Cryptography

Lab assignment Mid Semester

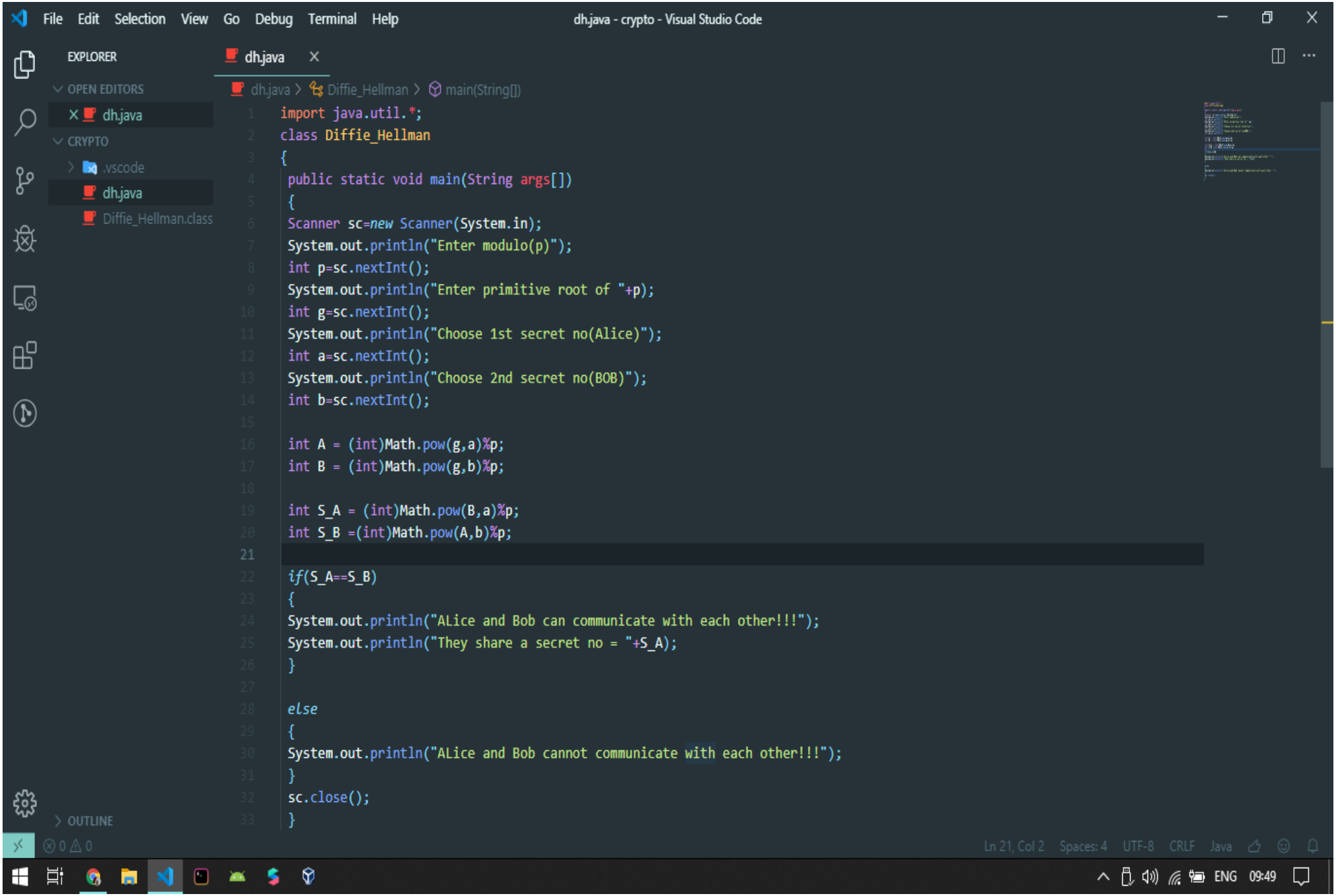
Harsh Gupta

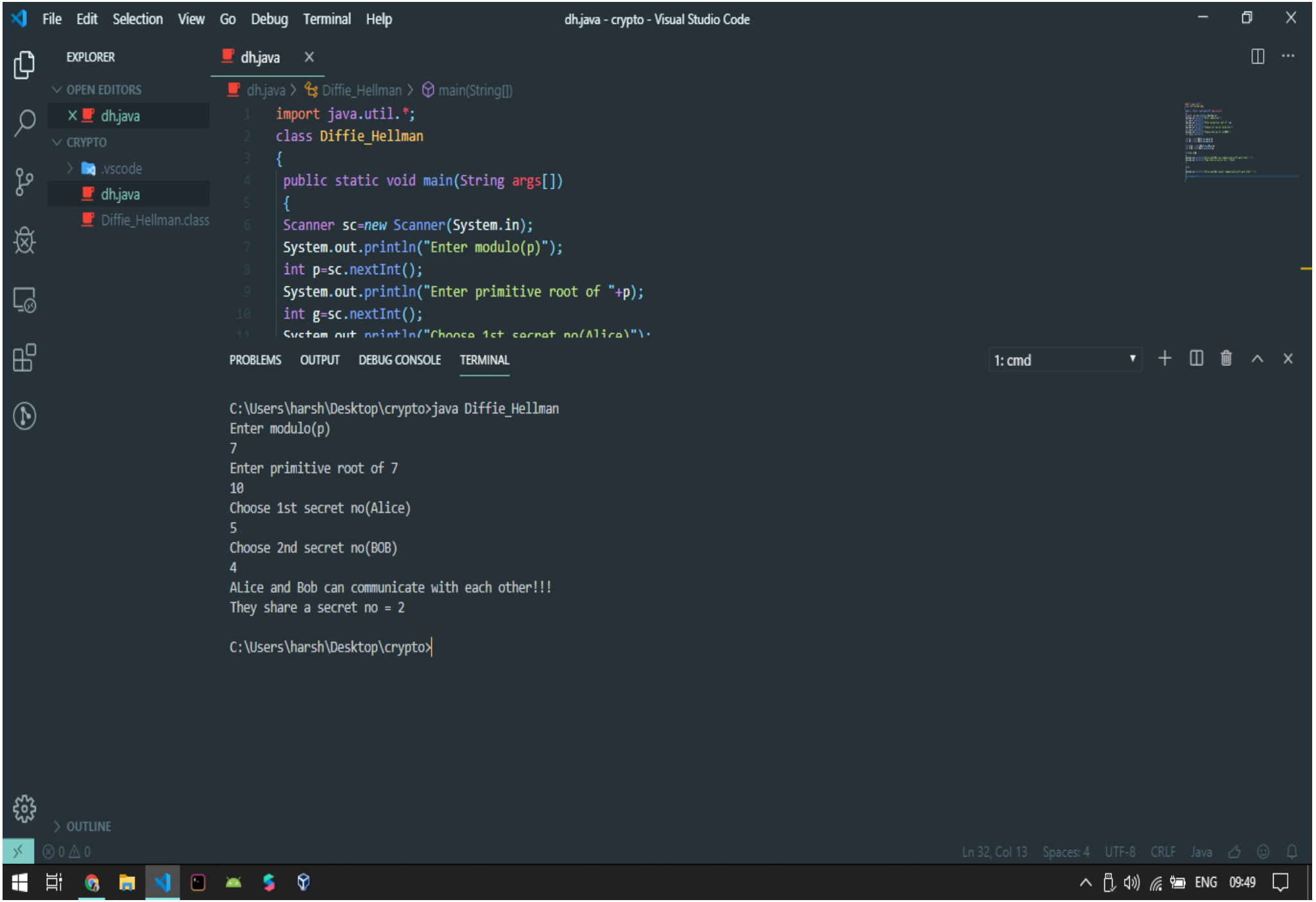
CSE-ccvt 2020

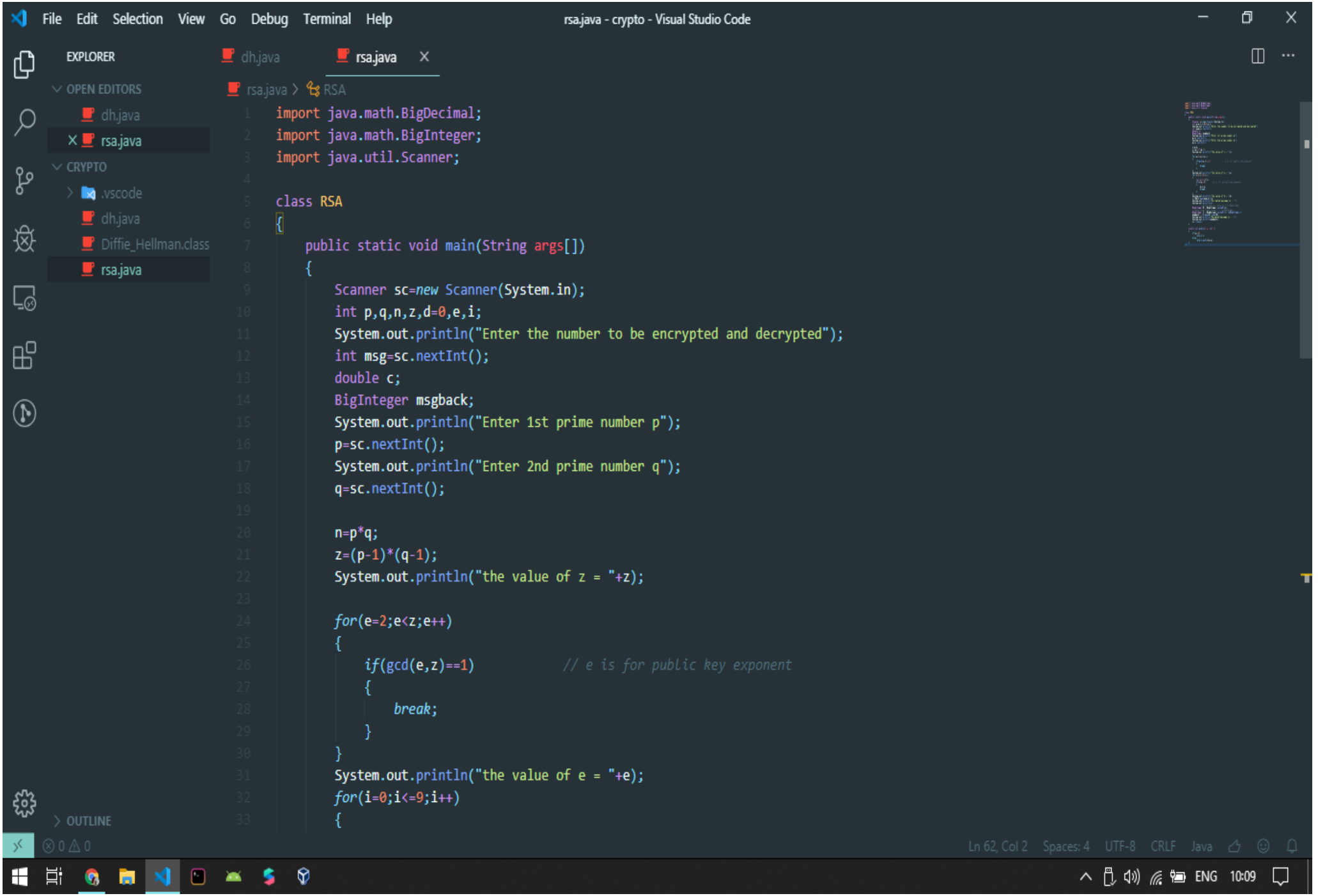
500053088

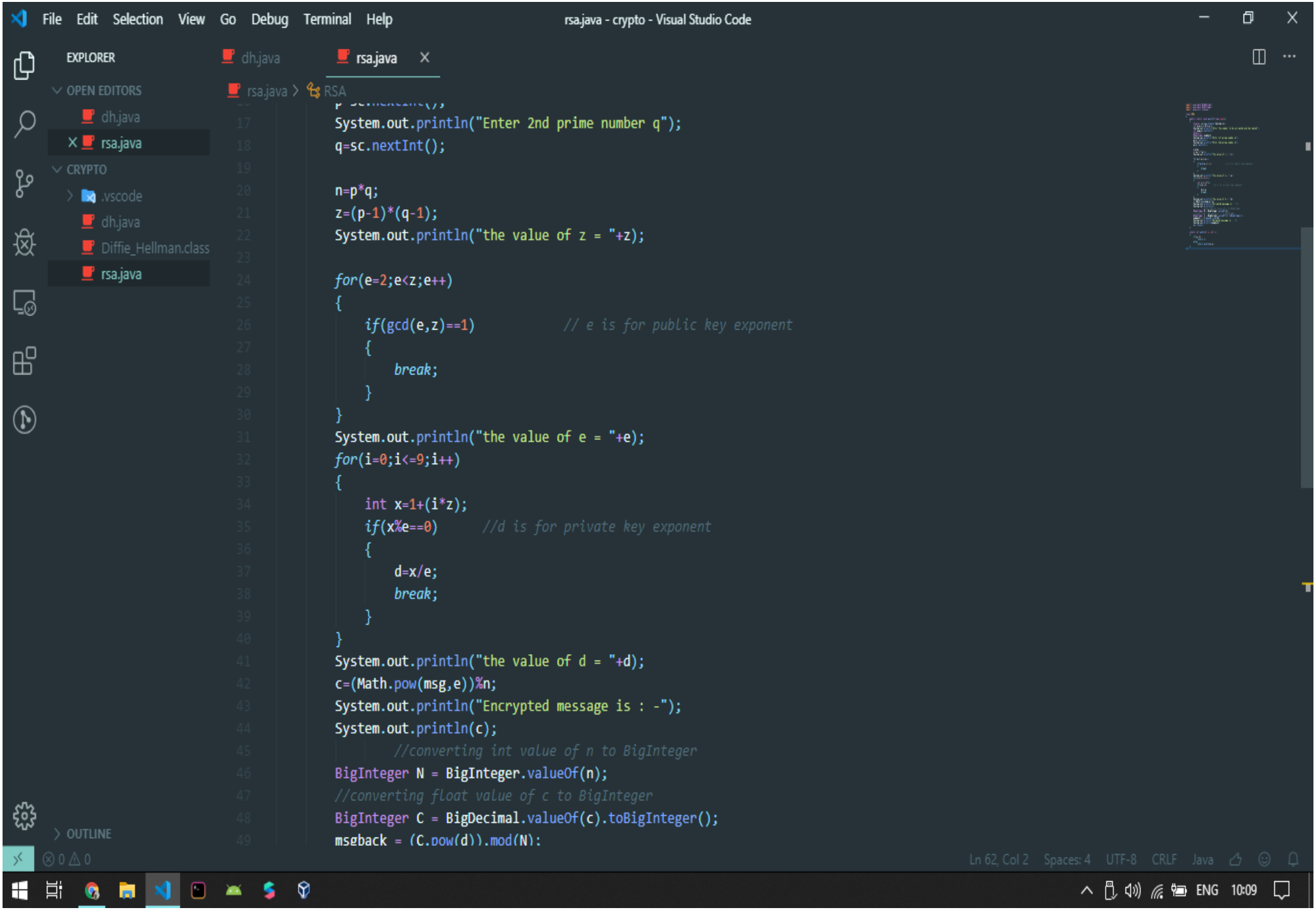
Batch b2

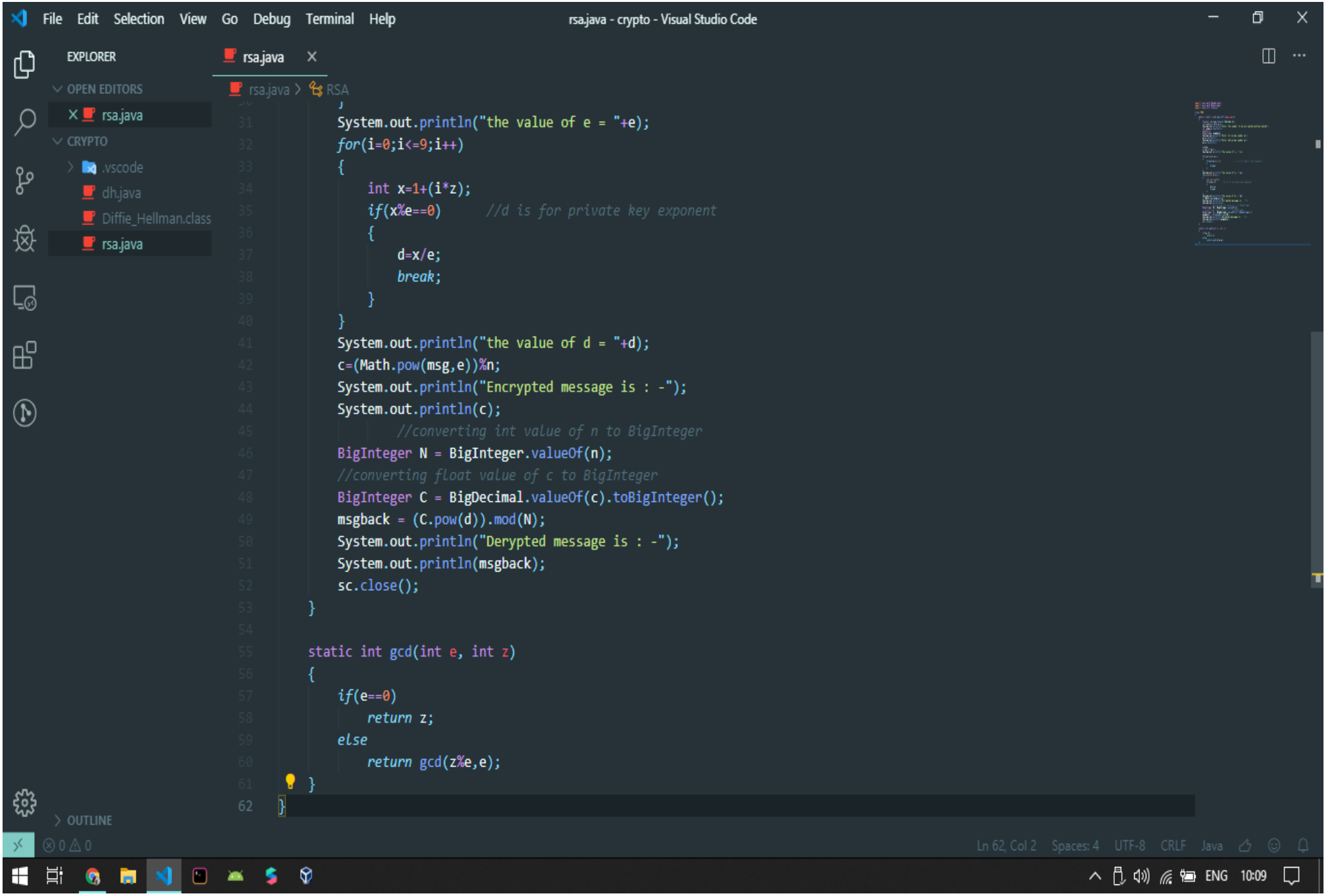
R110216070

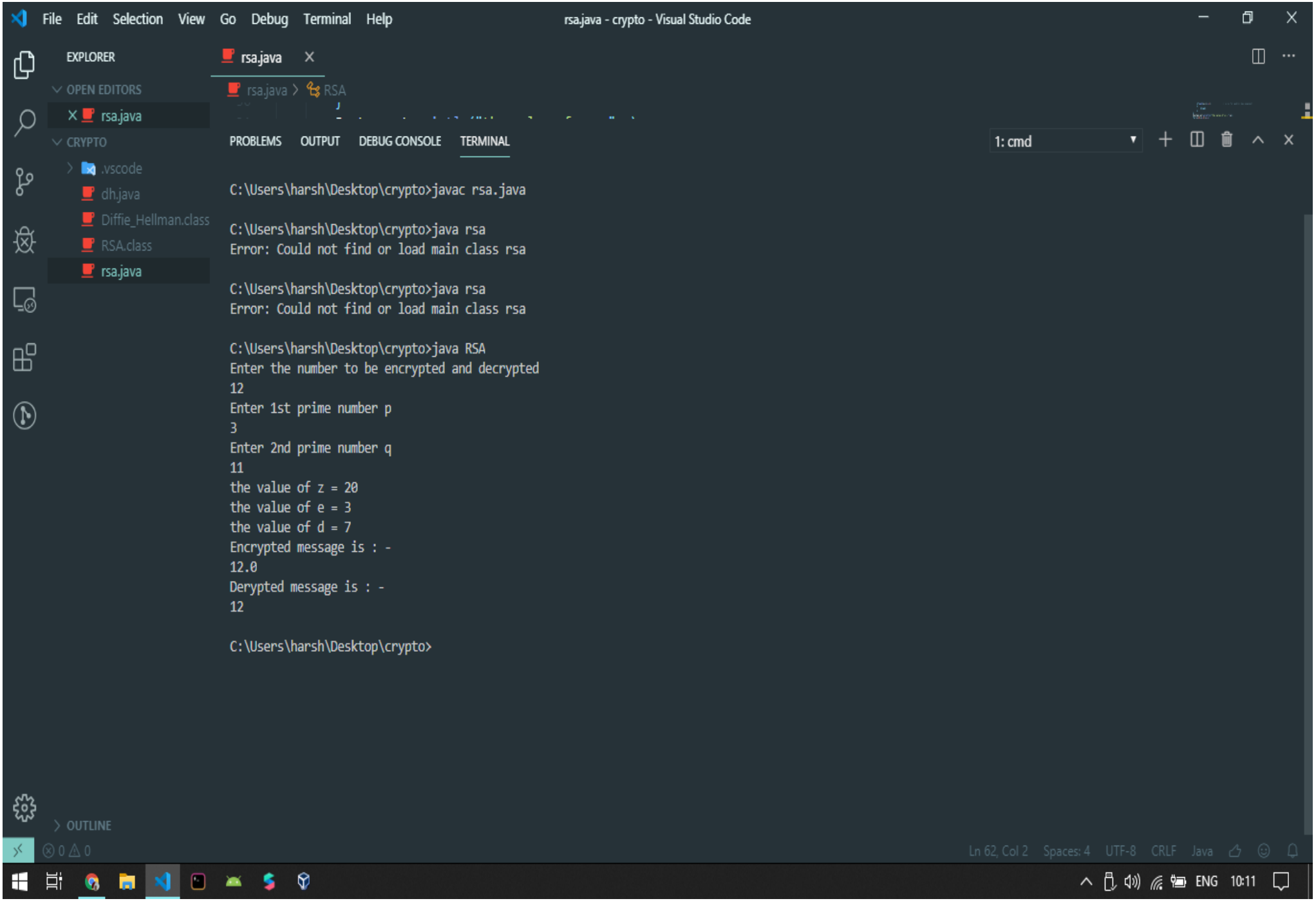

