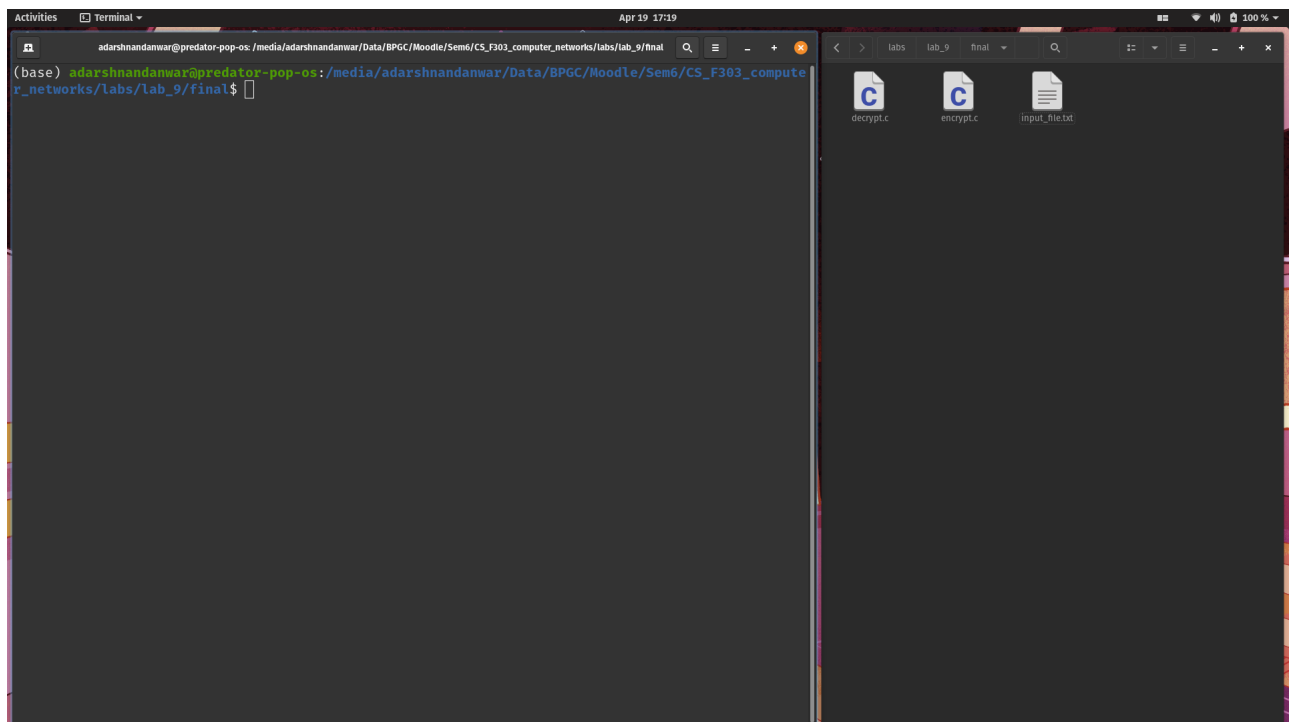


Lab 9

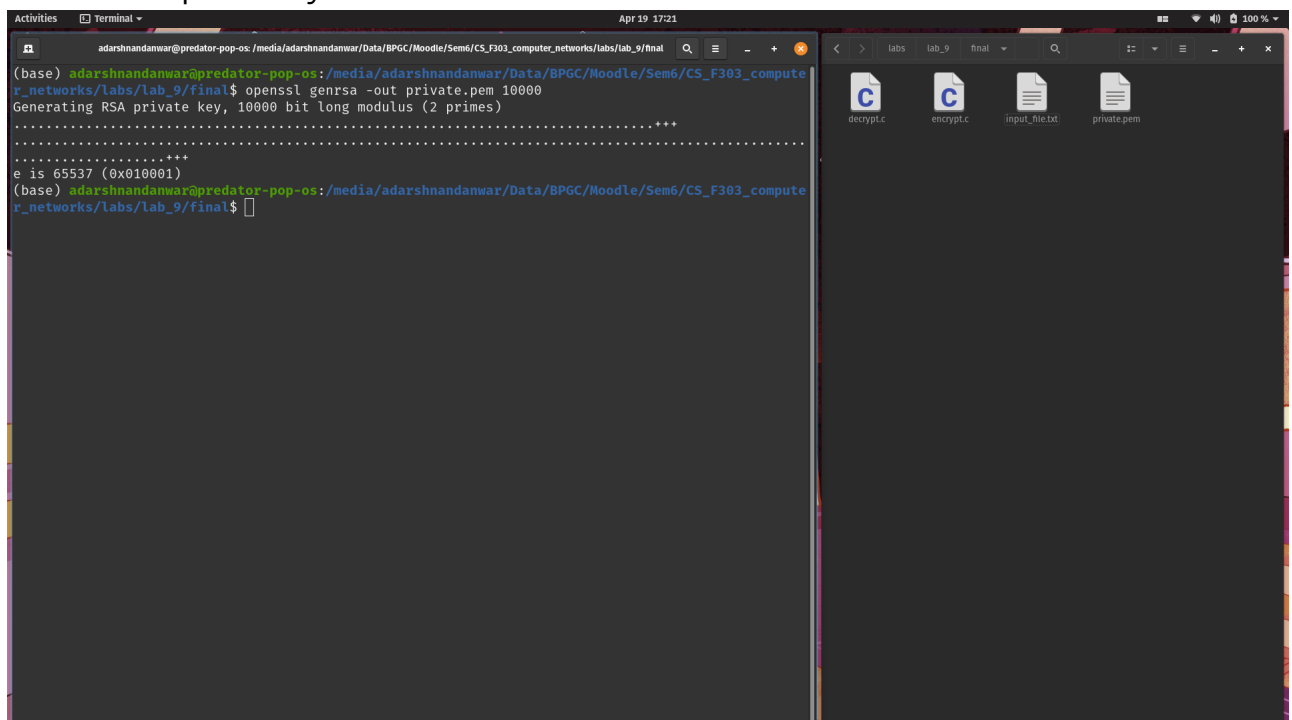
Name- Adarsh Nandanwar
BITS ID- 2018A7PS0396G

Program Screenshots

