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*2r.
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 = 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*x) % n.

b. If (x == 1) return false.

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

keygen.cpp -

1. Select p & q both primes p q
2. Calculate n = p×q
3. Calculate φ(n) = (p-1)×(q-1)
4. Select integer e such that gcd(e, φ(n)) = 1; 1 < e < φ(n)
5. Calculate d = e -1 mod φ(n)
6. Public key: e & n
7. Private key: d & n

encrypt.cpp -

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

decrypt.cpp -

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

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	815069019473774555	5	163013803531475837

34358689823	34347153401	1180123190007958538023	3	786748793292835129867
1097498331127	1097364209663	1204355388743641827080201	5	481742155496578785815765

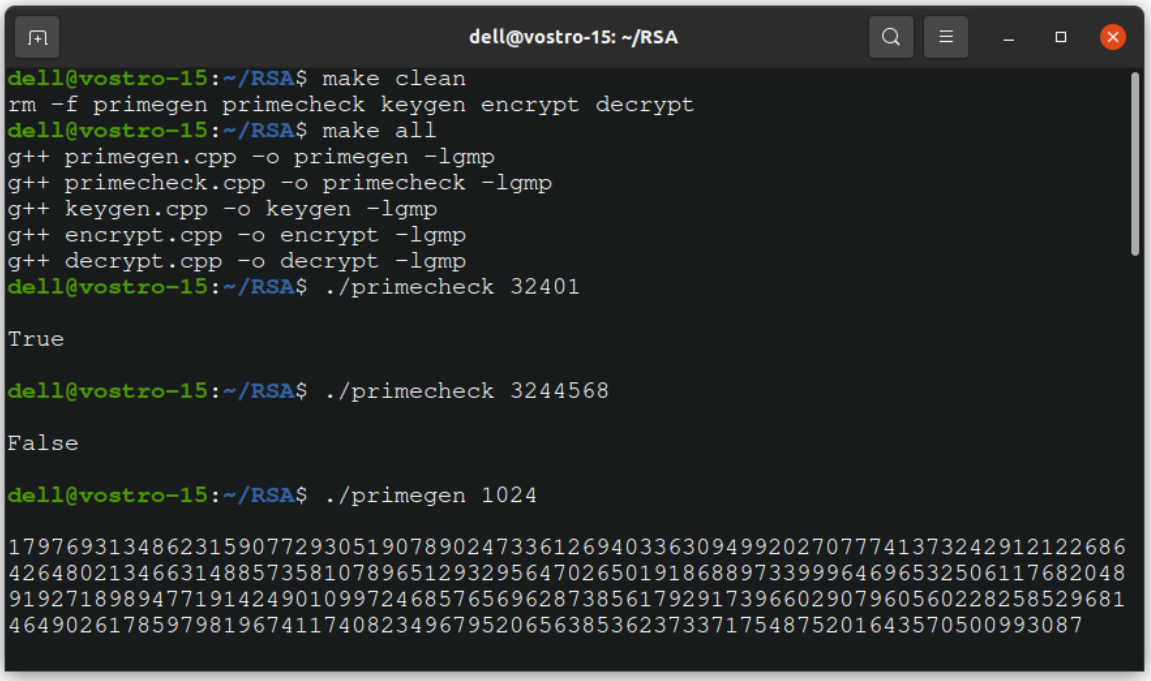
Encrypt

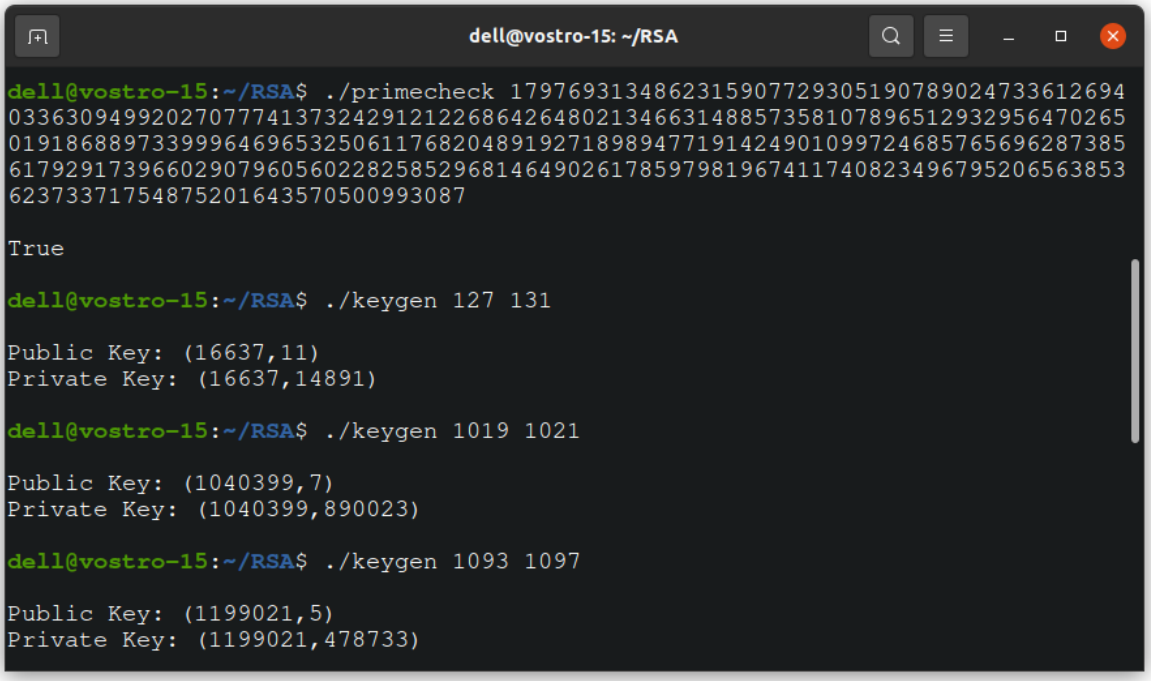
n	e	m	c
1040399	7	99	579196
1199021	5	70	871579
216067	5	89	23901
1127843	7	98	871444
1461617	7	113	1411436
105481	5	105	36549
193997	5	85	147738
815069019473774555	5	578964	312439488737255874
118012319000795853802 3	3	5984566	214337412073900233496
120435538874364182708 0201	5	795423947	105812537583960897140 2122