File Edit Selection View Go Debug Terminal Help
dh.java - crypto - Visual Studio Code
EXPLORER
OPEN EDITORS
dh.java
CRYPTO
.vscode
dh.java
Diffie_Hellman.class
OUTLINE
dh.java
dh.java > Diffie_Hellman > main(String[])
import java.util.*;
class Diffie_Hellman
{
public static void main(String args[])
{
Scanner sc=new Scanner(System.in);
System.out.println("Enter modulo(p)");
int p=sc.nextInt();
System.out.println("Enter primitive root of "+p);
int g=sc.nextInt();
System.out.println("Choose 1st secret no(Alice)");
int a=sc.nextInt();
System.out.println("Choose 2nd secret no(BOB)");
int b=sc.nextInt();
int A = (int)Math.pow(g,a)%p;
int B = (int)Math.pow(g,b)%p;
int S_A = (int)Math.pow(B,a)%p;
int S_B =(int)Math.pow(A,b)%p;
if(S_A==S_B)
{
System.out.println("ALice and Bob can communicate with each other!!!");
System.out.println("They share a secret no = "+S_A);
}
else
{
System.out.println("ALice and Bob cannot communicate with each other!!!");
}
sc.close();
}
Ln 21, Col 2 Spaces: 4 UTF-8 CRLF Java
ENG 09:49


File Edit Selection View Go Debug Terminal Help
dh.java - crypto - Visual Studio Code
EXPLORER
OPEN EDITORS
dh.java
CRYPTO
.vscode
dh.java
Diffie_Hellman.class
dh.java
dh.java > Diffie_Hellman > main(String[])
import java.util.*;
class Diffie_Hellman
{
public static void main(String args[])
{
Scanner sc=new Scanner(System.in);
System.out.println("Enter modulo(p)");
int p=sc.nextInt();
System.out.println("Enter primitive root of "+p);
int g=sc.nextInt();
PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL
1: cmd
C:\Users\harsh\Desktop\crypto>java Diffie_Hellman
Enter modulo(p)
7
Enter primitive root of 7
10
Choose 1st secret no(Alice)
5
Choose 2nd secret no(BOB)
4
ALice and Bob can communicate with each other!!!
They share a secret no = 2
C:\Users\harsh\Desktop\crypto>
OUTLINE
Ln 32, Col 13 Spaces: 4 UTF-8 CRLF Java
ENG 09:49


