

Report

Steps to run:

1. Open terminal using CTRL+ALT+T
2. Execute following code -
 - a. make clean
 - b. make all
3. Now all the executables have been generated.
4. Now individual files can be run.
5. Refer Screenshots given below for generating outputs.

Algorithms:

primegen.cpp -

1. Generate a random number.
2. Check if the number is prime or not using miller rabin algorithm
3. If number is not prime then go to step 1
4. If number is prime then end the program

primecheck.cpp -

1. Handle base cases for $n < 3$
2. If n is even, return false.
3. Find an odd number d such that $n-1$ can be written as $d \cdot 2^r$.
4. Do following k times

if (millerTest(n , d) == false)

return false

return true.

millerTest(int n , int d)

1. Pick a random number ' a ' in range $[2, n-2]$
2. Compute: $x = \text{pow}(a, d) \% n$
3. If $x == 1$ or $x == n-1$, return true.
4. Do the following while d doesn't become $n-1$.
 - a. $x = (x \cdot x) \% n$.

- b. If $(x == 1)$ return false.
- c. If $(x == n-1)$ return true.

keygen.cpp -

1. Select p & q both primes $p \neq q$
2. Calculate $n = p \times q$
3. Calculate $\phi(n) = (p-1) \times (q-1)$
4. Select integer e such that $\gcd(e, \phi(n)) = 1$; $1 < e < \phi(n)$
5. Calculate $d = e^{-1} \bmod \phi(n)$
6. Public key: e & n
7. Private key: d & n

encrypt.cpp -

$$C = M^e \pmod{n}$$

decrypt.cpp -

$$M = C^d \pmod{n}$$

Key Generation

First Number	Second Number	n	e	d
1019	1021	1040399	7	890023
1093	1097	1199021	5	478733
433	499	216067	5	172109
1061	1063	1127843	7	964903
1217	1201	1461617	7	1250743
313	337	105481	5	41933
419	463	193997	5	154493
1006960115	809435257	8150690194737 74555	5	1630138035314 75837

34358689823	34347153401	1180123190007 958538023	3	7867487932928 35129867
1097498331127	1097364209663	1204355388743 641827080201	5	4817421554965 78785815765

Encrypt

n	e	m	c
1040399	7	99	579196
1199021	5	70	871579
216067	5	89	23901
1127843	7	98	871444
1461617	7	113	1411436
105481	5	105	36549
193997	5	85	147738
81506901947377455 5	5	578964	31243948873725587 4
11801231900079585 38023	3	5984566	21433741207390023 3496
12043553887436418 27080201	5	795423947	10581253758396089 71402122

Decrypt

n	d	c	m
1040399	890023	16560	104
1199021	478733	901767	71
216067	172109	169487	101
1127843	964903	539710	119
1461617	1250743	93069	83
105481	41933	78579	76
193997	154493	1583	122

