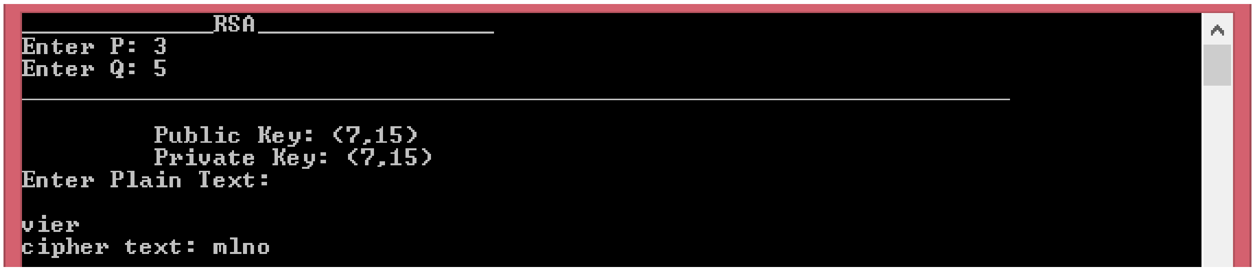
Practical:-7

Aim :-Implement RSA key generation.

```
#include <stdio.h>
#include<conio.h>
#include<string.h>
void E(char *s,char *enc,int e,int n){
        int i=0,j,l;
        l=strlen(s);
        while(i<l)    {
                j=(((s[i]%97)*e)%n)%26;
                enc[i++]=j+97;      }
        enc[i]='\0';
}
int euclid(int d,int f){
        int x,y,r;
        x=f;
        y=d;
        while(y!=0) {
                r=x%y;
                x=y;
                y=r; }
        return(x);    }
int exteuclid(int e,int r)  {
        int x[3],y[3],t[3],q;
        x[0]=1;y[0]=0;
        x[1]=0;y[1]=1;
        x[2]=r;y[2]=e;
        while(1) {
                if(y[2]<2)
                break;
                else    {
                q=(x[2]/y[2]);
                t[0]=x[0]-q*y[0];
                t[1]=x[1]-q*y[1];
                t[2]=x[2]-q*y[2];
                x[0]=y[0];
                x[1]=y[1];
                x[2]=y[2];
                y[0]=t[0];
                y[1]=t[1];
        y[2]=t[2];      }}
if(y[2]==0)
return 0;
else    {
        if(y[1]<0)
        return (r+y[1]);
        else
        return (y[1]);
        }
}
int main() {
        int p,q,n,r,e,d,i;
        char *s,*enc;
        printf("______________RSA_________________\n");
        printf("Enter P: ");
        scanf("%d",&p);
        printf("Enter Q: ");
        scanf("%d",&q);
        n=p*q;
        r=(p-1)*(q-1);
        if(q>p)
                i=q+1;
        else
                i=p+1;
        while(1)        {
                e=euclid(i++,r);
                if(e==1)
                        break;
        }
        e=i-1;
        d=exteuclid(e,r);
        printf("________________________________________________________________
_______\n\n");
```

```
printf("\n\n\t Public Key: (%d,%d)\n",e,n);
printf("\t Private Key: (%d,%d)\n",d,n);
printf("Enter Plain Text: \n\n");
scanf("%s",s);
E(s,enc,e,n);
printf("cipher text: %s",enc);
return 0;
getch();    }
```

Output:-



```
_________________RSA_____________________
Enter P: 3
Enter Q: 5
________________________________________________________________________________

           Public Key: (7,15)
           Private Key: (7,15)
Enter Plain Text:

vier
cipher text: mlno
```