Ridhwaan Ali

Mod 4 Assignment Number Theory and Public-Key Encryption

Problem 1:

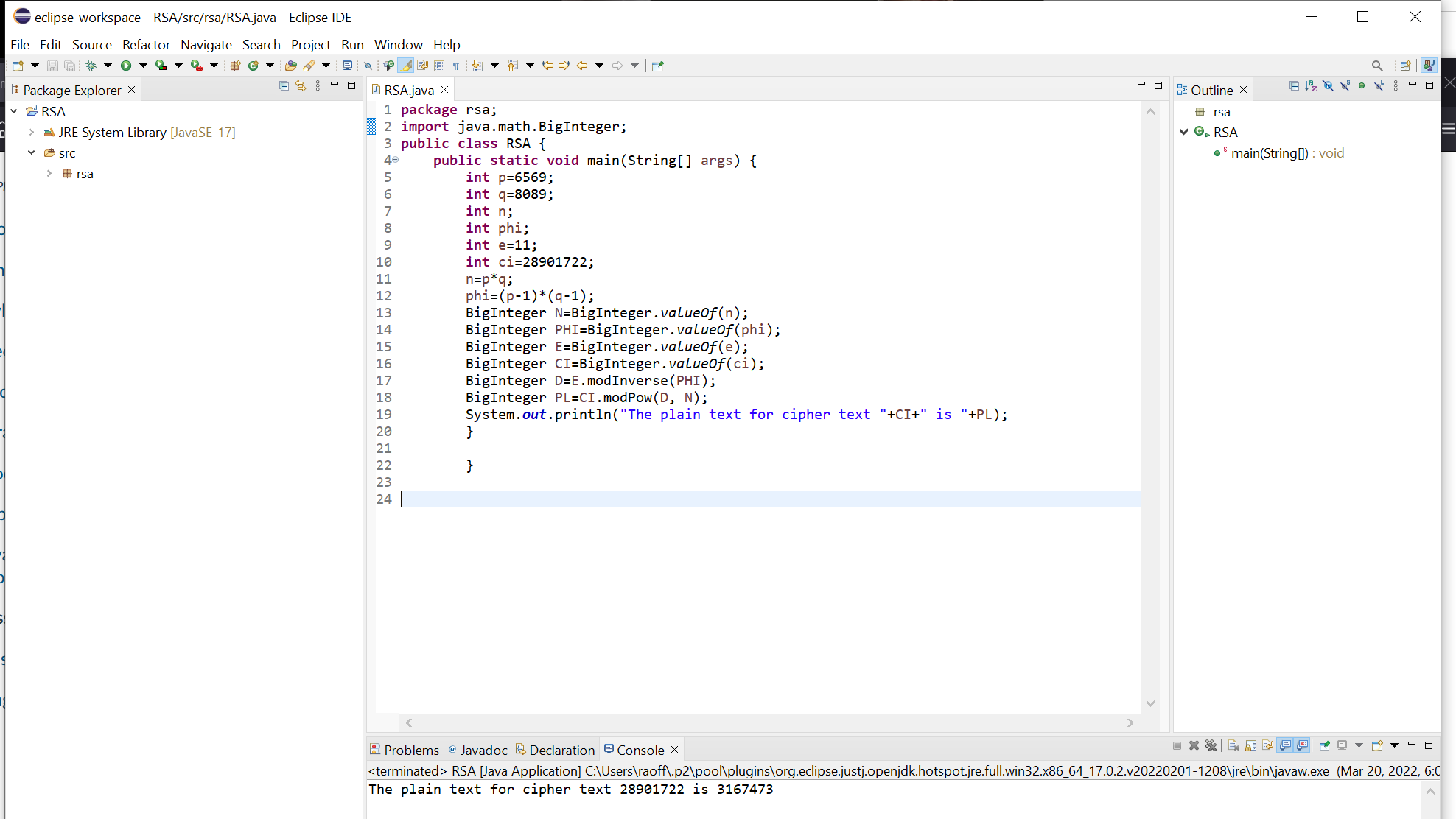
Z11\* = {1,2,3,4,5,6,7,8,9,10}

{1….10} are prime to 11

3 generator of Z11\*: (3^0= 1), (3^1=3), (3^2=9),(3^3=27(mod11)=5),(3^4(mod11)=10)

3 is not generating elements from Z11\* so it is not a generator.

Problem 2:



**package** rsa;

**import** java.math.BigInteger;

**public** **class** RSA {

**public** **static** **void** main(String[] args) {

**int** p=6569;

**int** q=8089;

**int** n;

**int** phi;

**int** e=11;

**int** ci=28901722;

n=p\*q;

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

BigInteger N=BigInteger.*valueOf*(n);

BigInteger PHI=BigInteger.*valueOf*(phi);

BigInteger E=BigInteger.*valueOf*(e);

BigInteger CI=BigInteger.*valueOf*(ci);

BigInteger D=E.modInverse(PHI);

BigInteger PL=CI.modPow(D, N);

System.***out***.println("The plain text for cipher text "+CI+" is "+PL);

}

}