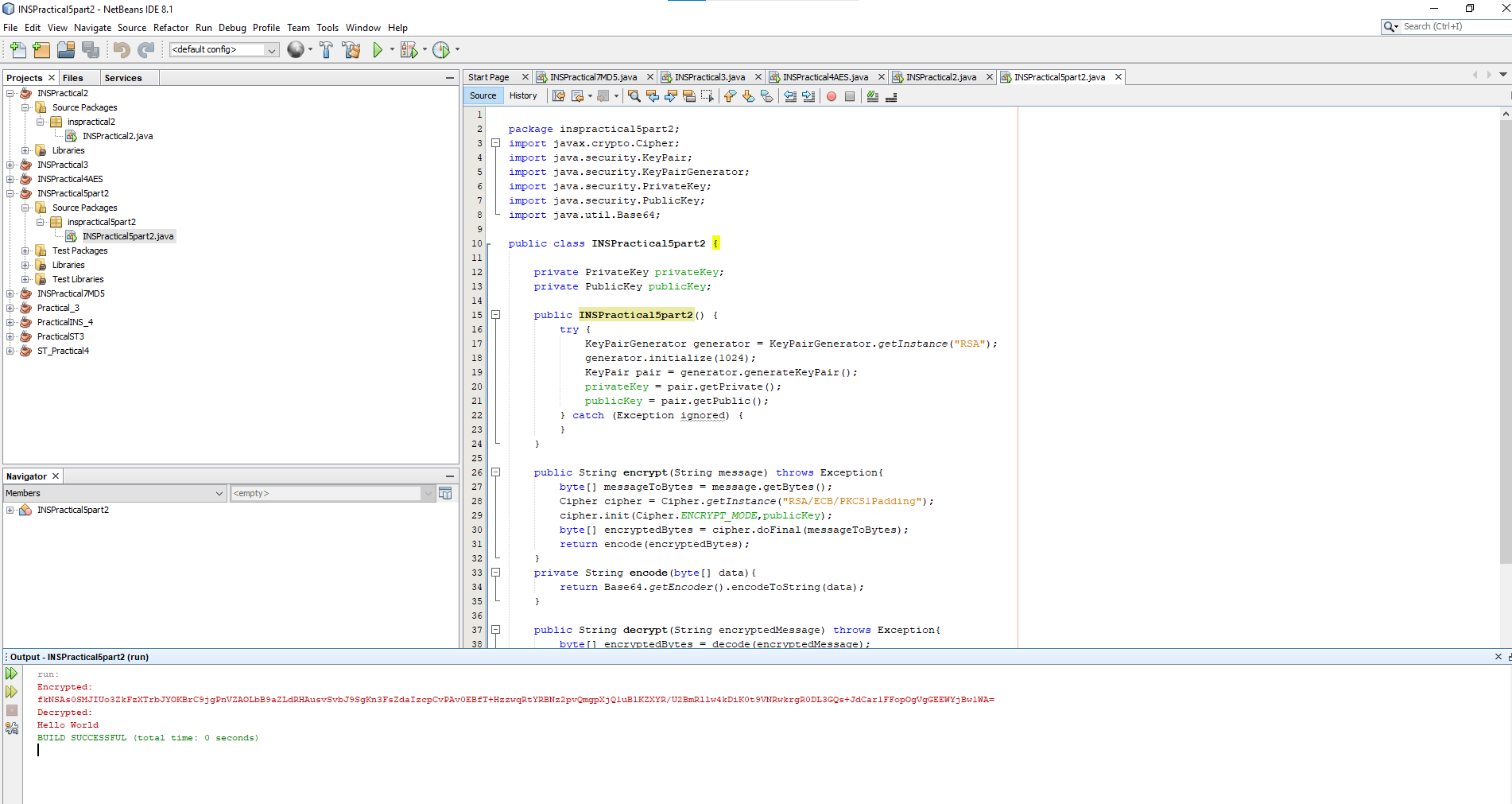
