Information Security & Cryptography

Nehal Jhajharia
Lab 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.

```
#include <iostream>
#include <fstream>
#include <string>

using namespace std;

int freq[26] = {0};

int setKey(int key) {
    return key % 26;
}

int getKey(char mode, char mode_gen) {
    int key = mode_gen - mode;
    if (key < 0) {
        key = 26 + key;
    }

    return 26 - key;
}

char encrypt(char ch, int key) {
    if (isupper(ch)) {
        return char (int (ch + key - 65) % 26 + 65);
    } else if (islower(ch)) {
        return char (int (ch + key - 97) % 26 + 97);
    }

    return ch;
}

string encrypt(string text, int key) {
    string result = "";

    for (int i = 0; i < text.length(); i++) {
        result += encrypt(text[i], key);
    }

    return result;
}

string decrypt(string text, int key) {
    return encrypt(text, 26 - setKey(key));
}
```

```
void setFrequency(string text) {
    for (int i = 0; i < text.length(); i++) {
        if (text[i] >= 'a' && text[i] <= 'z') {
            freq[text[i] - 97]++;
        }
    }
}

char getMode() {
    int mode = 0;
    for (int i = 1; i < 26; i++) {
        if (freq[i] > freq[i - 1]) {
            mode = i;
        }
    }
    freq[mode] = 0;

    return (char)(97 + mode);
}

void bruteForceAttack(string text) {
    for (int i = 0; i < 26; i++) {
        cout << "Key = " << i << " : \n" << encrypt(text, i) << endl;
    }
}

void frequencyAttack(string S) {
    setFrequency(S);
    string freq_table = "etaoinshrdlcumwfgypbvkjxqz";

    int key = 0;
    char mode = '\0';
    for (int i = 0; i < freq_table.length(); i++) {
        mode = getMode();
        key = getKey(mode, freq_table[i]);
        cout << mode << " -> " << freq_table[i] << " : \n" << decrypt(S, key) << endl;
    }
}

int main() {
    string text = "";
    int key = 4;

    fstream new_file;
    new_file.open("input.txt", ios::in);
    if (new_file.is_open()) {
        string tp;
        while(getline(new_file, tp)) {
            text += tp;
            text += "\n";
        }
        new_file.close();
    }

    string enc = encrypt(text, key);
    string dec = decrypt(enc, key);

    cout << text << endl;
    cout << "Key = " << key << endl << endl;

    cout << "Encrypting..." << endl << enc << endl;
    cout << "Decrypting..." << endl << dec << endl;

    cout << "\n********** Brute Force Method **********\n";
    bruteForceAttack(text);

    cout << "\n********** Frequency Analysis Method **********\n";
    frequencyAttack(text);
}
```

```
jhajharia@Nehals-MacBook-Air Asmt1 % clang++ cipher.cpp
```

```
jhajharia@Nehals-MacBook-Air Asmt1 % ./a.out
hello world it's incredible
what is to be explored further in the galaxy

Key = 4

Encrypting...
lipps asvph mx'w mrgvihmfpi
alex mw xs fi ibtpsvih jyvxliv mr xli kepebc

Decrypting...
hello world it's incredible
what is to be explored further in the galaxy


********** Brute Force Method **********
Key = 0 :
hello world it's incredible
what is to be explored further in the galaxy

Key = 1 :
ifmmp xpsme ju't jodsfejcmf
xibu jt up cf fyqmpsfe gvsuifs jo uif hbmbyz

Key = 2 :
jgnnq yqtnf kv'u kpetgfkdng
yjcv ku vq dg gzrnqtgf hwtvjgt kp vjg icncza

Key = 3 :
khoor zruog lw'v lqfuhgleoh
zkdw lv wr eh hasoruhg ixuwkhu lq wkh jdodab

Key = 4 :
lipps asvph mx'w mrgvihmfpi
alex mw xs fi ibtpsvih jyvxliv mr xli kepebc
```

```
Key = 5 :
mjqqt btwqi ny'x nshwjingqj
bmfy nx yt gj jcuqtwji kzwymjw ns ymj lfqfcd

Key = 6 :
nkrru cuxrj oz'y otixkjohrk
cngz oy zu hk kdvruxkj laxznkx ot znk mgrgde

Key = 7 :
olssv dvysk pa'z pujylkpisl
doha pz av il lewsvylk mbyaoly pu aol nhshef

Key = 8 :
pmttw ewztl qb'a qvkzmlqjtm
epib qa bw jm mfxtwzml nczbpmz qv bpm oitifg

Key = 9 :
qnuux fxaum rc'b rwlanmrkun
fqjc rb cx kn ngyuxanm odacqna rw cqn pjujgh

Key = 10 :
rovvy gybvn sd'c sxmbonslvo
grkd sc dy lo ohzvybon pebdrob sx dro qkvkhi

Key = 11 :
spwwz hzcwo te'd tyncpotmwp
hsle td ez mp piawzcpo qfcespc ty esp rlwlij

Key = 12 :
tqxxa iadxp uf'e uzodqpunxq
itmf ue fa nq qjbxadqp rgdftqd uz ftq smxmjk

Key = 13 :
uryyb jbeyq vg'f vaperqvoyr
jung vf gb or rkcyberq shegure va gur tnynkl
```

Key = 14 :
vszzc kcfzr wh'g wbqfsrwpzs
kvoh wg hc ps sldzcfsr tifhvsf wb hvs uozolm

