

Instructions

1. Prime number generation -

compile using the following command -

```
g++ prime.cpp -std=c++11 -o prime
```

run using -

```
./prime
```

Algorithm 1 – Random Search for primes using Miller Rabin Test (Algorithm 4.44 from Handbook of Cryptography).

Algorithm 2 – Gordon's Strong Primes (Algorithm 4.53 from Handbook of Cryptography).

2. Multiplicative Inverse

compile using the following command -

```
g++ modinverse.cpp -std=c++11 -o modinv
```

run using -

```
./modinv
```