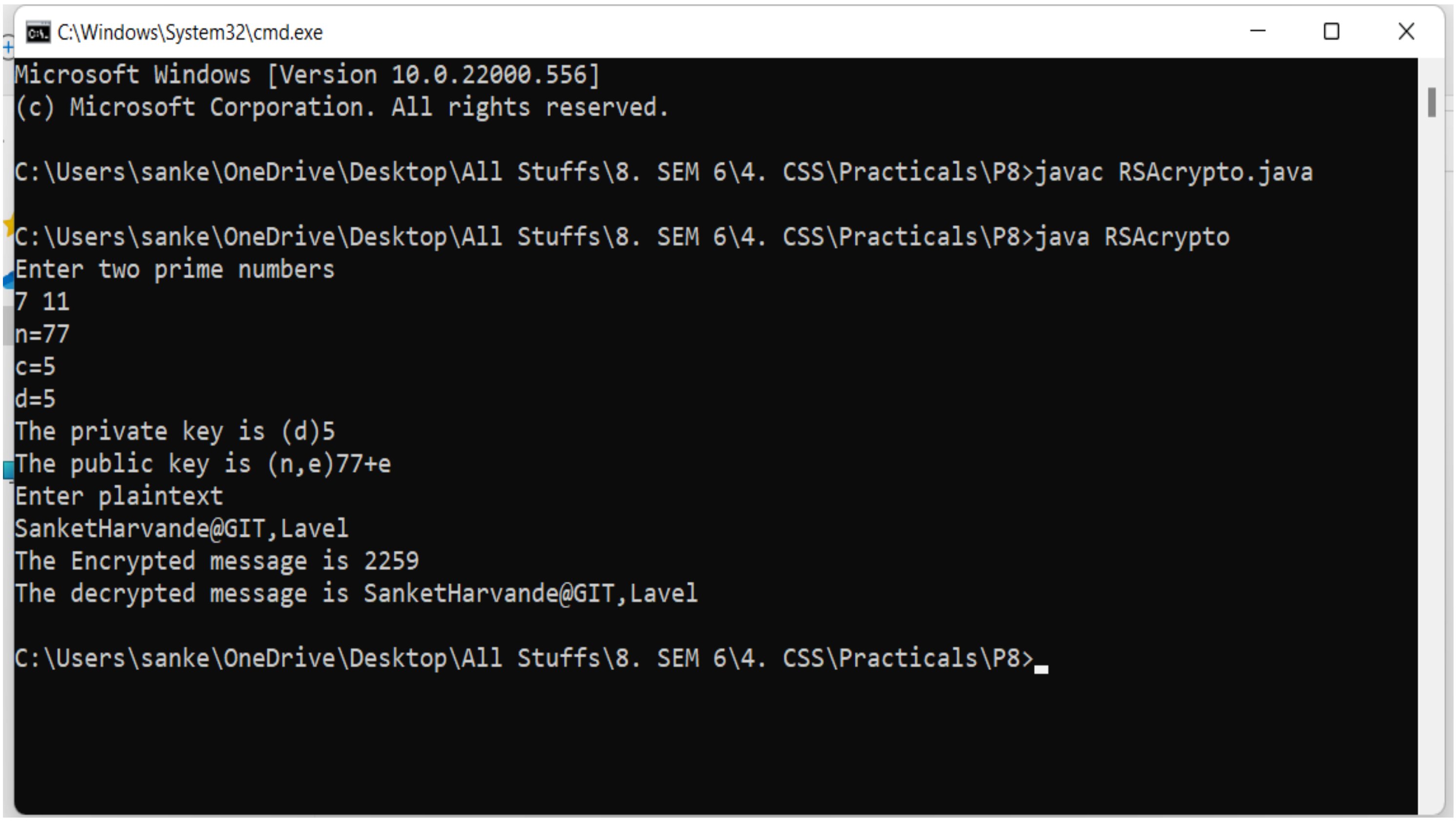
Program and Output

Program :

```
import java.util.*;
class RSAcrypto {
public static void main(String args[]) {
Scanner sc=new Scanner(System.in);
int d=0;
System.out.println("Enter two prime numbers");
int p=sc.nextInt();
int q=sc.nextInt();
int n=p*q;
System.out.println("n="+n);
int e=0;
int pn=(p-1);
search:
{
for(int i=2; i<=pn; i++) {
int r;
int j=i;
int k=pn;
while(k !=j) {
if(k>j)
k = k-j;
else
j = j-k;
}
if(k==1) {
e=i;
break search;
}}}
System.out.println("c="+e);
go: {
for(int i=1; i<pn; i++) {
int x=(e*i)%pn;
if(x==1) {
System.out.println("d="+i);
System.out.println("The private key is (d)"+i);
d=i;
break go;
}}}
System.out.println("The public key is (n,e)"+n+"+e");
String t;
int c;
System.out.println("Enter plaintext");
t=sc.next();
int m = 0;
