Date :

**PRACTICAL-11**

**Objective** – write a program to implement rsa algorithm.

**Code**-

#include <stdio.h>

#include <math.h>

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 = 3;

double q = 7;

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;

d = (1 + (k \* totient)) / e;

double msg = 12;

double c = pow(msg, e);

double m = pow(c, d);

c = fmod(c, n);

m = fmod(m, n);

printf("Message data = %lf", msg);

printf("\np = %lf", p);

printf("\nq = %lf", q);

printf("\nn = pq = %lf", n);

printf("\ntotient = %lf", totient);

printf("\ne = %lf", e);

printf("\nd = %lf", d);

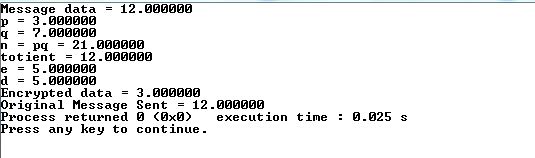
printf("\nEncrypted data = %lf", c);

printf("\nOriginal Message Sent = %lf", m);

return 0;

}

**Output-**

****