Key = 15 :
wtaad ldgas xi'h xcrgtsxqat
lwpi xh id qt tmeadgts ujgiwtg xc iwt vpapmn

Key = 16 :
xubbe mehbt yj'i ydshutyrbu
mxqj yi je ru unfbehut vkhjxuh yd jxu wqbqno

Key = 17 :
yvccf nficu zk'j zetivuzscv
nyrk zj kf sv vogcfivu wlikyvi ze kyv xrcrop

Key = 18 :
zwddg ogjdv al'k afujwvatdw
ozsl ak lg tw wphdgjwv xmjlzwj af lzw ysdspq

Key = 19 :
axeeh phkew bm'l bgvkxwbuex
patm bl mh ux xqiehkxw ynkmaxk bg max ztetqr

Key = 20 :
byffi qilfx cn'm chwlyxcvfy
qbun cm ni vy yrjfilyx zolnbyl ch nby aufurs

Key = 21 :
czggj rjmgy do'n dixmzydwgz
rcvo dn oj wz zskgjmzy apmoczm di ocz bvgvst

Key = 22 :
dahhk sknhz ep'o ejynazexha
sdwp eo pk xa atlhknaz bqnpdan ej pda cwhwtu

```
Key = 23 :
ebiil tloia fq'p fkzobafyib
texq fp ql yb bumiloba croqebo fk qeb dxixuv

Key = 24 :
fcjjm umpjb gr'q glapcbgzjc
ufyr gq rm zc cvnjmpcb dsprfcp gl rfc eyjyvw

Key = 25 :
gdkkn vnqkc hs'r hmbqdchakd
vgzs hr sn ad dwoknqdc etqsgdq hm sgd fzkzwx


********** Frequency Analysis Method **********
w -> e :
pmttw ewztl qb'a qvkzmlqjtm
epib qa bw jm mfxtwzml nczbpmz qv bpm oitifg

x -> t :
dahhk sknhz ep'o ejynazexha
sdwp eo pk xa atlhknaz bqnpdan ej pda cwhwtu

y -> a :
jgnnq yqtnf kv'u kpetgfkdng
yjcv ku vq dg gzrnqtgf hwtvjgt kp vjg icncza

t -> o :
czggj rjmgy do'n dixmzydwgz
rcvo dn oj wz zskgjmzy apmoczm di ocz bvgvst

u -> i :
vszzc kcfzr wh'g wbqfsrwpzs
kvoh wg hc ps sldzcfsr tifhvsf wb hvs uozolm

r -> n :
dahhk sknhz ep'o ejynazexha
```

sdwp eo pk xa atlhknaz bqnpdan ej pda cwhwtu

s -> s :
hello world it's incredible
what is to be explored further in the galaxy

o -> h :
axeeh phkew bm'l bgvkxwbuex
patm bl mh ux xqiehkxw ynkmaxk bg max ztetqr

p -> r :
jgnnq yqtnf kv'u kpetgfkdng
yjcv ku vq dg gzrnqtgf hwtvjgt kp vjg icncza

n -> d :
xubbe mehbt yj'i ydshutyrbu
mxqj yi je ru unfbehut vkhjxuh yd jxu wqbqno

l -> l :
hello world it's incredible
what is to be explored further in the galaxy

i -> c :
byffi qilfx cn'm chwlyxcvfy
qbun cm ni vy yrjfilyx zolnbyl ch nby aufurs

h -> u :
uryyb jbeyq vg'f vaperqvoyr
jung vf gb or rkcyberq shegure va gur tnynkl

e -> m :
pmttw ewztl qb'a qvkzmlqjtm
epib qa bw jm mfxtwzml nczbpmz qv bpm oitifg

f -> w :
yvccf nficu zk'j zetivuzscv

nyrk zj kf sv vogcfivu wlikyvi ze kyv xrcrop

g -> f :
gdkkn vnqkc hs'r hmbqdchakd
vgzs hr sn ad dwoknqdc etqsgdq hm sgd fzkzwx

d -> g :
khoor zruog lw'v lqfuhgleoh
zkdw lv wr eh hasoruhg ixuwkhu lq wkh jdodab

a -> y :
fcjjm umpjb gr'q glapcbgzjc
ufyr gq rm zc cvnjmpcb dsprfcp gl rfc eyjyvw

b -> p :
vszzc kcfzr wh'g wbqfsrwpzs
kvoh wg hc ps sldzcfsr tifhvsf wb hvs uozolm

c -> b :
gdkkn vnqkc hs'r hmbqdchakd
vgzs hr sn ad dwoknqdc etqsgdq hm sgd fzkzwx

a -> v :
czggj rjmgy do'n dixmzydwgz
rcvo dn oj wz zskgjmzy apmoczm di ocz bvgvst

a -> k :
rovvy gybvn sd'c sxmbonslvo
grkd sc dy lo ohzvybon pebdrob sx dro qkvkhi

a -> j :
qnuux fxaum rc'b rwlanmrkun
fqjc rb cx kn ngyuxanm odacqna rw cqn pjujgh

a -> x :
ebiil tloia fq'p fkzobafyib

```
texq fp ql yb bumiloba croqebo fk qeb dxixuv

a -> q :
xubbe mehbt yj'i ydshutyrbu
mxqj yi je ru unfbehut vkhjxuh yd jxu wqbqno

a -> z :
gdkkn vnqkc hs'r hmbqdchakd
vgzs hr sn ad dwoknqdc etqsgdq hm sgd fzkzwx

jhajharia@Nehals-MacBook-Air Asmt1 %
```