Information Security

Practical-7: Implement RSA Encryption-Decryption algorithm.

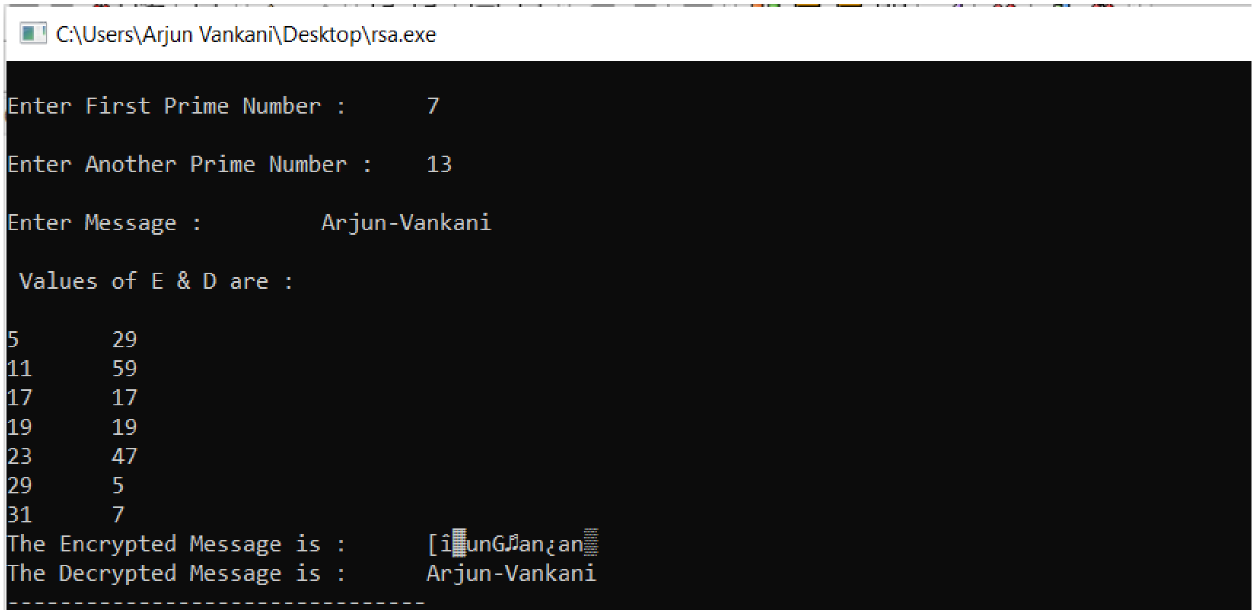
CODE:

```
#include<stdio.h>

#include<stdlib.h>

#include<math.h>

#include<string.h>

long int p,q,n,t,fl,e[100],d[100],temp[100],j,m[100],en[100],i;

char msg[100];

int prime(long int);

void ce();

long int cd(long int);

void encrypt();

void decrypt();

int main()

{

   printf("\nEnter First Prime Number :\t");

   scanf("%ld",&p);

   fl=prime(p);

   if(fl==0)

   {
    printf("\nWRONG INPUT\n");
    exit(1);
}
printf("\nEnter Another Prime Number :\t");
scanf("%ld",&q);
fl=prime(q);
if(fl==0||p==q)
{
    printf("\nWrong Input\n");
    exit(1);
}
printf("\nEnter Message : \t");
fflush(stdin);
scanf("%s",msg);
for(i=0;msg[i]!=NULL;i++)
    m[i]=msg[i];
n=p*q;
t=(p-1)*(q-1);
ce();
printf("\n Values of E & D are :\n");
for(i=0;i<j-1;i++)
    printf("\n%ld\t%ld",e[i],d[i]);
    encrypt();
    decrypt();
    return 0;
}

int prime(long int pr)
{
    int i;
    j=sqrt(pr);
    for(i=2;i<=j;i++)
    {
        if(pr%i==0)
            return 0;
    }
    return 1;
}

void ce()
{
    int k;
    k=0;
    for(i=2;i<t;i++)
```

```
        {
            if(t%i==0)
                continue;
                fl=prime(i);
            if(fl==1&&i!=p&&i!=q)
            {
                e[k]=i; fl=cd(e[k]);
                if(fl>0)
        {
            d[k]=fl;
            k++;
        }
        if(k==99)
            break;
        }
    }
}

long int cd(long int x)
{
    long int k=1;
    while(1)
    {
        k=k+t;
        if(k%x==0)
            return(k/x);
    }
}
void encrypt()
{
    long int pt,ct,key=e[0],k,len;
    i=0;
    len=strlen(msg);
    while(i!=len)
    {
        pt=m[i];
        pt=pt-96;
        k=1;
        for(j=0;j<key;j++)
        {
            k=k*pt;
            k=k%n;
        }
        temp[i]=k;
    ct=k+96;
    en[i]=ct;
    i++;
  }
  en[i]=-1;
  printf("\nThe Encrypted Message is :\t");
  for(i=0;en[i]!=-1;i++)
    printf("%c",en[i]);
}
void decrypt()
{
  long int pt,ct,key=d[0],k;
  i=0;
  while(en[i]!=-1)
  {
    ct=temp[i];
    k=1;
    for(j=0;j<key;j++)
    {
      k=k*ct;
      k=k%n;
    }
```

```
        pt=k+96;

        m[i]=pt;

        i++;

    }

    m[i]=-1;

    printf("\nThe Decrypted Message is : \t");

    for(i=0;m[i]!=-1;i++)

        printf("%c",m[i]);

}
```

Output:



C:\Users\Arjun Vankani\Desktop\rsa.exe

```
Enter First Prime Number :      7

Enter Another Prime Number :    13

Enter Message :         Arjun-Vankani

 Values of E & D are :

5       29
11      59
17      17
19      19
23      47
29      5
31      7
The Encrypted Message is :      [î▓unG♫an¿an▒
The Decrypted Message is :      Arjun-Vankani
--------------------------------
```