Practical no: 4

Name: Saloni Vishwakarma
Batch-Roll no: C1-13
Subject: Cryptography Lab

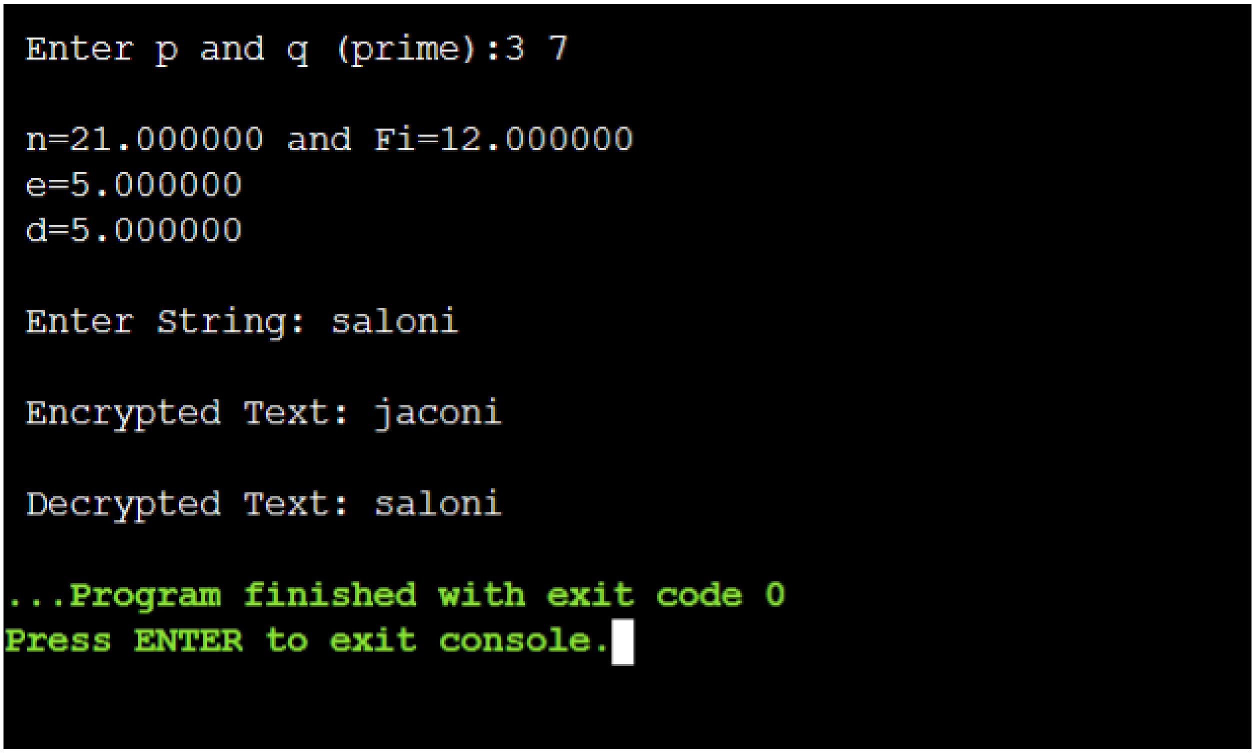
Aim: Administer RSA cryptosystem to build a public key infrastructure (PKI).

RSA Algorithm (Code and Output):

```
#include<stdio.h>
#include<math.h>
#include<string.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,q,n,Fi,e=2,k,d=2;
   char text[100],enc[100],dec[100],text_ascii[100];
   double len;
   //e=public key (cipher)
   //d=private key (decipher)

   printf("\n Enter p and q (prime):");
   scanf("%lf %lf",&p,&q);
   n=p*q;
   Fi=(p-1)*(q-1);
```

```
printf("\n n=%lf and Fi=%lf",n,Fi);

while(e<Fi){
    k = gcd(e,Fi);
    if(k==1)
        break;
    else
        e++;

}

printf("\n e=%lf",e);
while( fmod((e*d),Fi)!=1)
{
    d++;
}
printf("\n d=%lf",d);
printf("\n\n Enter String: ");
scanf("%s",text);
len=strlen(text);

//Encrypt
for(int i =0;i<len;i++)
{
    text_ascii[i]=text[i]-97;
    enc[i]=fmod((pow(text_ascii[i],e)),n);
    enc[i]=fmod(enc[i],26)+97;
}
printf("\n Encrypted Text: ");
for(int i=0;i<len;i++)
    printf("%c",enc[i]);

//Decrypt
for(int i =0;i<len;i++)
{
    text_ascii[i]=enc[i]-97;
    printf("%c",text_ascii[i]);
    dec[i]=fmod((pow(text_ascii[i],d)),n);
    dec[i]=fmod(dec[i],26)+97;
}
```

```
    printf("\n\n Decrypted Text: ");
    for(int i=0;i<len;i++)
    printf("%c",dec[i]);
}
```



```
 Enter p and q (prime):3 7

 n=21.000000 and Fi=12.000000
 e=5.000000
 d=5.000000

 Enter String: saloni

 Encrypted Text: jaconi

 Decrypted Text: saloni

...Program finished with exit code 0
Press ENTER to exit console.
```