Date :

PRACTICAL-11

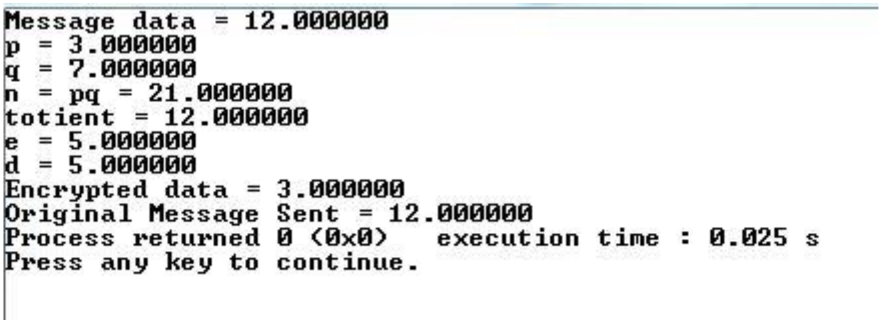
Objective – write a program to implement rsa algorithm.

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-



```
Message data = 12.000000
p = 3.000000
q = 7.000000
n = pq = 21.000000
totient = 12.000000
e = 5.000000
d = 5.000000
Encrypted data = 3.000000
Original Message Sent = 12.000000
Process returned 0 (0x0)   execution time : 0.025 s
Press any key to continue.
```