NAME – ASHUTOSH ARDU

REG NO – 20BRS1262

DATE – 17-6-2021

CIPHER CODE
CSE1004 DA – 3

ALGORITHM

- CIPHERS MENTIONED IN THE CODE
    - CAESAR'S CIPHER
    - HILL'S CIPHER
    - MONOALPHA CIPHER
    - POLYALPHABETIC SUBSTITUTION OR VIGENERE'S CIPHER

- CAESAR CIPHER
    - Read each alphabet of plain text.
    - Take the number for replacement.
    - Replace each alphabet with a specified number down.
    - Repeat the process for all alphabet in plain text.

- HILL CIPHER
    - Assign the number to each alphabet in plain text. A = 0, B= 1…. z = 25

- Organize the plain text message as a matrix of numbers based on the above step in number format. The resultant matrix is called a plain text matrix.
- Multiply the plain text matrix with a randomly chosen key. Note that the key matrix must be the size of n*n where n stands for the number of rows in a plain text matrix.
- Multiply both the matrix, i.e., step 2 and step 3.
- Calculate the mod 26 value of the above matrix, i.e. matrix results in step 4.
- Now translate the numbers to alphabets i.e., 0 =A, 1 =B, etc.
- The result of step 6 becomes our ciphertext.

- MONOALPHA CIPHER
  - As Caesar cipher and a modified version of Caesar cipher is easy to break, monoalphabetic cipher comes into the picture.
  - In monoalphabetic, each alphabet in plain text can be replaced by any other alphabet except the original alphabet.
  - That is, A can be replaced by any other alphabet from B to Z. B can be replaced by A or C to Z. C can be replaced by A, B, and D to z, etc.

- Mono alphabetic cipher causes difficulty to crack the message as there are random substitutions rather than a key number and a large number of permutation and combination are available.

- VIGENERE'S CIPHER

A polyalphabetic or Vigenere cipher is any cipher based on substitution, using multiple substitution alphabets .The encryption of the original text is done using the Vigenère square or Vigenère table.

- The table consists of the alphabets written out 26 times in different rows, each alphabet shifted cyclically to the left compared to the previous alphabet, corresponding to the 26 possible Caesar Ciphers.

- At different points in the encryption process, the cipher uses a different alphabet from one of the rows.

- The alphabet used at each point depends on a repeating keyword.

THE CODE

```
#include <bits/stdc++.h>
using namespace std;
float encrypt[3][1], decrypt[3][1], a[3][3], b[3][3],
mes[3][1], c[3][3];
// Above piece of variables are for the Hill cipher
unordered_map<char,char> hashMap;// for the Monoalpha
cipher
void inverse(); //finds inverse of key matrix
string caesar_encrypt(string message,int key){
char ch;
int i;
for(i = 0; message[i] != '\0'; ++i){
ch = message[i];
if(ch >= 'a' && ch <= 'z'){
ch = ch + key;
if(ch > 'z'){
ch = ch - 'z' + 'a' - 1;
}
message[i] = ch;
}
else if(ch >= 'A' && ch <= 'Z'){
ch = ch + key;
if(ch > 'Z'){
ch = ch - 'Z' + 'A' - 1;
}
message[i] = ch;
}
}
cout << "Encrypted message: " << message<<endl;
return message;
}
void caesar_decrypt(string message,int key){
char ch;
int i;
for(i = 0; message[i] != '\0'; ++i){
ch = message[i];
```

```
if(ch >= 'a' && ch <= 'z'){
ch = ch - key;
if(ch < 'a'){
ch = ch + 'z' - 'a' + 1;
}
message[i] = ch;
}
else if(ch >= 'A' && ch <= 'Z'){
ch = ch - key;
if(ch > 'a'){
ch = ch + 'Z' - 'A' + 1;
}
message[i] = ch;
}
}
cout << "Decrypted message: " << message;
}

void hill_encryption() {
int i, j, k;
for(i = 0; i < 3; i++)
for(j = 0; j < 1; j++)
for(k = 0; k < 3; k++)
encrypt[i][j] = encrypt[i][j] + a[i][k] * mes[k][j];
cout<<"\nEncrypted string is: ";
for(i = 0; i < 3; i++)
cout<<(char)(fmod(encrypt[i][0], 26) + 97);
}

void hill_decryption() {
int i, j, k;
inverse();
for(i = 0; i < 3; i++)
for(j = 0; j < 1; j++)
for(k = 0; k < 3; k++)
decrypt[i][j] = decrypt[i][j] + b[i][k] * encrypt[k][j]
;
cout<<"\nDecrypted string is: ";
for(i = 0; i < 3; i++)
cout<<(char)(fmod(decrypt[i][0], 26) + 97);
cout<<"\n";
}
```

```
void hill_getKeyMessage() {
int i, j;
char msg[3];

cout<<"Enter 3x3 matrix for key (It should be inversib
le):\n";
for(i = 0; i < 3; i++)
for(j = 0; j < 3; j++) {
cin>>a[i][j];
c[i][j] = a[i][j];
}
cout<<"\nEnter a 3 letter string: ";
cin>>msg;
for(i = 0; i < 3; i++)
mes[i][0] = msg[i] - 97;
}

void inverse() {
int i, j, k;
float p, q;
for(i = 0; i < 3; i++)
for(j = 0; j < 3; j++) {
if(i == j)
b[i][j]=1;
else
b[i][j]=0;
}
for(k = 0; k < 3; k++) {
for(i = 0; i < 3; i++) {
p = c[i][k];
q = c[k][k];
for(j = 0; j < 3; j++) {
if(i != k) {
c[i][j] = c[i][j]*q - p*c[k][j];
b[i][j] = b[i][j]*q - p*b[k][j];
}
}
}
}
for(i = 0; i < 3; i++)
for(j = 0; j < 3; j++)
```

