 0;
```

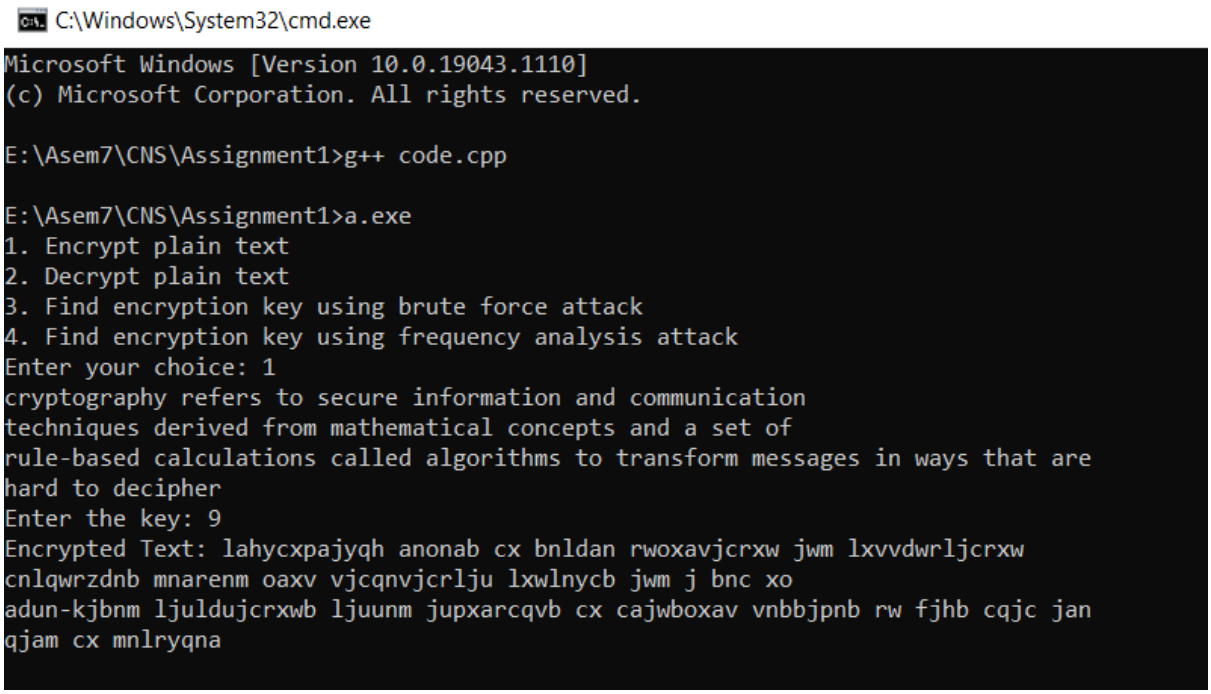
```
    vector<char> ch;

    for (int i = 0; i < 26; i++)
    {
        if (frequency[i] > max)
        {
            ch.clear();
            max = frequency[i];
            ch.push_back(i + 'a');
        }
        else if (frequency[i] == max)
        {
            ch.push_back(i + 'a');
        }
    }

    char input;

    for (int i = 0; i < freq.length(); i++)
    {
        for (char d : ch)
        {
            int key = d - freq[i];

            if (key < 0)
                key += 26;

            cout << decrypt(text, key) << endl;
            cout << "Is it correct plain text? Y/N" << endl;
            cin >> input;
            if (input == 'Y')
            {
                cout << "The Encryption key is : " << key;
                return;
            }
        }
        cout << endl;
    }
}

