/\*

Anudish Jinturkar

H-27

Subject: Network Security (Lab)

Lab8: Implementation of RSA Algorithm

\*/

#include <bits/stdc++.h>

#include <cmath>

#define gc getchar\_unlocked

using namespace std;

int main()

{

int plain\_text,i,j,p,q,flag,e,x,d,n,fn,abc,encryption,decryption;

cout<<"\nEnter Plain Text ( in numerical form ) : ";

cin>>plain\_text;

cout<<"\n"<<"Enter Value of p : ";

cin>>p;

cout<<endl<<"Enter Value of q : ";

cin>>q;

n = p \* q;

fn = (p-1)\*(q-1);

cout<<endl<<"Value of (p,q) : "<<p<<" "<<q<<endl;

cout<<"Value of n : "<<n<<endl;

cout<<"Value of fn : "<<fn<<endl;

cout<<"Select Key e (1 < e < "<<fn<<") : ";

cin>>e;

cout<<"\nPublic Key (e,n) : ( "<<e<<" , "<<n<<" )"<<endl;

for(i=1;i>0;i++)

{

x = i \* e ;

d = x % fn ;

if(d==1)

{

cout<<"\nPrivate Key (d,p,q) : ( "<<i<<" , "<<p<<" , "<<q<<" )"<<endl;

abc = i ;

break;

}

}

cout<<"Value of d : "<<abc;

encryption = 1 ;

for(i=0;i<e;i++)

encryption=(encryption\*plain\_text)%n;

encryption = encryption % n ;

cout<<"\nEncrypted Text : "<<encryption;

decryption = 1 ;

for(i=0;i<abc;i++)

decryption=(decryption\*encryption)%n;

decryption = decryption % n;

cout<<"\nDecrypted Text : "<<decryption;

return 0;

}

/\*

Output:

Enter Plain Text ( in numerical form ) : 88

Enter Value of p : 17

Enter Value of q : 11

Value of (p,q) : 17 11

Value of n : 187

Value of fn : 160

Select Key e (1 < e < 160) : 7

Public Key (e,n) : ( 7 , 187 )

Private Key (d,p,q) : ( 23 , 17 , 11 )

Value of d : 23

Encrypted Text : 11

Decrypted Text : 88

\*/