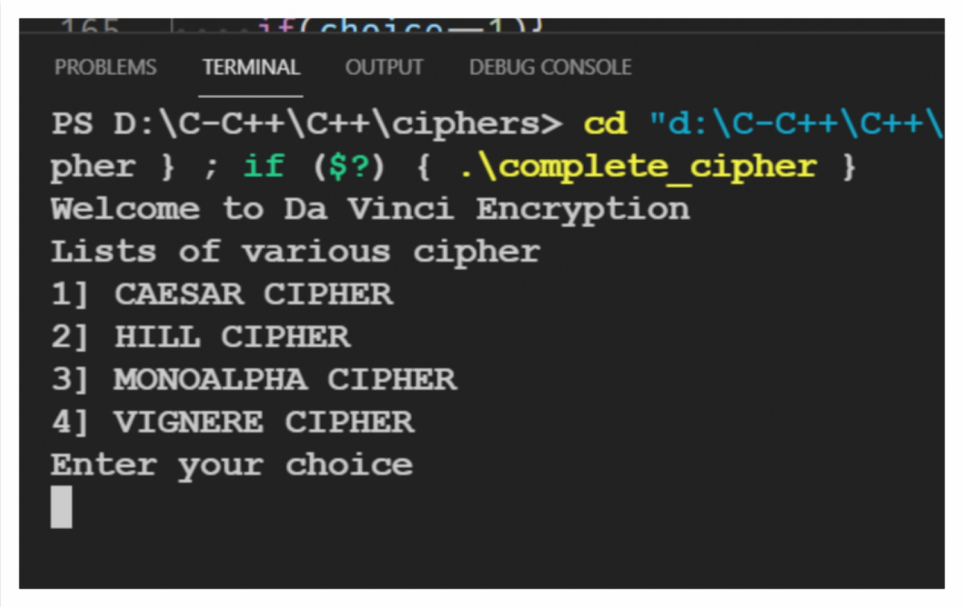
```
b[i][j] = b[i][j] / c[i][i];
cout<<"\n\nInverse Matrix is:\n";
for(i = 0; i < 3; i++) {
for(j = 0; j < 3; j++)
cout<<b[i][j]<<" ";
cout<<"\n";
}cout<<"Used for decryption\n";
}

string monoalpha_encrypt(string msg)
{
  string ciphertext;
  for(int i=0; i<msg.size(); i++)
  {
    ciphertext.push_back(hashMap[msg[i]]);
  }

  return ciphertext;
}

string monoalpha_decrypt(string msg)
{
  string plaintext;
  for(int i=0; i<msg.size(); i++)
  {
    plaintext.push_back(hashMap[msg[i]]);
  }

  return plaintext;
}

void hashFn(string a, string b)
{
  hashMap.clear();
  for(int i=0; i<a.size(); i++)
  {
    hashMap.insert(make_pair(a[i],b[i]));
  }
}

int main(){
    int choice;
```

```
    label:
    cout<<"Welcome to Da Vinci Encryption\n";
    cout<<"Lists of various cipher\n1] CAESAR CIPHER\n
2] HILL CIPHER\n3] MONOALPHA CIPHER\n4] VIGNERE CIPHER
\n";
    cout<<"Enter your choice\n";
    cin>>choice;
    cin.ignore();
    if(choice==1){
        cout<<"You have chosen CAESAR CIPHER\n";
        string message,en;
        int key;
        cout<<"Enter a message to encrypt: ";
        getline(cin,message);
        cout<<"Enter key: ";
        cin>>key;
        en=caesar_encrypt(message,key);
        caesar_decrypt(en,key);
    }
    else if(choice==2){
        cout<<"You have chosen HILL CIPHER\n";
        hill_getKeyMessage();
        hill_encryption();
        hill_decryption();
    }
    else if(choice==3){
        cout<<"You have chosen MONOALPHA CIPHER\n";
        string alphabet = "abcdefghijklmnopqrstuvwxyz";
        string substitution = "qwertyuiopasdfghjklzxcv
bnm";
        string msg = "hello";
        cout<<"The message "<<msg<<endl;
        hashFn(alphabet, substitution);
        string cipher =monoalpha_encrypt(msg);
        cout<<"Encrypted Cipher Text: "<<cipher<<endl;
        hashFn(substitution, alphabet);
        string plain =monoalpha_decrypt(cipher);
        cout<<"Decrypted Plain Text: "<<plain<<endl;
    }
    else if(choice==4){
        cout<<"You have chosen VIGNERE CIPHER\n";
        string msg,key;
```