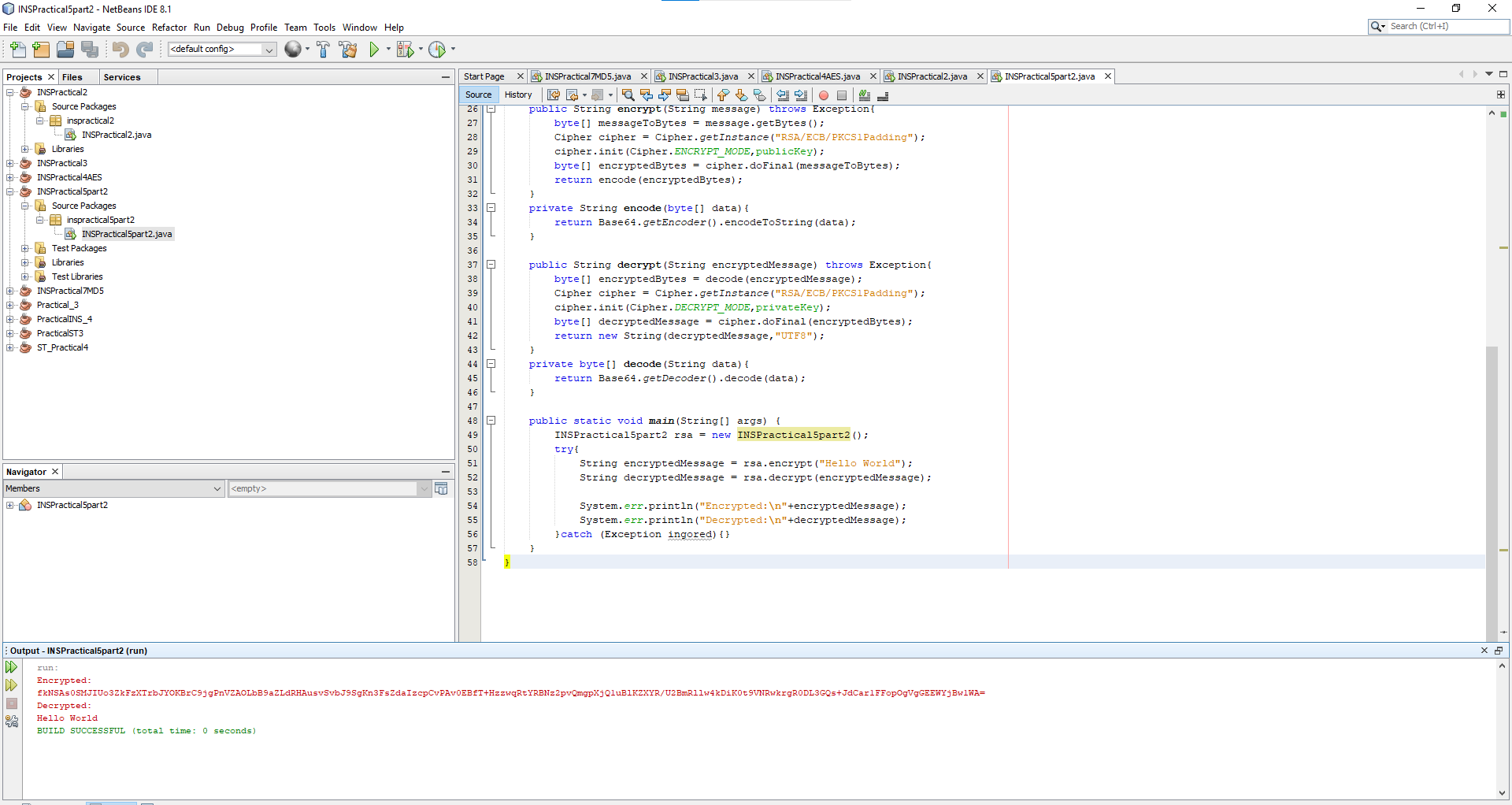
Practical 5