Output Screenshots:

```
dell@vostro-15: ~/RSA
dell@vostro-15:~/RSA$ make clean
rm -f primegen primecheck keygen encrypt decrypt
dell@vostro-15:~/RSA$ make all
g++ primegen.cpp -o primegen -lgmp
g++ primecheck.cpp -o primecheck -lgmp
g++ keygen.cpp -o keygen -lgmp
g++ encrypt.cpp -o encrypt -lgmp
g++ decrypt.cpp -o decrypt -lgmp
dell@vostro-15:~/RSA$ ./primecheck 32401

True

dell@vostro-15:~/RSA$ ./primecheck 3244568

False

dell@vostro-15:~/RSA$ ./primegen 1024

179769313486231590772930519078902473361269403363094992027077741373242912122686
426480213466314885735810789651293295647026501918688973399964696532506117682048
919271898947719142490109972468576569628738561792917396602907960560228258529681
464902617859798196741174082349679520656385362373371754875201643570500993087
```

```
dell@vostro-15: ~/RSA
dell@vostro-15:~/RSA$ ./primecheck 1797693134862315907729305190789024733612694
033630949920270777413732429121226864264802134663148857358107896512932956470265
019186889733999646965325061176820489192718989477191424901099724685765696287385
617929173966029079605602282585296814649026178597981967411740823496795206563853
62373371754875201643570500993087

True

dell@vostro-15:~/RSA$ ./keygen 127 131

Public Key: (16637,11)
Private Key: (16637,14891)

dell@vostro-15:~/RSA$ ./keygen 1019 1021

Public Key: (1040399,7)
Private Key: (1040399,890023)

dell@vostro-15:~/RSA$ ./keygen 1093 1097

Public Key: (1199021,5)
Private Key: (1199021,478733)
```

```
dell@vostro-15: ~/RSA
dell@vostro-15:~/RSA$ ./keygen 433 499
Public Key: (216067,5)
Private Key: (216067,172109)

dell@vostro-15:~/RSA$ ./keygen 1061 1063
Public Key: (1127843,7)
Private Key: (1127843,964903)

dell@vostro-15:~/RSA$ ./keygen 1217 1201
Public Key: (1461617,7)
Private Key: (1461617,1250743)

dell@vostro-15:~/RSA$ ./keygen 313 337
Public Key: (105481,5)
Private Key: (105481,41933)

dell@vostro-15:~/RSA$ ./keygen 419 463
Public Key: (193997,5)
Private Key: (193997,154493)
```

```
dell@vostro-15: ~/RSA
dell@vostro-15:~/RSA$ ./keygen 1006960115 809435257
Public Key: (815069019473774555,5)
Private Key: (815069019473774555,163013803531475837)

dell@vostro-15:~/RSA$ ./keygen 34358689823 34347153401
Public Key: (1180123190007958538023,3)
Private Key: (1180123190007958538023,786748793292835129867)

dell@vostro-15:~/RSA$ ./keygen 1097498331127 1097364209663
Public Key: (1204355388743641827080201,5)
Private Key: (1204355388743641827080201,481742155496578785815765)
```

```
dell@vostro-15: ~/RSA
dell@vostro-15:~/RSA$ ./encrypt 16637 11 20
12046
dell@vostro-15:~/RSA$ ./encrypt 1040399 7 99
579196
dell@vostro-15:~/RSA$ ./encrypt 1199021 5 70
871579
dell@vostro-15:~/RSA$ ./encrypt 216067 5 89
23901
dell@vostro-15:~/RSA$ ./encrypt 1127843 7 98
871444
```

```
dell@vostro-15: ~/RSA
871444
dell@vostro-15:~/RSA$ ./encrypt 1461617 7 113
1411436
dell@vostro-15:~/RSA$ ./encrypt 105481 5 105
36549
dell@vostro-15:~/RSA$ ./encrypt 193997 5 85
147738
dell@vostro-15:~/RSA$ ./encrypt 815069019473774555 5 578964
312439488737255874
```

```
dell@vostro-15: ~/RSA
dell@vostro-15:~/RSA$ ./encrypt 1180123190007958538023 3 5984566
214337412073900233496
dell@vostro-15:~/RSA$ ./encrypt 1204355388743641827080201 5 795423947
1058125375839608971402122
```

```
dell@vostro-15: ~/RSA
dell@vostro-15:~/RSA$ ./decrypt 1040399 890023 16560
104
dell@vostro-15:~/RSA$ ./decrypt 1199021 478733 901767
71
dell@vostro-15:~/RSA$ ./decrypt 216067 172109 169487
101
dell@vostro-15:~/RSA$ ./decrypt 1127843 964903 539710
119
dell@vostro-15:~/RSA$ ./decrypt 1461617 1250743 93069
83
dell@vostro-15:~/RSA$ ./decrypt 105481 41933 78579
76
dell@vostro-15:~/RSA$ ./decrypt 193997 154493 1583
122
dell@vostro-15:~/RSA$ |
```