Assignment no 10

Input-

```
#include <iostream>
#include <cmath>
using namespace std;
bool isPrime(int n) {
   if (n <= 1) return false;
   if (n <= 3) return true;

   if (n % 2 == 0 || n % 3 == 0) return false;

   for (int i = 5; i * i <= n; i += 6) {
      if (n % i == 0 || n % (i + 2) == 0) return false;
   }
   return true;
}
int gcd(int a, int b) {
   if (b == 0)
      return a;
   return gcd(b, a % b);
}
void generateKeys(int p, int q, int& n, int& e, int& d)
{
   n = p * q;
   int phi = (p - 1) * (q - 1);
   cout<<" n = " << n <<endl;
   cout<<" phi = " << phi <<endl;

   for (e = 2; e < phi; e++)
         {
```

```
        if (gcd(e, phi) == 1)
          break;
    }
    cout<<" e = " << e <<endl;
    for (d = 2; d < phi; d++)
            {
       if ((d * e) % phi == 1)
          break;
    }
    cout<<" d = "<< d <<endl;
}
void encrypt(int msg, int e, int n, int& c)
{
    c = pow(msg, e);
    c = fmod(c, n);
}
void decrypt(int c, int d, int n, int& m)
{
            m=1;
    for(int i=0;i<d;i++)
    {
            m=(m*c)%n;
            }
}

int main() {
    int p, q, n, e, d, msg, c, m;

    cout << "Enter two prime numbers (p and q): ";
    cin>>p>>q;
```

```
    if (!isPrime(p) || !isPrime(q))
            {
        cout << "Both numbers must be prime." << endl;
        return 1;
    }
    generateKeys(p, q, n, e, d);

    cout << "Enter the message to be encrypted: ";
    cin >> msg;
    encrypt(msg, e, n, c);
    cout << "Encrypted message: " << c << endl;
    decrypt(c, d, n, m);
    cout << "Decrypted message: " << m << endl;

    return 0;
}
```

Output-

```
Enter two prime numbers (p and q): 7 13
 n = 91
 phi = 72
 e = 5
 d = 29
Enter the message to be encrypted: 25
Encrypted message: 51
Decrypted message: 25
```