Name:-Satishkumar Rajan Nadar

Aim:-RSA





package inspractical5part2;

import javax.crypto.Cipher;

import java.security.KeyPair;

import java.security.KeyPairGenerator;

import java.security.PrivateKey;

import java.security.PublicKey;

import java.util.Base64;

public class INSPractical5part2 {

private PrivateKey privateKey;

private PublicKey publicKey;

public INSPractical5part2() {

try {

KeyPairGenerator generator = KeyPairGenerator.getInstance("RSA");

generator.initialize(1024);

KeyPair pair = generator.generateKeyPair();

privateKey = pair.getPrivate();

publicKey = pair.getPublic();

} catch (Exception ignored) {

}

}

public String encrypt(String message) throws Exception{

byte[] messageToBytes = message.getBytes();

Cipher cipher = Cipher.getInstance("RSA/ECB/PKCS1Padding");

cipher.init(Cipher.ENCRYPT\_MODE,publicKey);

byte[] encryptedBytes = cipher.doFinal(messageToBytes);

return encode(encryptedBytes);

}

private String encode(byte[] data){

return Base64.getEncoder().encodeToString(data);

}

public String decrypt(String encryptedMessage) throws Exception{

byte[] encryptedBytes = decode(encryptedMessage);

Cipher cipher = Cipher.getInstance("RSA/ECB/PKCS1Padding");

cipher.init(Cipher.DECRYPT\_MODE,privateKey);

byte[] decryptedMessage = cipher.doFinal(encryptedBytes);

return new String(decryptedMessage,"UTF8");

}

private byte[] decode(String data){

return Base64.getDecoder().decode(data);

}

public static void main(String[] args) {

INSPractical5part2 rsa = new INSPractical5part2();

try{

String encryptedMessage = rsa.encrypt("Hello World");

String decryptedMessage = rsa.decrypt(encryptedMessage);

System.err.println("Encrypted:\n"+encryptedMessage);

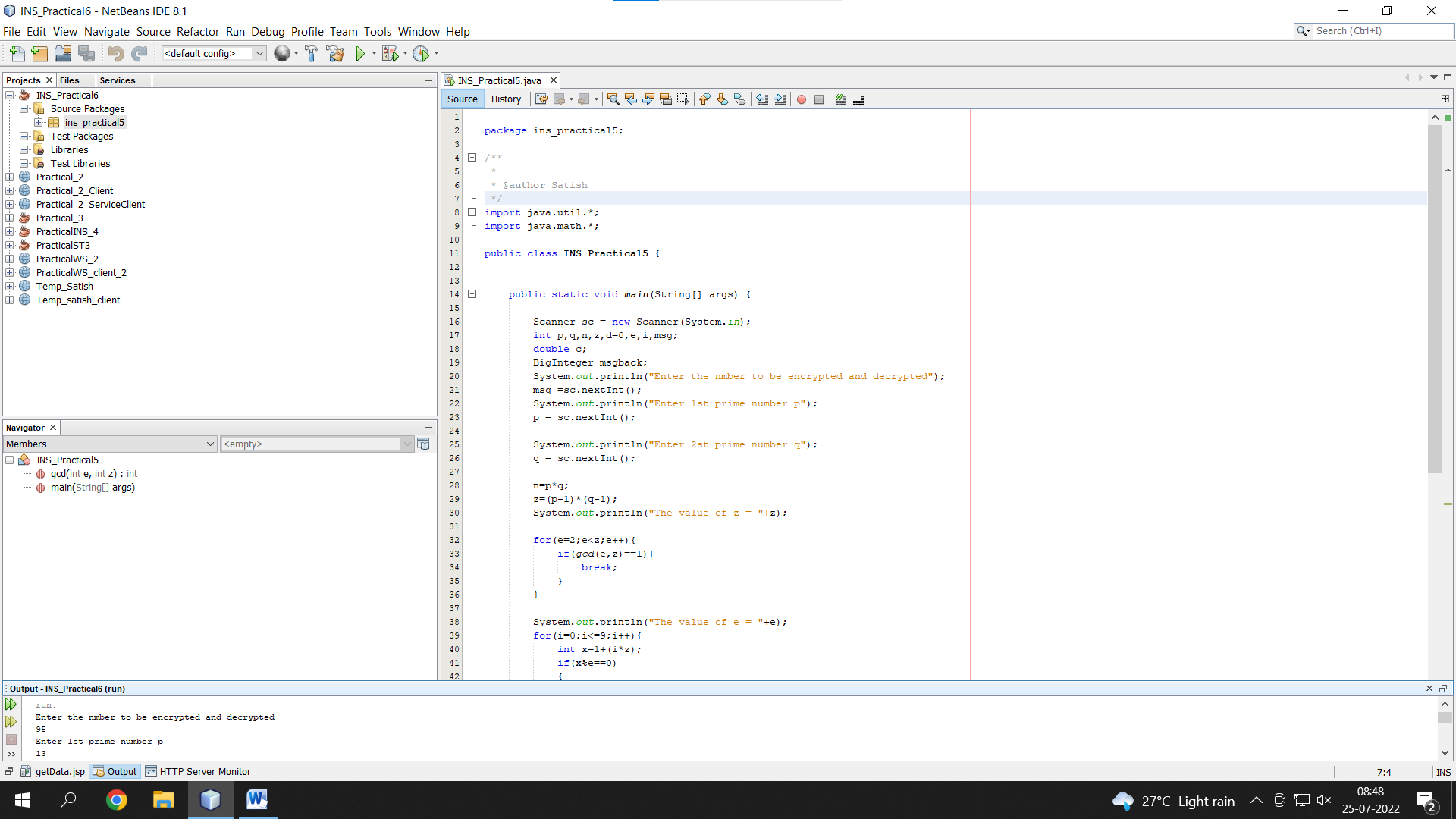
System.err.println("Decrypted:\n"+decryptedMessage);