for (int i = 0; i<t.length(); i++) {
m+=(int)t.charAt(i);
}
c=((m)^e)%n;
System.out.println("The Encrypted message is "+m);
m=(c^d)%n;
System.out.println("The decrypted message is "+t);
}}
```

Output :

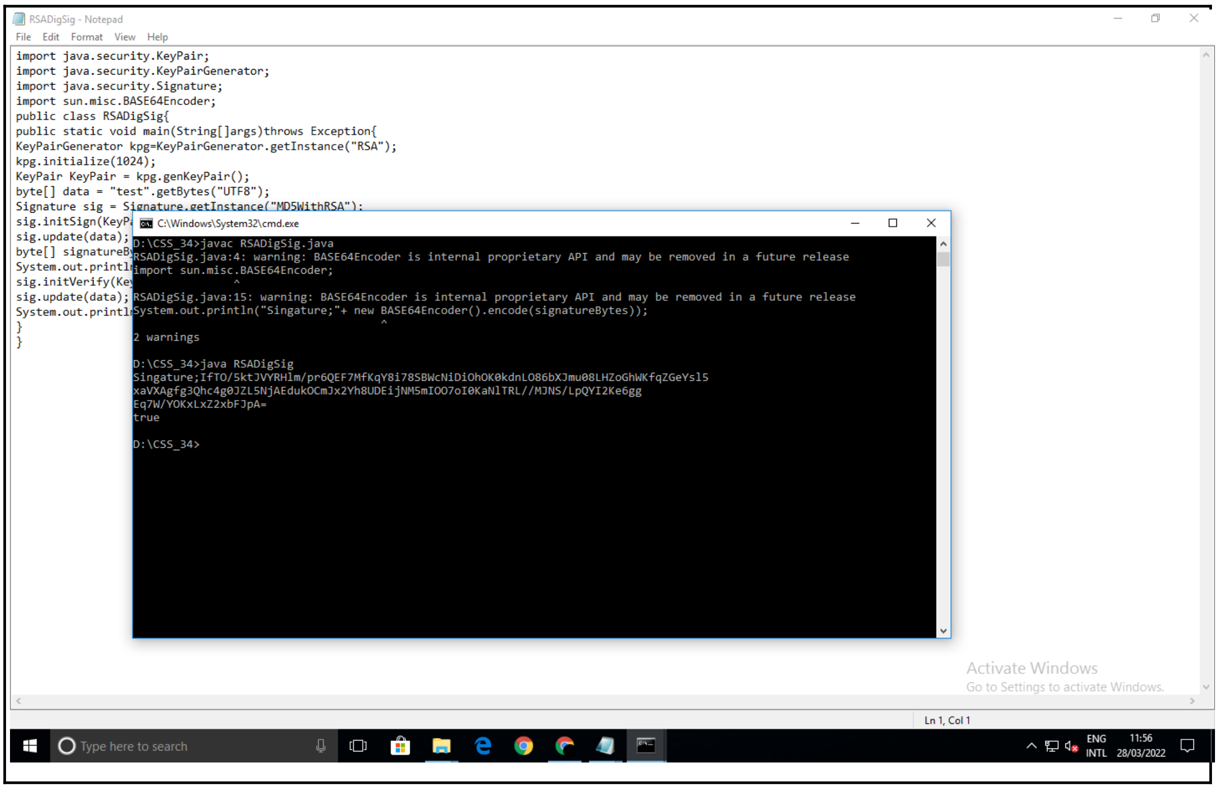


```
Microsoft Windows [Version 10.0.22000.556]
(c) Microsoft Corporation. All rights reserved.

C:\Users\sanke\OneDrive\Desktop\All Stuffs\8. SEM 6\4. CSS\Practicals\P8>javac RSAcrypto.java

C:\Users\sanke\OneDrive\Desktop\All Stuffs\8. SEM 6\4. CSS\Practicals\P8>java RSAcrypto
Enter two prime numbers
7 11
n=77
c=5
d=5
The private key is (d)5
The public key is (n,e)77+e
Enter plaintext
SanketHarvande@GIT,Lavel
The Encrypted message is 2259
The decrypted message is SanketHarvande@GIT,Lavel

C:\Users\sanke\OneDrive\Desktop\All Stuffs\8. SEM 6\4. CSS\Practicals\P8>
```