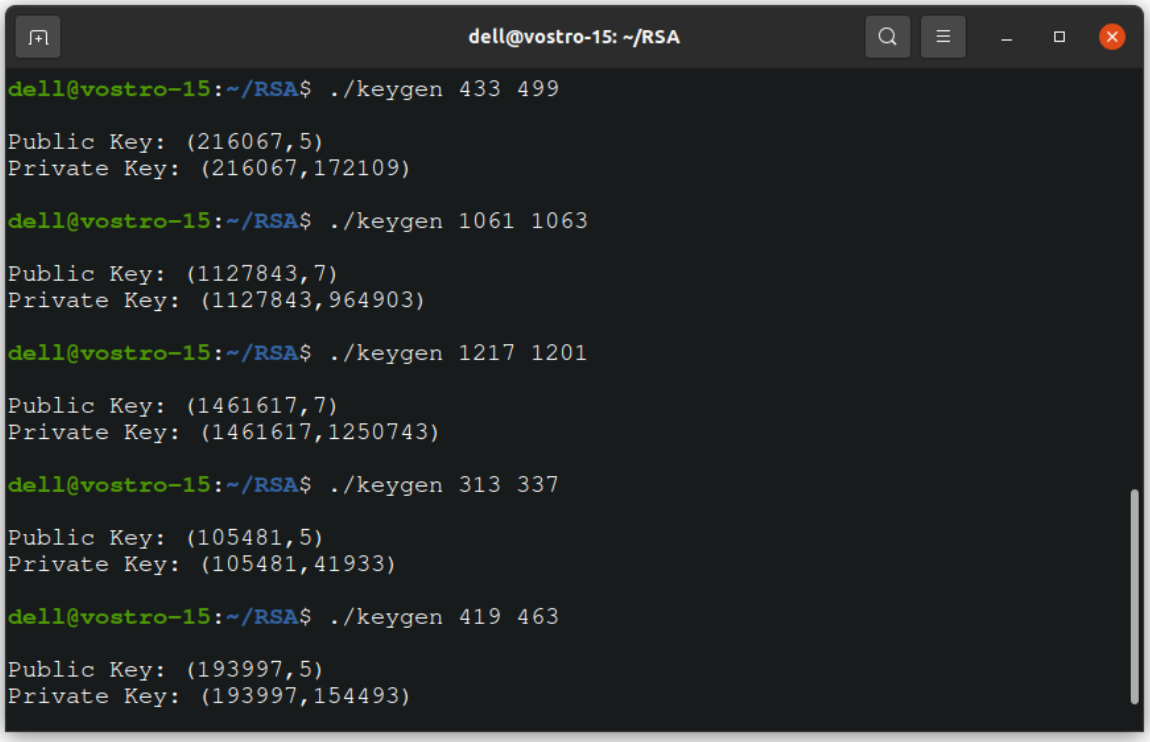
Decrypt

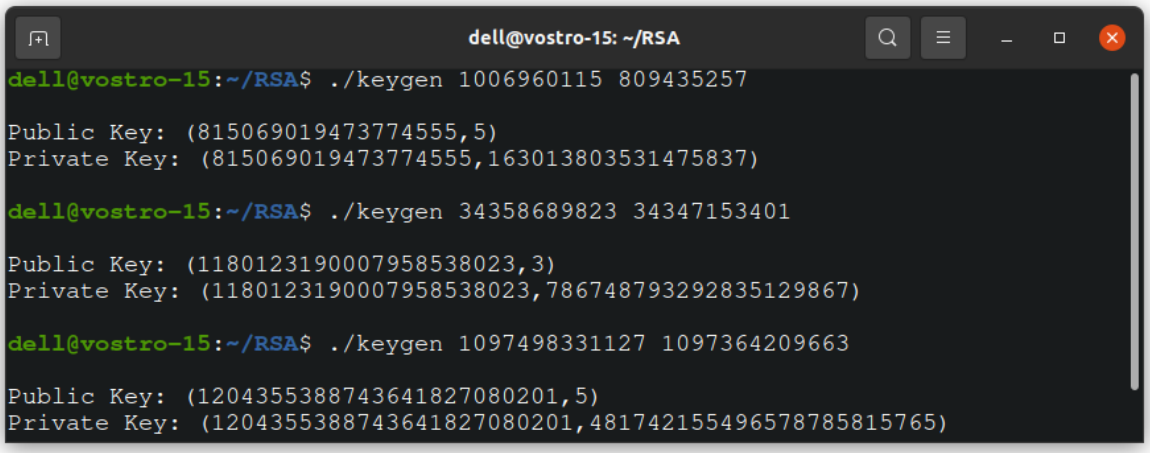
n	d	c	m
1040399	890023	16560	104
1199021	478733	901767	71
216067	172109	169487	101
1127843	964903	539710	119
1461617	1250743	93069	83
105481	41933	78579	76
193997	154493	1583	122

