CS302 Information Security and Cryptography

Assignment - 1

U20CS135

1. Implement a menu driven program for Caesar Cipher with following functions.

a. Encrypt given plain text.

Code

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

int main()
{
    map<char,char>m;
    map<int,char>ma;
    for(int i=0;i<26;i++)
    {
        ma[i]=i+97;
    }
    string s;
    cin>>s;
    string sj;
    int j;
    cin>>j;
    for(int i=0;i<26;i++)
    {
         char c=ma[i];
         int k=(i+j)%26;
         char ck=ma[k];
         m[c]=ck;
    }

    for(int i=0;i<s.length();i++)
    {

        sj+=m[s[i]];
    }
    cout<<sj<<endl;

    return 0;
}
```

Output

```
SHIVAM@LAPTOP-6H150TV6 MINGW64 ~/OneDrive/Desktop/CourseWork/ict/Assignment 1
$ g++ 1.cpp -o 1

SHIVAM@LAPTOP-6H150TV6 MINGW64 ~/OneDrive/Desktop/CourseWork/ict/Assignment 1
$ ./1
shivam
3
vklydp
```

---

b. Decrypt given cipher text.

Code

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

int main()
{

    map<int,char>ma;
    for(int i=0;i<26;i++)
    {
        ma[i]=i+97;
    }
    string s;
    cin>>s;
    string sj;
    int j;
    cin>>j;

    for(int i=0;i<s.length();i++)
    {

        int k=j%26;
        int f=s[i]-'0'-49;
        k=f-k;
        if(k<0)
        k+=26;
        sj+=ma[k];

    }
    cout<<sj<<endl;

    return 0;
}
```

Output

```
SHIVAM@LAPTOP-6H150TV6 MINGW64 ~/OneDrive/Desktop/CourseWork/ict/Assignment 1
$ g++ 2.cpp -o 2

SHIVAM@LAPTOP-6H150TV6 MINGW64 ~/OneDrive/Desktop/CourseWork/ict/Assignment 1
$ ./2
vklydp
3
shivam
```

---

c. Find encryption key using brute force attack.

```
#include<bits/stdc++.h>
using namespace std;
void decrypt(string x)
    {
    string text;
    for(int n=0;n<26;n++)
        {
        text = "";
        for(int i=0;i<x.length();i++)
            {
            if(isupper(x[i]))
                {
                if((x[i] - n - 65)<0)
                    text += 91 + (x[i] - n - 65);
                else
                    text += (x[i] - n - 65)%26 + 65;
                }
            else if(islower(x[i]))
                {
                if((x[i] - n - 97) < 0)
                    text += 123 + (x[i] - n - 97);
                else
                    text += (x[i] - n - 97)%26 + 97;
                }
            else
                text += x[i];
            }
        cout << "plain text for key " << n << " :- " << text << endl;
        }
    }
int main()
{

    string text;
    getline(cin,text);
    decrypt(text);
```

```
    return 0;
}
```

Output

```
SHIVAM@LAPTOP-6H150TV6 MINGW64 ~/OneDrive/Desktop/CourseWork/ict/Assignment 1
$ g++ 2.cpp -o 2

SHIVAM@LAPTOP-6H150TV6 MINGW64 ~/OneDrive/Desktop/CourseWork/ict/Assignment 1
$ ./3
sdflknsd lljdlsf lkds kd
plain text for key 0 :- sdflknsd lljdlsf lkds kd
plain text for key 1 :- rcekjmrc kkickre kjcr jc
plain text for key 2 :- qbdjilqb jjhbjqd jibq ib
plain text for key 3 :- pacihkpa iigaipc ihap ha
plain text for key 4 :- ozbhgjoz hhfzhob hgzo gz
plain text for key 5 :- nyagfiny ggeygna gfyn fy
plain text for key 6 :- mxzfehmx ffdxfmz fexm ex
plain text for key 7 :- lwyedglw eecwely edwl dw
plain text for key 8 :- kvxdcfkv ddbvdkx dcvk cv
plain text for key 9 :- juwcbeju ccaucjw cbuj bu
plain text for key 10 :- itvbadit bbztbiv bati at
plain text for key 11 :- hsuazchs aaysahu azsh zs
plain text for key 12 :- grtzybgr zzxrzgt zyrg yr
plain text for key 13 :- fqsyxafq yywqyfs yxqf xq
plain text for key 14 :- eprxwzep xxvpxer xwpe wp
plain text for key 15 :- doqwvydo wwuowdq wvod vo
plain text for key 16 :- cnpvuxcn vvtnvcp vunc un
plain text for key 17 :- bmoutwbm uusmubo utmb tm
plain text for key 18 :- alntsval ttrltan tsla sl
plain text for key 19 :- zkmsruzk ssqkszm srkz rk
plain text for key 20 :- yjlrqtyj rrpjryl rqjy qj
plain text for key 21 :- xikqpsxi qqoiqxk qpix pi
plain text for key 22 :- whjporwh ppnhpwj pohw oh
plain text for key 23 :- vgionqvg oomgovi ongv ng
plain text for key 24 :- ufhnmpuf nnlfnuh nmfu mf
plain text for key 25 :- tegmlote mmkemtg mlet le
```

d.Find encryption key using frequency analysis attack.

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

using namespace std;

int main()
{

    string text;
    getline(cin,text);
    map<char,int>m;
```

```
    for(int i=0;i<text.length();i++)
    {
        if(text[i]!=' ')
        m[text[i]]++;
    }
    int maxi=0;
    char c;
    for(auto x:m)
    {
        if(x.second>maxi)
        {
            maxi=x.second;
            c=x.first;

        }
    }
    // cout<<c<<endl;

    int key=abs((int)(101-c));
    cout<<key<<endl;
    return 0;
}
```

Output

```
SHIVAM@LAPTOP-6H150TV6 MINGW64 ~/OneDrive/Desktop/CourseWork/ict/Assignment 1
$ g++ 4.cpp -o 4

SHIVAM@LAPTOP-6H150TV6 MINGW64 ~/OneDrive/Desktop/CourseWork/ict/Assignment 1
$ ./4
ljsdf lsdfk sldlfk
7
```

SUBMITTED BY: U20CS135

Shivam Mishra