/\*

Anudish Jinturkar

H-27

Subject: Network Security (Lab)

Lab4: Implementation of Hill Cipher for 2\*2 matrix input

\*/

#include <bits/stdc++.h>

using namespace std;

#define gc getchar\_unlocked

int key\_mat[2][2];

int key\_inv\_mat[2][2];

int text\_mat[2];

int text\_inv\_mat[2];

int res\_mat[2];

int res\_inv\_mat[2];

int main()

{

string key,str,encrypt="",decrypt="";

int d,k=0,flag=0;

cout<<"Enter the key(four characters):"<<endl;

cin>>key;

cout<<"\n"<<"Enter the string"<<endl;

cin>>str;

for(int i=0;i<2;++i)

for(int j=0;j<2;++j)

key\_mat[i][j]=(key[k++]-'A');

cout<<"Key Matrix is:"<<endl;

for(int i=0;i<2;++i)

{

for(int j=0;j<2;++j)

cout<<key\_mat[i][j]<<" ";

cout<<"\n";

}

if(str.length()%2)

{

flag=1;

str[str.length()]='X';

}

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

{

text\_mat[0]=str[i++]-'A';

text\_mat[1]=str[i]-'A';

res\_mat[0]=(text\_mat[0]\*key\_mat[0][0]+text\_mat[1]\*key\_mat[1][0])%26;

res\_mat[1]=(text\_mat[0]\*key\_mat[0][1]+text\_mat[1]\*key\_mat[1][1])%26;

encrypt+=char(res\_mat[0]+'A');

encrypt+=char(res\_mat[1]+'A');

}

cout<<"\nEncrypted String is: "<<encrypt<<"\n";

d=key\_mat[0][0]\*key\_mat[1][1]-key\_mat[0][1]\*key\_mat[1][0];

cout<<"Determinant of the Key Matrix is: "<<d<<"\n";

key\_inv\_mat[0][0]=key\_mat[1][1]/d;

key\_inv\_mat[0][1]=key\_mat[0][1]/(-d);

key\_inv\_mat[1][0]=key\_mat[1][0]/(-d);

key\_inv\_mat[1][1]=key\_mat[0][0]/d;

cout<<"Inverse of the Key matrix is: "<<endl;

for (int i = 0; i < 2; i++)

{

for (int j = 0;j < 2; j++)

cout<<key\_inv\_mat[i][j]<<" ";

cout<<"\n";

}

cout<<"\n";

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

{

text\_inv\_mat[0]=encrypt[i++]-'A';

text\_inv\_mat[1]=encrypt[i]-'A';

res\_inv\_mat[0]=(text\_inv\_mat[0]\*key\_inv\_mat[0][0]+text\_inv\_mat[1]\*key\_inv\_mat[1][0])%26;

res\_inv\_mat[1]=(text\_inv\_mat[0]\*key\_inv\_mat[0][1]+text\_inv\_mat[1]\*key\_inv\_mat[1][1])%26;

if(res\_inv\_mat[0]<0)

res\_inv\_mat[0]+=26;

if(res\_inv\_mat[1]<0)

res\_inv\_mat[1]+=26;

decrypt+=char(res\_inv\_mat[0]+'A');

decrypt+=char(res\_inv\_mat[1]+'A');

}

if(flag==1)

decrypt[decrypt.length()-1]='\0';

cout<<"\nDecrypted String is: "<<decrypt<<"\n";

return 0;

}

/\*

Output:

Enter the key(four characters):

HFED

Enter the string

ANUDISH

Key Matrix is:

7 5

4 3

Encrypted String is: ANWFYQLA

Determinant of the Key Matrix is: 1

Inverse of the Key matrix is:

3 -5

-4 7

Decrypted String is: ANUDISH

\*/