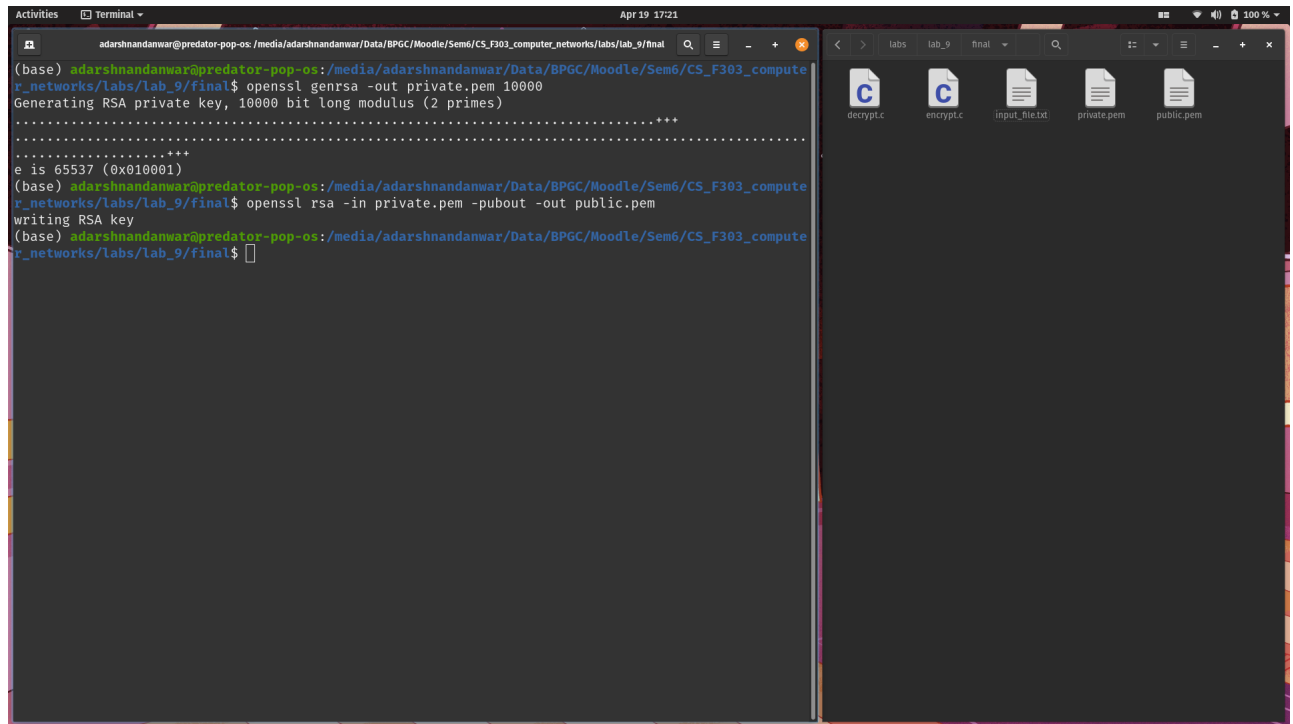
1. Open a terminal window in the directory containing `input_file.txt`, `encrypt.c` and `decrypt.c` file.



