RSA ALGO IMPLEMENTATION IN C/S MODEL USING C LANGUAGE

The prime numbers used are 11 and 13.

HOW TO EXECUTE THE C CODE FILES:

1. Compile the server file first. Filename : serverrsa.c

   Command : gcc serverrsa.c -lm

```
bharat@khandelwal-PC:~/Downloads/3-2/ComputerNetworks/lab$ gcc serverrsa.c -lm
serverrsa.c: In function ‘isprime’:
serverrsa.c:23:31: warning: implicit declaration of function ‘sqrt’ [-Wimplicit-function-declaration]
     for(long long int i=2; i<=sqrt(x); i++)
                               ^~~~
serverrsa.c:23:31: warning: incompatible implicit declaration of built-in function ‘sqrt’
serverrsa.c:23:31: note: include ‘<math.h>’ or provide a declaration of ‘sqrt’
serverrsa.c: In function ‘error’:
serverrsa.c:65:5: warning: implicit declaration of function ‘exit’ [-Wimplicit-function-declaration]
     exit(1);
     ^~~~
serverrsa.c:65:5: warning: incompatible implicit declaration of built-in function ‘exit’
serverrsa.c:65:5: note: include ‘<stdlib.h>’ or provide a declaration of ‘exit’
serverrsa.c: In function ‘main’:
serverrsa.c:94:10: warning: incompatible implicit declaration of built-in function ‘exit’
          exit(1);
          ^~~~
serverrsa.c:94:10: note: include ‘<stdlib.h>’ or provide a declaration of ‘exit’
serverrsa.c:99:6: warning: implicit declaration of function ‘bzero’ [-Wimplicit-function-declaration]
      bzero((char *) &serv_addr, sizeof(serv_addr));
      ^~~~~
serverrsa.c:99:6: warning: incompatible implicit declaration of built-in function ‘bzero’
serverrsa.c:100:15: warning: implicit declaration of function ‘atoi’ [-Wimplicit-function-declaration]
      portno = atoi(argv[1]);
               ^~~~
serverrsa.c:117:11: warning: implicit declaration of function ‘read’; did you mean ‘fread’? [-Wimplicit-function-declaration]
      n1 = read(newsockfd,buffer,255);
           ^~~~
           fread
serverrsa.c:127:10: warning: implicit declaration of function ‘write’; did you mean ‘fwrite’? [-Wimplicit-function-declaration]
     n1 = write(newsockfd,buffer,strlen(buffer));
          ^~~~~
          fwrite
serverrsa.c:127:33: warning: implicit declaration of function ‘strlen’ [-Wimplicit-function-declaration]
     n1 = write(newsockfd,buffer,strlen(buffer));
                                 ^~~~~~
serverrsa.c:127:33: warning: incompatible implicit declaration of built-in function ‘strlen’
serverrsa.c:127:33: note: include ‘<string.h>’ or provide a declaration of ‘strlen’
```

2. Run the server file giving a portnumber.

   Command : ./a.out 5050

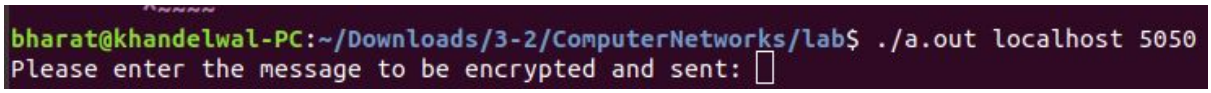
```
bharat@khandelwal-PC:~/Downloads/3-2/ComputerNetworks/lab$ ./a.out 5050
```

