package com.mycompany.discreteproject1;

import static java.lang.Math.pow;

import java.util.Scanner;

import java.math.BigInteger;

public class RSA {

public static void main(String[] args) {

int flag=0;

int p=2;

int q=2;

Scanner s=new Scanner(System.in);

System.out.println("Enter TWO distinct upper limits for the two primes p , q: ");

System.out.print("Upper limit for p:");

int maxp=s.nextInt();

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

{

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

{

if(i%k==0)

{

flag=1;

break;

}

}

if(flag==0)

{

if(i>p)

{

p=i;

}

}

flag=0;

}

System.out.print("Upper limit for q:");

int maxq=s.nextInt();

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

{

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

{

if(i%k==0)

{

flag=1;

break;

}

}

if(flag==0)

{

if(i>q)

{

q=i;

}

}

flag=0;

}

System.out.println("p= "+p); //secret key

System.out.println("q= "+q); //secret key

int n=p\*q; //public key

System.out.println("n= "+n);

int m=(p-1)\*(q-1); //secret key

System.out.println("m= "+m);

int e;

for(e=1;e<=m;e++)

{

if(m%e!=0)

{

System.out.println("e= "+e); //public key

break;

}

}

int de;

int d = 0;

for(int k=0;k>=0;k++)

{

de=(m\*k)+1;

if(de%e==0)

{

d=((m\*k)+1)/e;

System.out.println("d= "+d);

break;

}

}

System.out.print("Enter original Message:");

s.nextLine();

String h=s.nextLine();

BigInteger a,b,t,g,enc;

a=BigInteger.valueOf(n);

b=BigInteger.valueOf(e);

t=BigInteger.valueOf(d);

String decrypt[]=new String[h.length()];

System.out.print("Encrypted Message: ");

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

char o=h.charAt(i);

int ascinum=(int)o;

String asc=String.valueOf(ascinum);

g=new BigInteger(asc);

enc=g.modPow(b, a);

decrypt[i]=enc.toString();

System.out.print(new String(enc.toByteArray()));

}

System.out.print("\nDecrypted Message: ");

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

String dy=decrypt[i];

g=new BigInteger(dy);

enc=g.modPow(t, a);

System.out.print(new String(enc.toByteArray()));

}

}

}