2. Generate the private key.

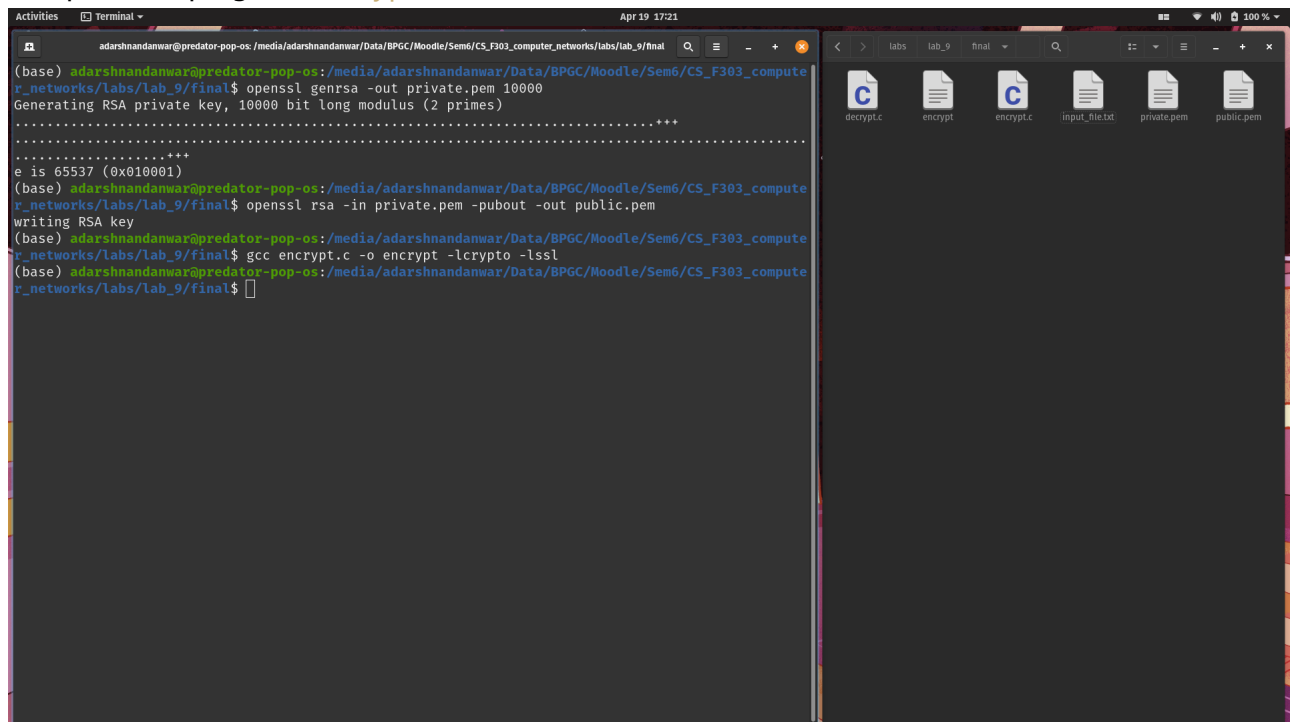


3. Generate the public key.

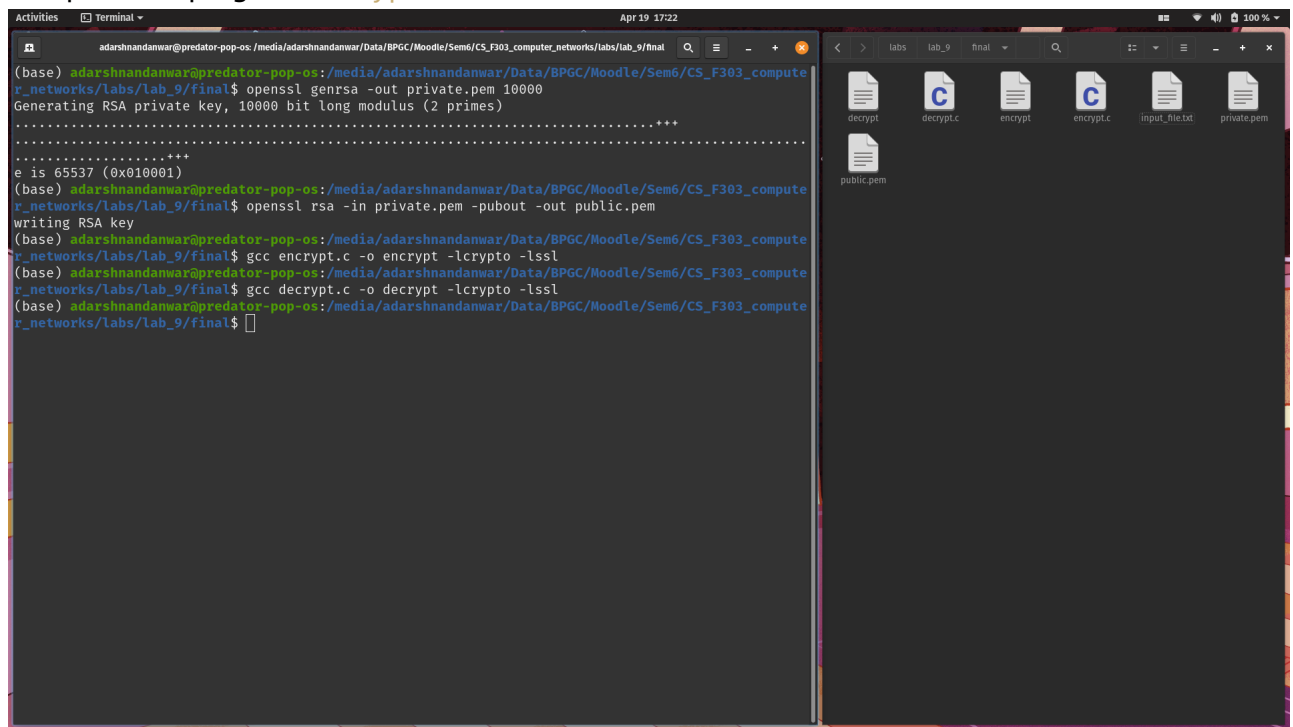


```
(base) adarshnandanwar@predator-pop-os:/media/adarshnandanwar/Data/BPGC/Moodle/Sem6/CS_F303_computer_networks/labs/lab_9/final$ openssl genrsa -out private.pem 10000
Generating RSA private key, 10000 bit long modulus (2 primes)
.....+++
e is 65537 (0x010001)
(base) adarshnandanwar@predator-pop-os:/media/adarshnandanwar/Data/BPGC/Moodle/Sem6/CS_F303_computer_networks/labs/lab_9/final$ openssl rsa -in private.pem -pubout -out public.pem
writing RSA key
(base) adarshnandanwar@predator-pop-os:/media/adarshnandanwar/Data/BPGC/Moodle/Sem6/CS_F303_computer_networks/labs/lab_9/final$
```

