COMPUTER NETWORKS LAB 11

1.

- Generate random numbers till we get 2 prime numbers a and b
- Calculate the product of these numbers and get an integer e such that it is coprime with (a-1)X(b-1) (totient function)
- e,n will be the public key
- Now calculate d for some integer k as (k X (Totient Function) + 1) /e
- D,n will be the private key
- Store 2 public private keys for A and B save it in respective files

```
parvathy@parvathy-Vostro-3590:~/Desktop/CNLabs/Lab11$ python3 q1.py
parvathy@parvathy-Vostro-3590:~/Desktop/CNLabs/Lab11$ cat A.pub
3 506557parvathy@parvathy-Vostro-3590:~/Desktop/CNLabs/Lab11$ cat A.pri
336747 506557parvathy@parvathy-Vostro-3590:~/Desktop/CNLabs/Lab11$ cat B.pub
13 417091parvathy@parvathy-Vostro-3590:~/Desktop/CNLabs/Lab11$ cat B.pri
255877 417091parvathy@parvathy-Vostro-3590:~/Desktop/CNLabs/Lab11$
```

2.

- Read the public key of B and private key of A
- Read the text in the file message.txt
- Convert each character in the text to its corresponding ASCII value
- Encrypt the value initially with the private key o A to capture its signature and then with the public key of B and append it to a string
- Encrypt the original values just with the public key of B and append it to the string
- Now open a file secret.txt in write mode and write the string into it.

```
parvathy@parvathy-Vostro-3590:~/Desktop/CNLabs/Lab11$ python3 q2.py
parvathy@parvathy-Vostro-3590:~/Desktop/CNLabs/Lab11$ cat secret.txt
394379 22007 83974 340203 449557 70651 613162 19489 429642 586417 22007 362278 235844
03 615617 362278 83974 22007 449557 601816 83974 313425 362278 615617 429642 22007 194
```

```
parvathy@parvathy-Vostro-3590:~/Desktop/CNLabs/Lab11$ python3 q3.py
Successfully Verified the Message sent by A!!
A computer is a digital electronic machine that can be programmed to carry out sequences of arithmetic or
 logical operations (computation) automatically. Modern computers can perform generic sets of operations
known as programs. These programs enable computers to perform a wide range of tasks.

parvathy@parvathy-Vostro-3590:~/Desktop/CNLabs/Lab11$
```