3. Compile the client file next. Filename : clientrsa.c

   Command : gcc clientrsa.c -lm

```
bharat@khandelwal-PC:~/Downloads/3-2/ComputerNetworks/lab$ gcc clientrsa.c -lm
clientrsa.c: In function ‘error’:
clientrsa.c:28:5: warning: implicit declaration of function ‘exit’ [-Wimplicit-function-declaration]
     exit(0);
     ^~~~
clientrsa.c:28:5: warning: incompatible implicit declaration of built-in function ‘exit’
clientrsa.c:28:5: note: include ‘<stdlib.h>’ or provide a declaration of ‘exit’
clientrsa.c: In function ‘main’:
clientrsa.c:40:8: warning: incompatible implicit declaration of built-in function ‘exit’
        exit(0);
        ^~~~
clientrsa.c:40:8: note: include ‘<stdlib.h>’ or provide a declaration of ‘exit’
clientrsa.c:42:14: warning: implicit declaration of function ‘atoi’ [-Wimplicit-function-declaration]
     portno = atoi(argv[2]);
              ^~~~
clientrsa.c:49:9: warning: incompatible implicit declaration of built-in function ‘exit’
         exit(0);
         ^~~~
clientrsa.c:49:9: note: include ‘<stdlib.h>’ or provide a declaration of ‘exit’
clientrsa.c:51:5: warning: implicit declaration of function ‘bzero’ [-Wimplicit-function-declaration]
     bzero((char *) &serv_addr, sizeof(serv_addr));
     ^~~~~
clientrsa.c:51:5: warning: incompatible implicit declaration of built-in function ‘bzero’
clientrsa.c:53:5: warning: implicit declaration of function ‘bcopy’ [-Wimplicit-function-declaration]
     bcopy((char *)server->h_addr,
     ^~~~~
clientrsa.c:53:5: warning: incompatible implicit declaration of built-in function ‘bcopy’
clientrsa.c:64:25: warning: implicit declaration of function ‘strlen’ [-Wimplicit-function-declaration]
     long long int len = strlen(str);
                         ^~~~~~
clientrsa.c:64:25: warning: incompatible implicit declaration of built-in function ‘strlen’
clientrsa.c:64:25: note: include ‘<string.h>’ or provide a declaration of ‘strlen’
clientrsa.c:73:10: warning: implicit declaration of function ‘write’; did you mean ‘fwrite’? [-Wimplicit-function-declaration]
     n1 = write(sockfd, buffer, strlen(buffer));
          ^~~~~
          fwrite
clientrsa.c:79:10: warning: implicit declaration of function ‘read’; did you mean ‘fread’? [-Wimplicit-function-declaration]
     n1 = read(sockfd,buffer,255);
```

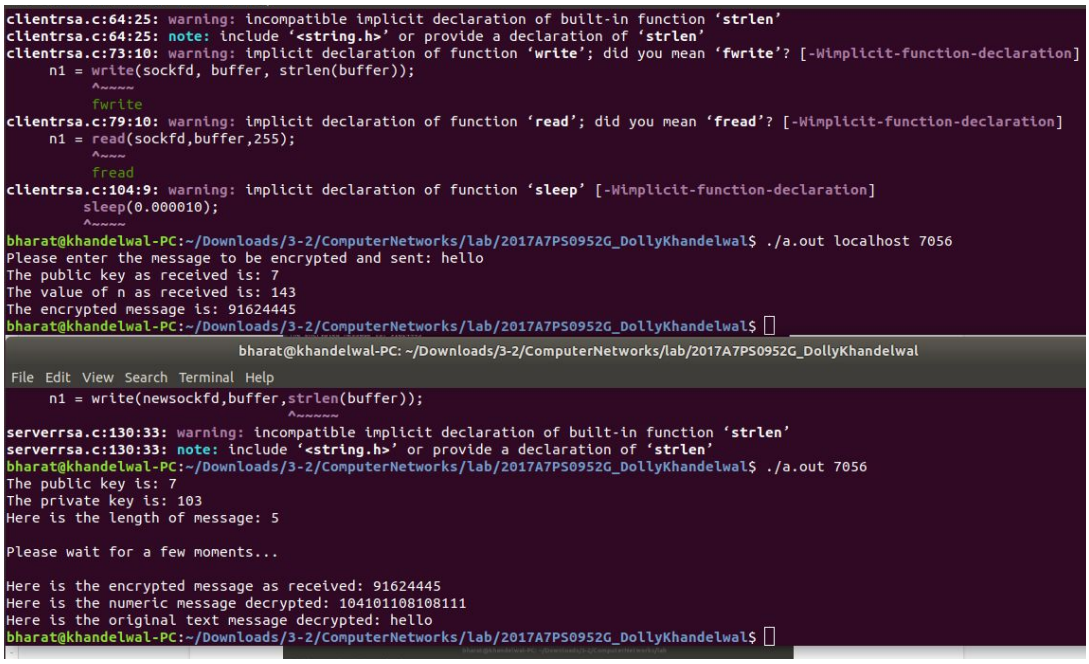
4. Run the client file giving the same portnumber.
   Command : ./a.out localhost 5050



Screenshots are given below for two inputs.
Input 1: hello
Input 2: abcdefghijklmnopqrstuvwxyz

PLEASE WAIT A FEW MOMENTS FOR THE OUTPUT TO BE DISPLAYED ON THE SCREEN.

1.



2.