4. Compile the c program `encrypt.c`.



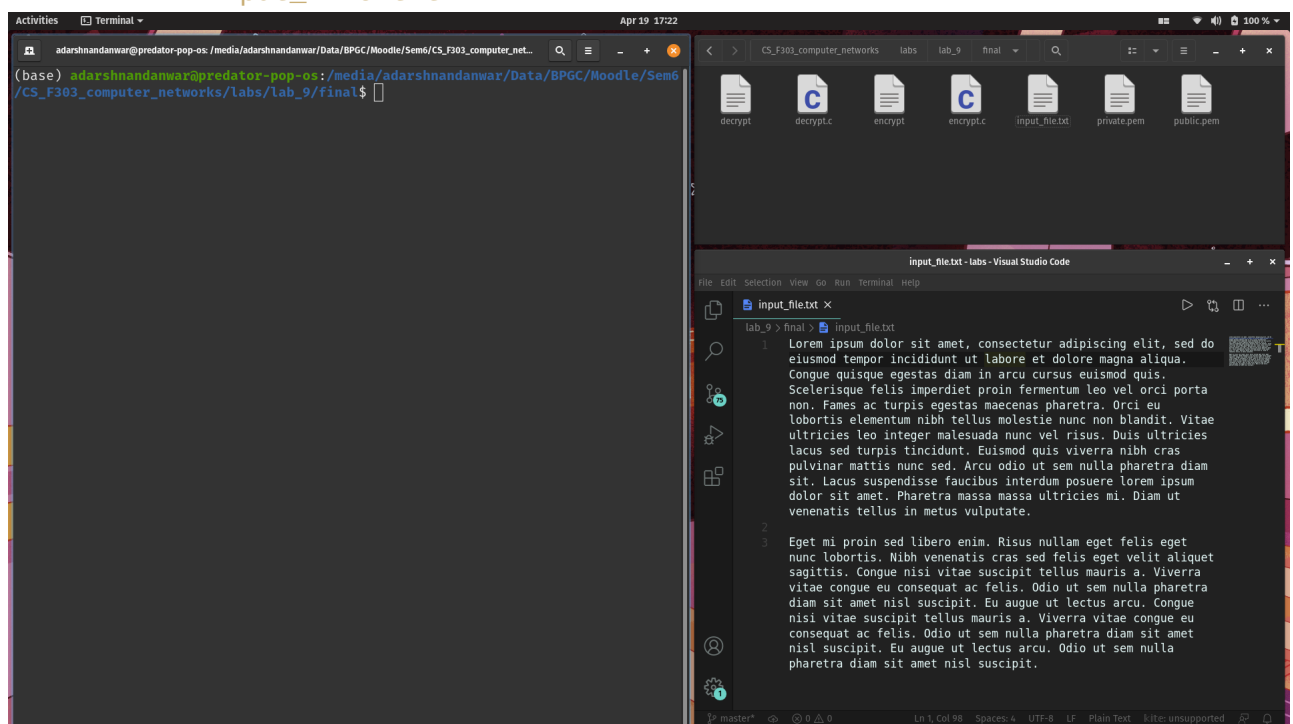
```
(base) adarshnandanwar@predator-pop-os:/media/adarshnandanwar/Data/BPGC/Moodle/Sem6/CS_F303_computer_networks/labs/lab_9/final$ openssl genrsa -out private.pem 10000
Generating RSA private key, 10000 bit long modulus (2 primes)
.....+++
e is 65537 (0x010001)
(base) adarshnandanwar@predator-pop-os:/media/adarshnandanwar/Data/BPGC/Moodle/Sem6/CS_F303_computer_networks/labs/lab_9/final$ openssl rsa -in private.pem -pubout -out public.pem
writing RSA key
(base) adarshnandanwar@predator-pop-os:/media/adarshnandanwar/Data/BPGC/Moodle/Sem6/CS_F303_computer_networks/labs/lab_9/final$ gcc encrypt.c -o encrypt -lcrypto -lssl
(base) adarshnandanwar@predator-pop-os:/media/adarshnandanwar/Data/BPGC/Moodle/Sem6/CS_F303_computer_networks/labs/lab_9/final$
```

