

Program

```
import java.util.*;

public class Rsa {

    static int gcd(int a, int b)
    {
        if (b == 0)
            return a;
        return gcd(b, a % b);
    }

    public static void main(String[] args) {
        // TODO Auto-generated method stub

        Scanner sc = new Scanner(System.in);
        int p,q;

        System.out.println("Enter two prime numbers");
        p = sc.nextInt();
        q = sc.nextInt();

        // First part of public key:
        long n = p*q;

        // Finding other part of public key e stands for encrypt
        int e = 2;
        long phi = (p-1)*(q-1);
        while (e < phi){
            // e must be co-prime to phi and smaller than phi.
            if (gcd((int)e, (int)phi)==1)
                break;
            else
                e++;
        }
        System.out.println(e);
        // Private key (d stands for decrypt)
        // choosing d such that it satisfies  $d \cdot e = 1 + k \cdot \text{totient}$ 
        int k = 1; // A constant value
        double d1;
        long d;
        for(;;k++) {
            d1 = (1 + (k*phi))/(double)e;
            if (d1 == Math.floor(d1))
            {
                break;
            }
        }

        d = (long) d1;
    }
}
```

```

// Message to be encrypted
System.out.println("Enter a small integer");
int msg = sc.nextInt();
System.out.println("Message data:" + msg);

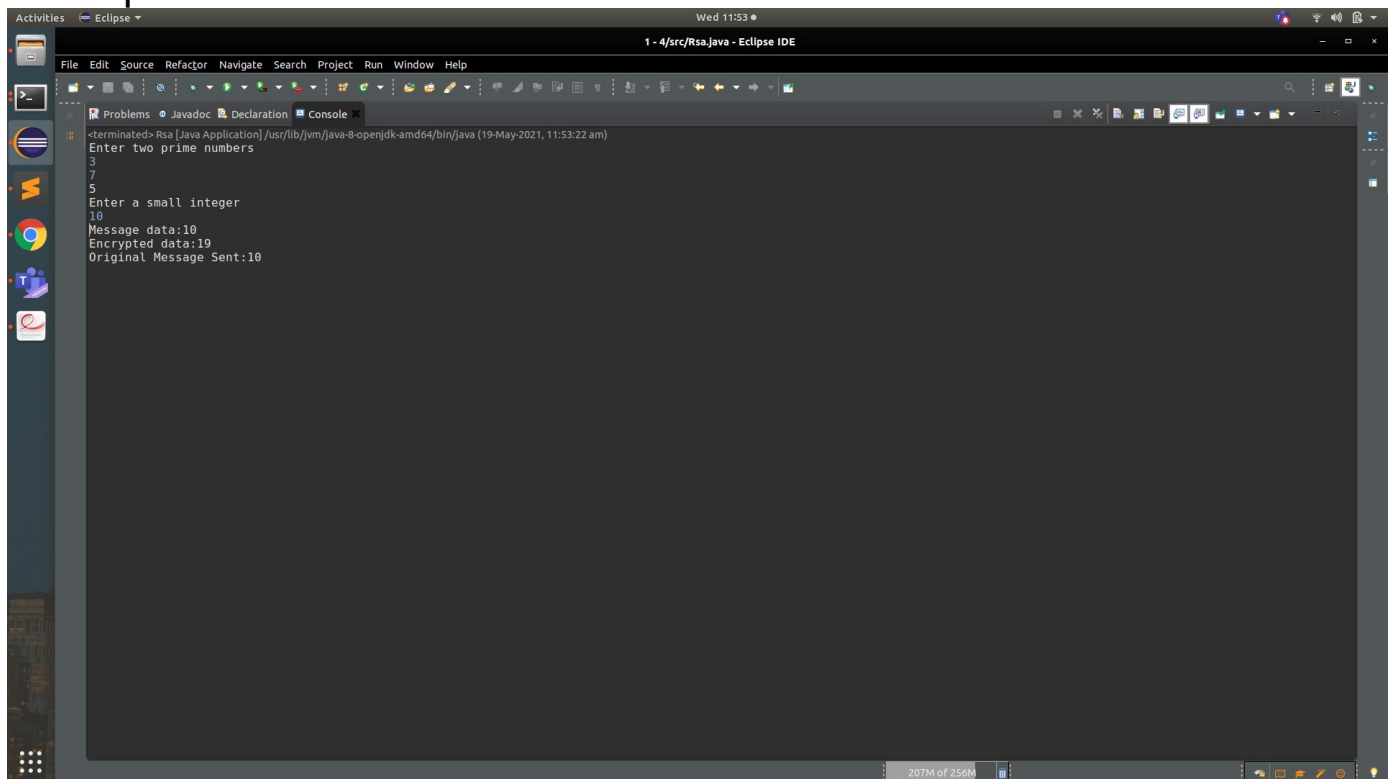
// Encryption c = (msg ^ e) % n
long c = (long) Math.pow(msg, e);
c = c % n;
System.out.println("Encrypted data:"+ c);

//Decryption m = (c ^ d) % n
long m = (long) (Math.pow(c, d));
m = m % n;
System.out.println("Original Message Sent:"+ m);

    sc.close();
}
}

```

Output:



The screenshot shows the Eclipse IDE interface with the console window open. The console output is as follows:

```

<terminated> Rsa [Java Application] /usr/lib/jvm/java-8-openjdk-amd64/bin/java (19-May-2021, 11:53:22 am)
Enter two prime numbers
3
7
5
Enter a small integer
10
Message data:10
Encrypted data:19
Original Message Sent:10

```

The console output matches the program's logic: it prompts for two prime numbers (3, 7, 5), a small integer (10), and then displays the message data (10), the encrypted data (19), and the original message sent (10).