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 input;

    int key, choice;
    cout << "1. Encrypt plain text" << endl;
    cout << "2. Decrypt plain text" << endl;
    cout << "3. Find encryption key using brute force attack" << endl;
    cout << "4. Find encryption key using frequency analysis attack" << endl;
    cout << "Enter your choice: ";
    cin >> choice;

    switch (choice)
    {
    case 1:
    {

        string plainText = readFrom("input1.txt");

        cout << plainText << endl;

        cout << "Enter the key: ";
        cin >> key;
        string cipherText = encrypt(plainText, key);
        cout << "Encrypted Text: " << cipherText << endl;

        writeTo("output1.txt", cipherText);

        break;
    }

    case 2:
    {
        string cipherText = readFrom("output1.txt");
```

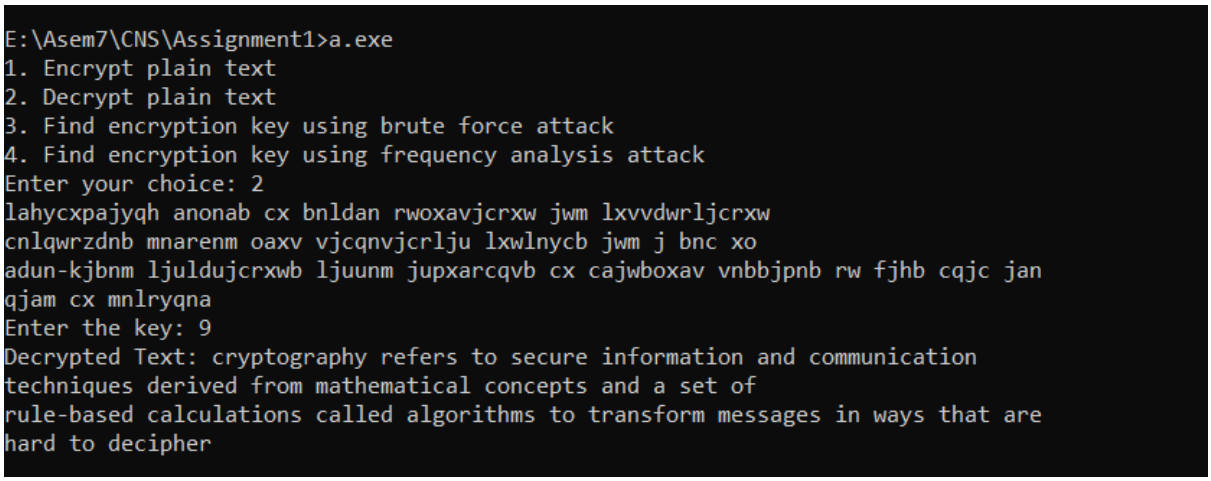
```
            cout << cipherText << endl;

            cout << "Enter the key: ";
            cin >> key;
            string plainText = decrypt(cipherText, key);
            cout << "Decrypted Text: " << plainText << endl;

            writeTo("output2.txt", plainText);

            break;
        }

        case 3:
        {
            string plainText = readFrom("input1.txt");
            string cipherText = readFrom("output1.txt");

            cout << plainText << endl;
            cout << cipherText << endl;

            findEncryptionKeyUsingBruteForce(plainText, cipherText);
            break;
        }

        case 4:
        {
            string cipherText = readFrom("output1.txt");

            cout << cipherText << endl;