Program :

```
import java.security.KeyPair;
import java.security.KeyPairGenerator;
import java.security.Signature;
import sun.misc.BASE64Encoder;

public class RSADigSig{
public static void main(String[] args) throws Exception{
KeyPairGenerator kpg = KeyPairGenerator.getInstance("RSA");
kpg.initialize(1024);
KeyPair keyPair = kpg.genKeyPair();
byte[] data = "test".getBytes("UTF8");
Signature sig = Signature.getInstance("MD5WithRSA");
sig.initSign(keyPair.getPrivate());
sig.update(data);
byte[] signatureBytes = sig.sign();
System.out.println("Signature:"+ new
BASE64Encoder().encode(signatureBytes));
sig.initVerify(keyPair.getPublic());
sig.update(data);
System.out.println(sig.verify(signatureBytes));
}
}
```

Output :



RSADigSig - Notepad
File Edit Format View Help
C:\Windows\System32\cmd.exe
Activate Windows
Go to Settings to activate Windows.
Ln 1, Col 1
Type here to search
ENG
INTL
11:56
28/03/2022

```
import java.security.KeyPair;
import java.security.KeyPairGenerator;
import java.security.Signature;
import sun.misc.BASE64Encoder;
public class RSADigSig{
public static void main(String[]args)throws Exception{
KeyPairGenerator kpg=KeyPairGenerator.getInstance("RSA");
kpg.initialize(1024);
KeyPair KeyPair = kpg.genKeyPair();
byte[] data = "test".getBytes("UTF8");
Signature sig = Signature.getInstance("MD5WithRSA");
sig.initSign(KeyPa
sig.update(data);
byte[] signatureBy
System.out.printl
sig.initVerify(Key
sig.update(data);
System.out.printl
}
}
```

```
D:\CSS_34>javac RSADigSig.java
RSADigSig.java:4: warning: BASE64Encoder is internal proprietary API and may be removed in a future release
import sun.misc.BASE64Encoder;
                ^
RSADigSig.java:15: warning: BASE64Encoder is internal proprietary API and may be removed in a future release
System.out.println("Singature;"+ new BASE64Encoder().encode(signatureBytes));
                                     ^

2 warnings

D:\CSS_34>java RSADigSig
Singature;IfTO/5ktJVYRHlm/pr6QEF7MfKqY8i78SBWcNiDiOhOK0kdnLO86bXJmu08LHZoGhWKfqZGeYsl5
xaVXAgfg3Qhc4g0JZL5NjAEdukOCmJx2Yh8UDEijNM5mIOO7oI0KaNlTRL//MJNS/LpQYI2Ke6gg
Eq7W/YOKxLxZ2xbFJpA=
true

D:\CSS_34>
```