

## Program: RSA

```
#include<stdio.h>

#include<math.h>

//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(){
    //2 random prime numbers
    double p = 3;
    double q = 7;
    double n=p*q;
    double count;
    double totient = (p-1)*(q-1);
    //public key
    //e stands for encrypt
    double e=2;
    //for checking co-prime which satisfies e>1
    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("Name:Vaibhav Mehar Rollno:58 Batch:B2\n");

printf("Aim:To implement RSA algorithm\n\n");

printf("Message data which is being sent = %lf",msg);

printf("\nThe value of p = %lf",p);

printf("\nThe value of q = %lf",q);

printf("\nThe value of n = pq = %lf",n);

printf("\nThe value of k = %lf",totient);

printf("\nThe value of e = %lf",e);

printf("\nThe value of d = %lf",d);

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

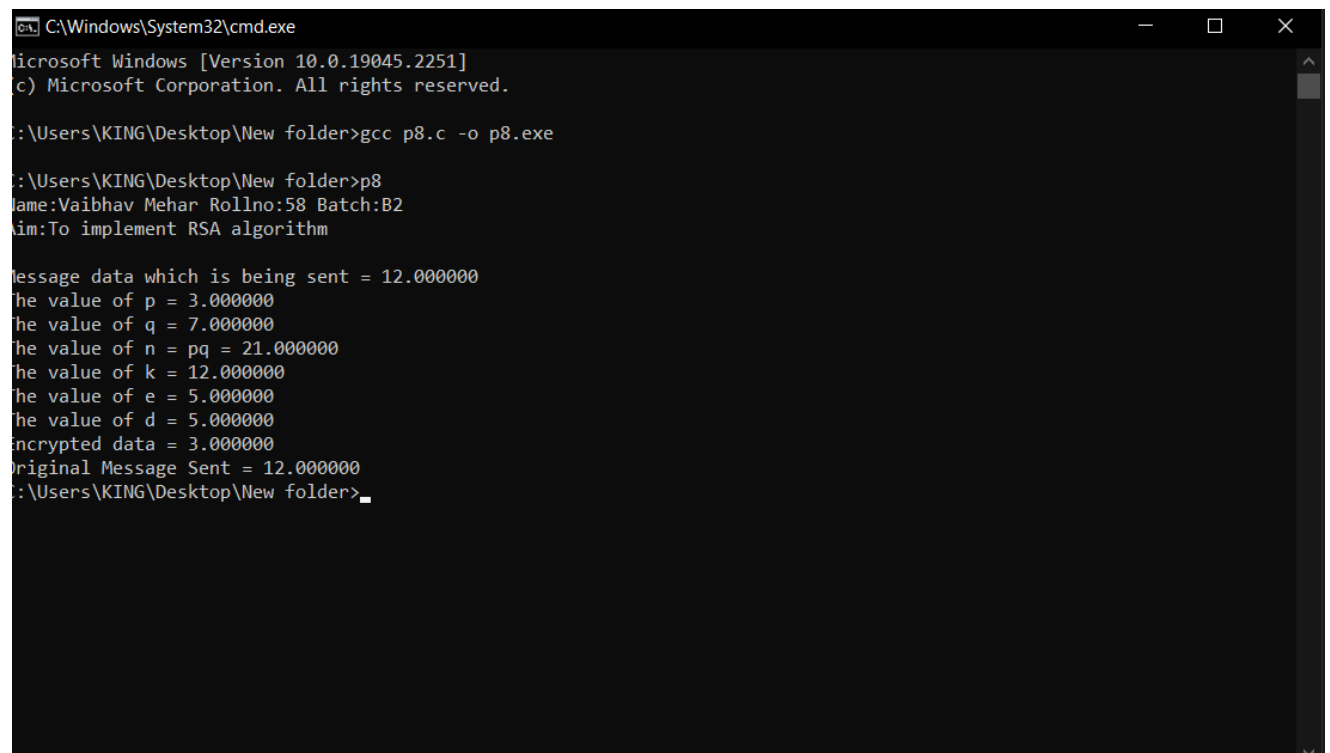
printf("\nOriginal Message Sent = %lf",m);

return 0;

}

```

### Output:



```

C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.19045.2251]
(c) Microsoft Corporation. All rights reserved.

C:\Users\KING\Desktop\New folder>gcc p8.c -o p8.exe

C:\Users\KING\Desktop\New folder>p8
Name:Vaibhav Mehar Rollno:58 Batch:B2
Aim:To implement RSA algorithm

Message data which is being sent = 12.000000
The value of p = 3.000000
The value of q = 7.000000
The value of n = pq = 21.000000
The value of k = 12.000000
The value of e = 5.000000
The value of d = 5.000000
Encrypted data = 3.000000
Original Message Sent = 12.000000
C:\Users\KING\Desktop\New folder>

```