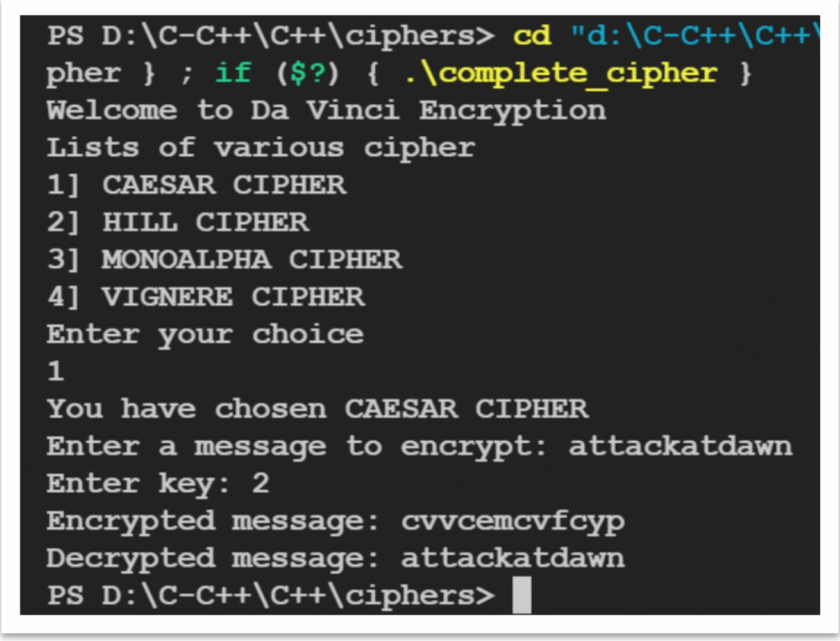
```
        cin>>msg>>key;
        int msgLen = msg.length(), keyLen = key.length
(), i, j;
        char newKey[msgLen], encryptedMsg[msgLen], dec
ryptedMsg[msgLen];
        //generating new key
        for(i = 0, j = 0; i < msgLen; ++i, ++j){
            if(j == keyLen)
                j = 0;
            newKey[i] = key[j];
        }newKey[i] = '\0';
        //encryption
        for(i = 0; i < msgLen; ++i)
            encryptedMsg[i] = ((msg[i] + newKey[i]) %
26) + 'A';
        encryptedMsg[i] = '\0';
        //decryption
        for(i = 0; i < msgLen; ++i)
            decryptedMsg[i] = (((encryptedMsg[i] -
 newKey[i]) + 26) % 26) + 'A';
        decryptedMsg[i] = '\0';
        cout<<"Original Message: "<<msg;
        cout<<"\nKey: "<<key;
        cout<<"\nNew Generated Key: "<<newKey;
        cout<<"\nEncrypted Message: "<<encryptedMsg;
        cout<<"\nDecrypted Message: "<<decryptedMsg;
        }
    else{
        cout<<"Incorrect choice\n";
        cout<<"Enter the \"0\" to quit the cipher mani
a\n";
        if(choice!=0) goto label;
    }
}
```

OUTPUTS

THE MAIN WINDOW



CAESAR CIPHER



HILL CIPHER

```
PS D:\C-C++\C++\ciphers> cd "d:\C-C++\C++\ciphers\" ; i
pher } ; if ($?) { .\complete_cipher }
Welcome to Da Vinci Encryption
Lists of various cipher
1] CAESAR CIPHER
2] HILL CIPHER
3] MONOALPHA CIPHER
4] VIGNERE CIPHER
Enter your choice
2
You have chosen HILL CIPHER
Enter 3x3 matrix for key (It should be inversible):
6 24 1
13 16 10
20 17 15

Enter a 3 letter string: act

Encrypted string is: poh

Inverse Matrix is:
0.15873 -0.777778 0.507937
0.0113379 0.15873 -0.106576
-0.22449 0.857143 -0.489796
Used for decryption

Decrypted string is: act
PS D:\C-C++\C++\ciphers>
```

MONOALPHA CIPHER

```
Welcome to Da Vinci Encryption
Lists of various cipher
1] CAESAR CIPHER
2] HILL CIPHER
3] MONOALPHA CIPHER
4] VIGNERE CIPHER
Enter your choice
3
You have chosen MONOALPHA CIPHER
The message hello
Encrypted Cipher Text: itssg
Decrypted Plain Text: hello
PS D:\C-C++\C++\ciphers>
```

VIGNERE CIPHER