File Edit Selection View Go Debug Terminal Help
rsa.java - crypto - Visual Studio Code
EXPLORER
OPEN EDITORS
dh.java
rsa.java
CRYPTO
.vscode
dh.java
Diffie_Hellman.class
rsa.java
OUTLINE
dh.java
rsa.java
rsa.java > RSA
import java.math.BigDecimal;
import java.math.BigInteger;
import java.util.Scanner;
class RSA
{
public static void main(String args[])
{
Scanner sc=new Scanner(System.in);
int p,q,n,z,d=0,e,i;
System.out.println("Enter the number to be encrypted and decrypted");
int msg=sc.nextInt();
double c;
BigInteger msgback;
System.out.println("Enter 1st prime number p");
p=sc.nextInt();
System.out.println("Enter 2nd prime number q");
q=sc.nextInt();
n=p*q;
z=(p-1)*(q-1);
System.out.println("the value of z = "+z);
for(e=2;e<z;e++)
{
if(gcd(e,z)==1) // e is for public key exponent
{
break;
}
}
System.out.println("the value of e = "+e);
for(i=0;i<=9;i++)
{
Ln 62, Col 2 Spaces: 4 UTF-8 CRLF Java
ENG 10:09


File Edit Selection View Go Debug Terminal Help
rsa.java - crypto - Visual Studio Code
EXPLORER
OPEN EDITORS
dh.java
rsa.java
CRYPTO
.vscode
dh.java
Diffie_Hellman.class
rsa.java
OUTLINE
dh.java
rsa.java
rsa.java > RSA
System.out.println("Enter 2nd prime number q");
q=sc.nextInt();
n=p*q;
z=(p-1)*(q-1);
System.out.println("the value of z = "+z);
for(e=2;e<z;e++)
{
if(gcd(e,z)==1) // e is for public key exponent
{
break;
}
}
System.out.println("the value of e = "+e);
for(i=0;i<=9;i++)
{
int x=1+(i*z);
if(x%e==0) //d is for private key exponent
{
d=x/e;
break;
}
}
System.out.println("the value of d = "+d);
c=(Math.pow(msg,e))%n;
System.out.println("Encrypted message is : -");
System.out.println(c);
//converting int value of n to BigInteger
BigInteger N = BigInteger.valueOf(n);
//converting float value of c to BigInteger
BigInteger C = BigDecimal.valueOf(c).toBigInteger();
msgback = (C.pow(d)).mod(N);
Ln 62, Col 2 Spaces: 4 UTF-8 CRLF Java
ENG 10:09


File Edit Selection View Go Debug Terminal Help
rsa.java - crypto - Visual Studio Code
EXPLORER
OPEN EDITORS
rsa.java
CRYPTO
.vscode
dh.java
Diffie_Hellman.class
rsa.java
OUTLINE
rsa.java
rsa.java > RSA
System.out.println("the value of e = "+e);
for(i=0;i<=9;i++)
{
int x=1+(i*z);
if(x%e==0) //d is for private key exponent
{
d=x/e;
break;
}
}
System.out.println("the value of d = "+d);
c=(Math.pow(msg,e))%n;
System.out.println("Encrypted message is : -");
System.out.println(c);
//converting int value of n to BigInteger
BigInteger N = BigInteger.valueOf(n);
//converting float value of c to BigInteger
BigInteger C = BigDecimal.valueOf(c).toBigInteger();
msgback = (C.pow(d)).mod(N);
System.out.println("Derypted message is : -");
System.out.println(msgback);
sc.close();
}
static int gcd(int e, int z)
{
if(e==0)
return z;
else
return gcd(z%e,e);
}
}
Ln 62, Col 2 Spaces: 4 UTF-8 CRLF Java
ENG 10:09


File Edit Selection View Go Debug Terminal Help
rsa.java - crypto - Visual Studio Code
EXPLORER
rsa.java
OPEN EDITORS
rsa.java
CRYPTO
.vscode
dh.java
Diffie_Hellman.class
RSA.class
rsa.java
rsa.java > RSA
PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL
1: cmd
C:\Users\harsh\Desktop\crypto>javac rsa.java
C:\Users\harsh\Desktop\crypto>java rsa
Error: Could not find or load main class rsa
C:\Users\harsh\Desktop\crypto>java rsa
Error: Could not find or load main class rsa
C:\Users\harsh\Desktop\crypto>java RSA
Enter the number to be encrypted and decrypted
12
Enter 1st prime number p
3
Enter 2nd prime number q
11
the value of z = 20
the value of e = 3
the value of d = 7
Encrypted message is : -
12.0
Derypted message is : -
12
C:\Users\harsh\Desktop\crypto>
OUTLINE
Ln 62, Col 2 Spaces: 4 UTF-8 CRLF Java
ENG 10:11