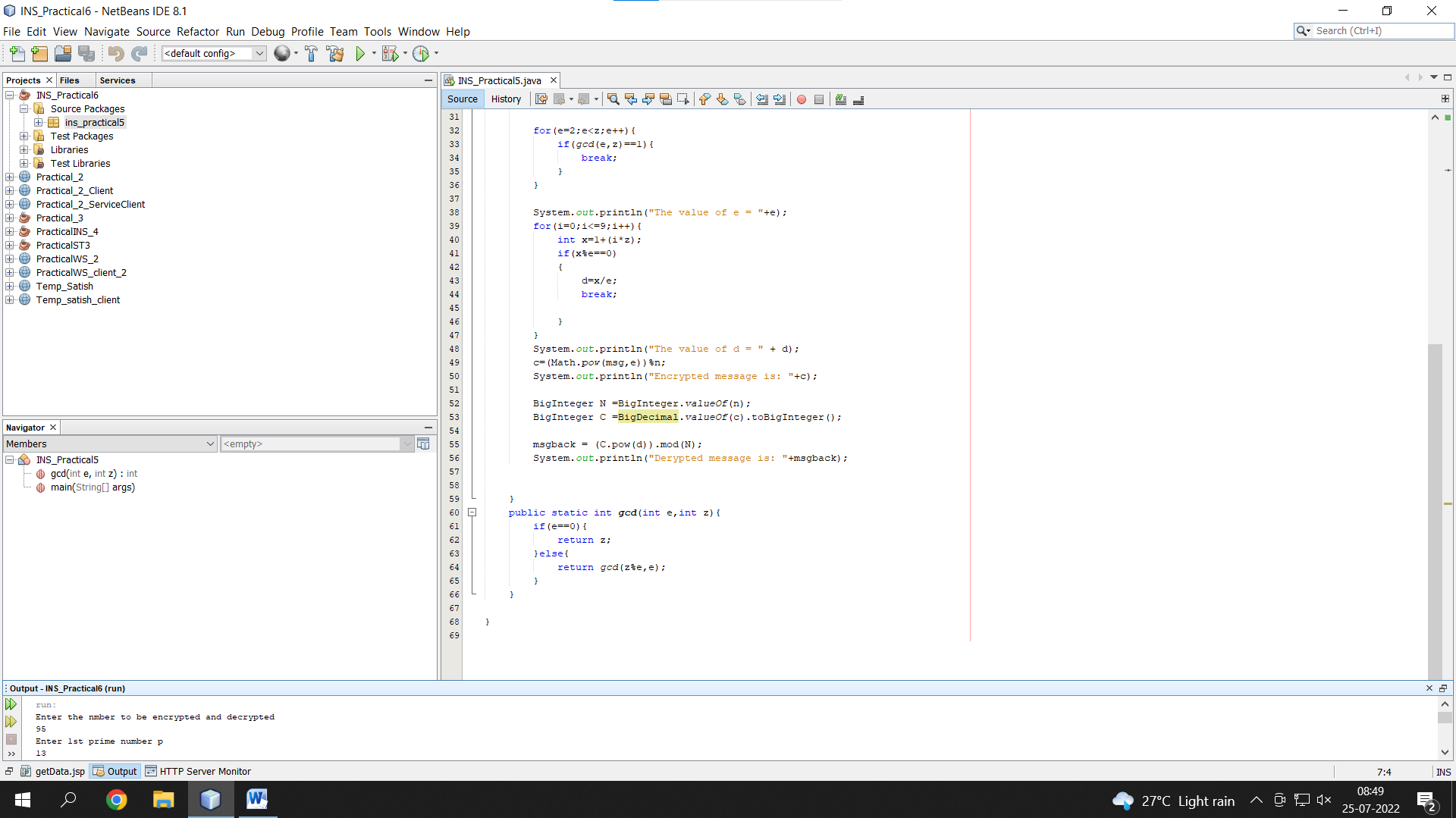
}catch (Exception ingored){}

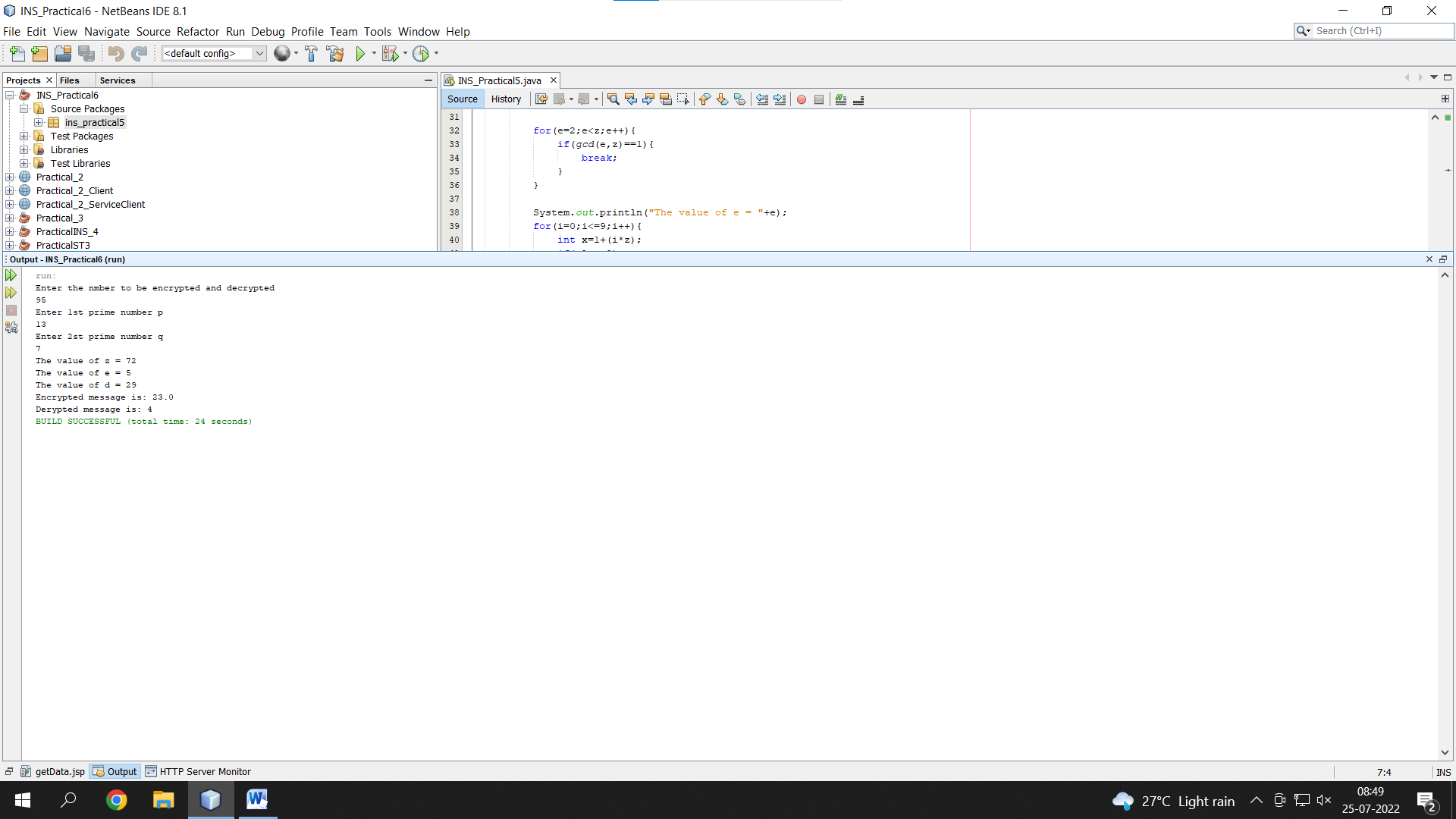
}

}

Part 2







package ins\_practical5;

/\*\*

\*

\* @author Satish

\*/

import java.util.\*;

import java.math.\*;

public class INS\_Practical5 {

public static void main(String[] args) {

Scanner sc = new Scanner(System.in);

int p,q,n,z,d=0,e,i,msg;

double c;

BigInteger msgback;

System.out.println("Enter the nmber to be encrypted and decrypted");

msg =sc.nextInt();

System.out.println("Enter 1st prime number p");

p = sc.nextInt();

System.out.println("Enter 2st 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){

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=x/e;

break;

}

}

System.out.println("The value of d = " + d);

c=(Math.pow(msg,e))%n;

System.out.println("Encrypted message is: "+c);

BigInteger N =BigInteger.valueOf(n);

BigInteger C =BigDecimal.valueOf(c).toBigInteger();

msgback = (C.pow(d)).mod(N);

System.out.println("Derypted message is: "+msgback);

}

public static int gcd(int e,int z){

if(e==0){

return z;

}else{

return gcd(z%e,e);

}

}

}