            findEncryptionKeyUsingFrequencyAnalysis(cipherText);
            break;
        }
        default:
            cout << "You have entered wrong choice!!" << endl;
            break;
        }
        return 0;
}
```

Ans.

A.


C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.19043.1110]
(c) Microsoft Corporation. All rights reserved.
E:\Asem7\CNS\Assignment1>g++ code.cpp
E:\Asem7\CNS\Assignment1>a.exe
1. Encrypt plain text
2. Decrypt plain text
3. Find encryption key using brute force attack
4. Find encryption key using frequency analysis attack
Enter your choice: 1
cryptography refers to secure information and communication
techniques derived from mathematical concepts and a set of
rule-based calculations called algorithms to transform messages in ways that are
hard to decipher
Enter the key: 9
Encrypted Text: lahycxpajyqh anonab cx bnldan rwoxavjcrxw jwm lxvvdwrljcrxw
cnlqwrzdnb mnarenm oaxv vjcqnvjcrlju lxwlnycb jwm j bnc xo
adun-kjbnm ljuldujcrxwb ljuunm jupxarcqvb cx cajwboxav vnbbjpnb rw fjhb cqjc jan
qjam cx mnlryqna

B.


E:\Asem7\CNS\Assignment1>a.exe
1. Encrypt plain text
2. Decrypt plain text
3. Find encryption key using brute force attack
4. Find encryption key using frequency analysis attack
Enter your choice: 2
lahycxpajyqh anonab cx bnldan rwoxavjcrxw jwm lxvvdwrljcrxw
cnlqwrzdnb mnarenm oaxv vjcqnvjcrlju lxwlnycb jwm j bnc xo
adun-kjbnm ljuldujcrxwb ljuunm jupxarcqvb cx cajwboxav vnbbjpnb rw fjhb cqjc jan
qjam cx mnlryqna
Enter the key: 9
Decrypted Text: cryptography refers to secure information and communication
techniques derived from mathematical concepts and a set of
rule-based calculations called algorithms to transform messages in ways that are
hard to decipher

C.

```
E:\Asem7\CNS\Assignment1>a.exe
1. Encrypt plain text
2. Decrypt plain text
3. Find encryption key using brute force attack
4. Find encryption key using frequency analysis attack
Enter your choice: 3
cryptography refers to secure information and communication
techniques derived from mathematical concepts and a set of
rule-based calculations called algorithms to transform messages in ways that are
hard to decipher
lahycxpajyqh anonab cx bnldan rwoxavjcrxw jwm lxvvdwrljcrxw
cnlqwrzdnb mnarenm oaxv vjcqnvjcrlju lxwlnycb jwm j bnc xo
adun-kjbnm ljuldujcrxwb ljuunm jupxarcqvb cx cajwboxav vnbbjpnb rw fjhb cqjc jan
qjam cx mnlryqna
The key is: 9
```

D.

```
E:\Asem7\CNS\Assignment1>a.exe
1. Encrypt plain text
2. Decrypt plain text
3. Find encryption key using brute force attack
4. Find encryption key using frequency analysis attack
Enter your choice: 4
lahycxpajyqh anonab cx bnldan rwoxavjcrxw jwm lxvvdwrljcrxw
cnlqwrzdnb mnarenm oaxv vjcqnvjcrlju lxwlnycb jwm j bnc xo
adun-kjbnm ljuldujcrxwb ljuunm jupxarcqvb cx cajwboxav vnbbjpnb rw fjhb cqjc jan
qjam cx mnlryqna
gvctxskvetlc vijivw xs wigyvi mrjsvqexmsr erh gsqqyrmgexmsr
xiglrmuyiw hivmzih jvsq qexliqexmgep gsrgitxw erh e wix sj
vypi-fewih gepgypexmsrw geppih epksvmxlqw xs xverwjsvq qiwwekiw mr aecw xlex evi
levh xs higmtliv
Is it correct plain text? Y/N
N

vkrimhzktiar kxyxkl mh lxvnkx bgyhkftmbhg tgw vhffngbvtmbhg
mxvagbjnxl wxkboxw ykhf ftmaxftmbvte vhgvximl tgw t lxm hy
knex-utlxw vtevnetmbhgl vteexw tezhkbmafl mh mktglyhkf fxlltzxl bg ptrl matm tkx
atkw mh wxvbiaxk
Is it correct plain text? Y/N
N

cryptography refers to secure information and communication
techniques derived from mathematical concepts and a set of
rule-based calculations called algorithms to transform messages in ways that are
hard to decipher
Is it correct plain text? Y/N
Y
The Encryption key is : 9
```

Input1.txt

cryptography refers to secure information and communication
techniques derived from mathematical concepts and a set of
rule-based calculations called algorithms to transform messages in ways that are
hard to decipher