**PRACTICAL NO: 4**

**Aim: Write a program to implement RSA algorithm to perform encryption & decryption of a given string.**

**CODE:**

import java.math.\*;

import java.security.\*;

public class RSA{

BigInteger p,q,p1,q1,n,phi,e,d,msg,ct,pt;

SecureRandom r;

public RSA()

{

r=new SecureRandom();

p=new BigInteger(512,100,r);

q=new BigInteger(512,100,r);

n=p.multiply(q);

System.out.println("Prime no p is:"+p.intValue());

System.out.println("Prime no q is :"+q.intValue());

System.out.println("N=P\*Q is:"+n.intValue());

p1=p.subtract(new BigInteger("1"));

q1=q.subtract(new BigInteger("1"));

phi=p1.multiply(q1);

e=new BigInteger("2");

while(phi.gcd(e).intValue()>1 || e.compareTo(p1)!=-1)

{

e=e.add(new BigInteger("1"));

}

System.out.println("Public Key is ("+n.intValue()+","+e.intValue()+")");

d=e.modInverse(phi);

System.out.println("Private key is("+n.intValue()+","+d.intValue()+")");

msg=new BigInteger("3");

ct=msg.modPow(e,n);

System.out.println("Encrypted text is:"+ct.intValue());

pt=ct.modPow(d,n);

System.out.println("Decrypted text is:"+pt.intValue());

}

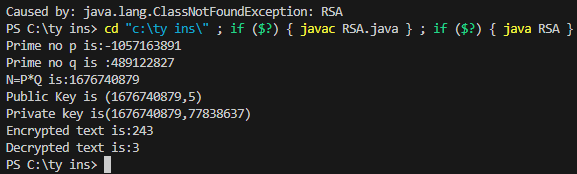
public static void main(String [] args){

new RSA();

}

}

**OUTPUT:**

****