**Name: Dhanraj Subhash Kore**

**Div : B Roll No: 60**

**Batch: B-3**

**Sub : CS LAB Assignment**

LAB 5 Encryption and Decryption by RSA algorithm

**Code:**

#include<iostream>

#include<math.h>

using namespace std;

//to find gcd

int gcd(int a, int h)

{

int temp;

while (1)

{

temp = a % h;

if (temp == 0)

return h;

a = h;

h = temp;

}

}

int main()

{

double p;

double q;

cout << "enter any two prime no. " << endl;

cin >> p >> q;

double n = p \* q;

double count;

double totient = (p - 1) \* (q - 1);

double e = 2;

while (e < totient) {

count = gcd(e, totient);

if (count == 1)

break;

else

e++;

}

double d;

double k = 2;

double d1 = 1 / e;

d = fmod(d1, totient);

double msg;

cout << "enter message data"<<endl;

cin >> msg;

double c = pow(msg, e);

double m = pow(c, d);

c = fmod(c, n);

m = fmod(m, n);

cout << "Message data = " << msg;

cout << "\n" << "p = " << p;

cout << "\n" << "q = " << q;

cout << "\n" << "n = pq = " << n;

cout << "\n" << "totient = " << totient;

cout << "\n" << "e = " << e;

cout << "\n" << "d = " << d;

cout << "\n" << "Encrypted data = " << c;

cout << "\n" << "Original Message sent = " << m;

return 0;

}

**O/P:**