5. Compile the c program `decrypt.c`.


```

(base) adarshnandanwar@predator-pop-os: /media/adarshnandanwar/Data/BPGC/Moodle/Sem6/CS_F303_computer_networks/labs/lab_9/final
adarshnandanwar@predator-pop-os: /media/adarshnandanwar/Data/BPGC/Moodle/Sem6/CS_F303_computer_networks/labs/lab_9/final$ openssl genrsa -out private.pem 10000
Generating RSA private key, 10000 bit long modulus (2 primes)
.....+++++
e is 65537 (0x010001)
(base) adarshnandanwar@predator-pop-os: /media/adarshnandanwar/Data/BPGC/Moodle/Sem6/CS_F303_computer_networks/labs/lab_9/final$ openssl rsa -in private.pem -pubout -out public.pem
writing RSA key
(base) adarshnandanwar@predator-pop-os: /media/adarshnandanwar/Data/BPGC/Moodle/Sem6/CS_F303_computer_networks/labs/lab_9/final$ gcc encrypt.c -o encrypt -lcrypto -lssl
(base) adarshnandanwar@predator-pop-os: /media/adarshnandanwar/Data/BPGC/Moodle/Sem6/CS_F303_computer_networks/labs/lab_9/final$ gcc decrypt.c -o decrypt -lcrypto -lssl
(base) adarshnandanwar@predator-pop-os: /media/adarshnandanwar/Data/BPGC/Moodle/Sem6/CS_F303_computer_networks/labs/lab_9/final$

```

6. Add content to `input_file.txt`.


```

(base) adarshnandanwar@predator-pop-os: /media/adarshnandanwar/Data/BPGC/Moodle/Sem6/CS_F303_computer_networks/labs/lab_9/final$ gcc encrypt.c -o encrypt -lcrypto -lssl
(base) adarshnandanwar@predator-pop-os: /media/adarshnandanwar/Data/BPGC/Moodle/Sem6/CS_F303_computer_networks/labs/lab_9/final$ gcc decrypt.c -o decrypt -lcrypto -lssl
(base) adarshnandanwar@predator-pop-os: /media/adarshnandanwar/Data/BPGC/Moodle/Sem6/CS_F303_computer_networks/labs/lab_9/final$

```

input_file.txt - Visual Studio Code

```

1 Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do
  eiusmod tempor incididunt ut labore et dolore magna aliqua.
  Congue quisque egestas diam in arcu cursus euismod quis.
  Scelerisque felis imperdiet proin fermentum leo vel orci porta
  non. Fames ac turpis egestas maecenas pharetra. Orci eu
  lobortis elementum nibh tellus molestie nunc non blandit. Vitae
  ultricies leo integer malesuada nunc vel risus. Duis ultricies
  lacus sed turpis tincidunt. Euismod quis viverra nibh cras
  pulvinar mattis nunc sed. Arcu odio ut sem nulla pharetra diam
  sit. Lacus suspendisse faucibus interdum posuere lorem ipsum
  dolor sit amet. Pharetra massa massa ultricies mi. Diam ut
  venenatis tellus in metus vulputate.

2
3 Eget mi proin sed libero enim. Risus nullam eget felis eget
  nunc lobortis. Nibh venenatis cras sed felis eget velit aliquet
  sagittis. Congue nisi vitae suscipit tellus mauris a. Viverra
  vitae congue eu consequat ac felis. Odio ut sem nulla pharetra
  diam sit amet nisl suscipit. Eu augue ut lectus arcu. Congue
  nisl vitae suscipit tellus mauris a. Viverra vitae congue eu
  consequat ac felis. Odio ut sem nulla pharetra diam sit amet
  nisl suscipit. Eu augue ut lectus arcu. Odio ut sem nulla
  pharetra diam sit amet nisl suscipit.

```

7. Encrypt the file using the executable `encrypt`. Parameters: {public_key, input_file_name, output_file_name}

