Assignment 6

MIS 111703060

1. Check whether given number is prime or not?

```
(base) hp@shweta:~/Subject/CNS$ gcc prime.c
(base) hp@shweta:~/Subject/CNS$ ./a.out
To quit use ctrl^c.
Enter a positive integer: 14
14 is not a prime number.
Enter a positive integer: 23
23 is a prime number.
Enter a positive integer: ^C
(base) hp@shweta:~/Subject/CNS$
```

2. Find GCD (Greatest Common Divisor) of given two numbers.

```
(base) hp@shweta:~/Subject/CNS$ gcc gcd.c
(base) hp@shweta:~/Subject/CNS$ ./a.out
To quit use ctrl^c.
Enter p: 12
Enter q: 5
GCD: 1
Enter p: 3456
Enter q: 9854
GCD: 2
Enter p: 12
Enter q: 24
GCD: 12
Enter p: 60
Enter q: 36
GCD: 12
Enter p: ^C
(base) hp@shweta:~/Subject/CNS$
```

3. Check whether given numbers are relatively prime or not?

```
(base) hp@shweta:~/Subject/CNS$ gcc relative_prime.c
(base) hp@shweta:~/Subject/CNS$ ./a.out
To quit use ctrl^c.
Enter n: 15
Enter m: 4
Relative prime numbers.
Enter n: 56
Enter m: 14
Not relative prime numbers.
Enter n: ^C
(base) hp@shweta:~/Subject/CNS$
```

4. Find multiplicative inverse of given two numbers

```
(base) hp@shweta:~/Subject/CNS$ gcc multiplicative_invers.c
(base) hp@shweta:~/Subject/CNS$ ./a.out
To quit use ctrl^c.
n*multi_inverse mod m = 1
Enter n: 56
Enter m: 17
Multiplicative inverse: 7
Enter n: 7
Enter m: 23
Multiplicative inverse: 10
Enter n: ^C
(base) hp@shweta:~/Subject/CNS$
```

5. Implement RSA algorithm

```
(base) hp@shweta:~/Subject/CNS$ gcc rsa.c
(base) hp@shweta:~/Subject/CNS$ ./a.out
To quit use ctrl^c.
Enter p: 17
Enter q: 19
Enter plaintext: fdfsd23fdkf&$jvcx

Value of e: 5
Value of d: 173

Plaintext ascii values:
102 100 102 115 100 50 51 102 100 107 102 38 36 106 118 99 120

Cipher values:
68 104 68 115 104 84 204 68 104 65 68 38 253 140 169 131 290
Time required for encryption: 3 usec

The decrypted text is: fdfsd23fdkf&$jvcx
Time required for decryption: 7 usec

Enter p: 19
Enter q: 23
Enter plaintext: Shweta05

Value of e: 5
Value of d: 317

Plaintext ascii values:
83 104 119 101 116 97 48 53

Cipher values:
429 225 104 100 70 89 193 40
Time required for encryption: 3 usec

The decrypted text is: Shweta05
Time required for decryption: 6 usec

Enter p: ^C
(base) hp@shweta:~/Subject/CNS$
```