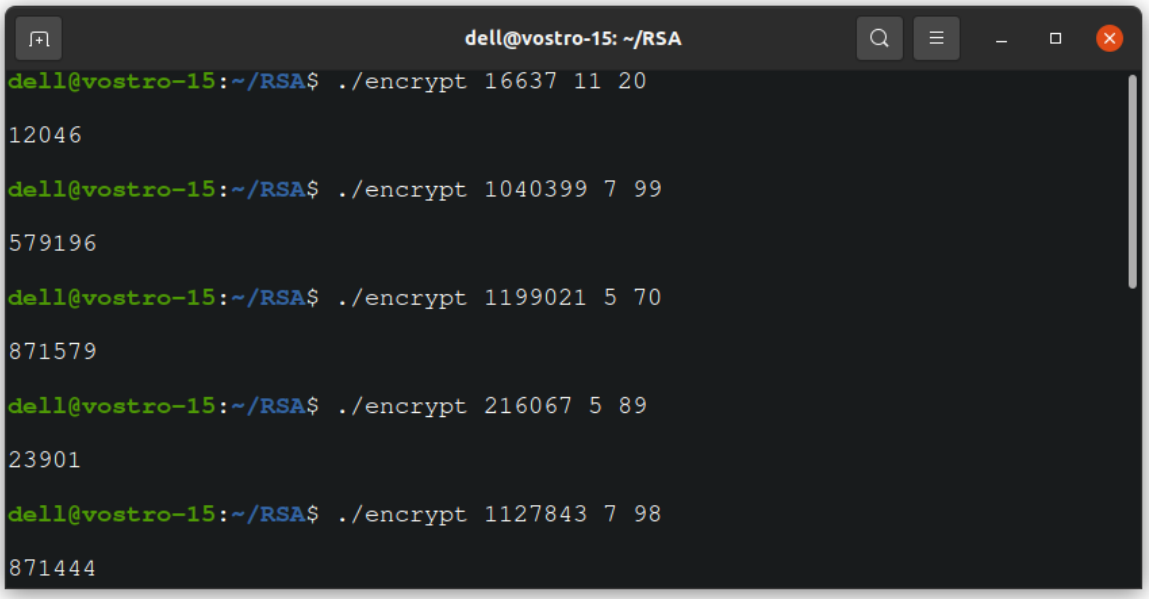
Output Screenshots:

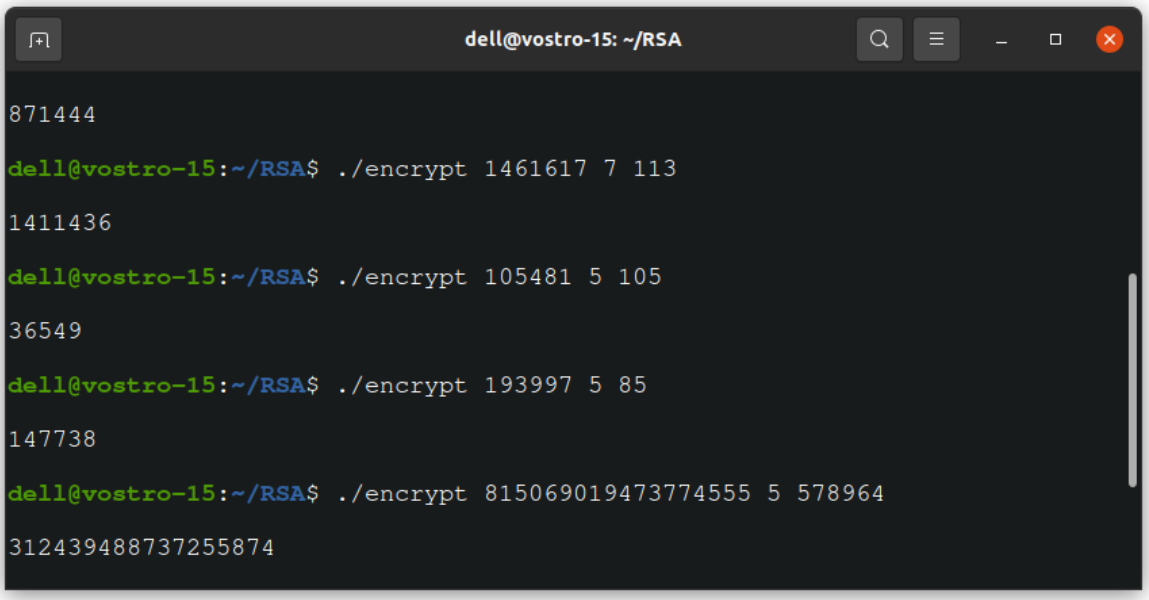


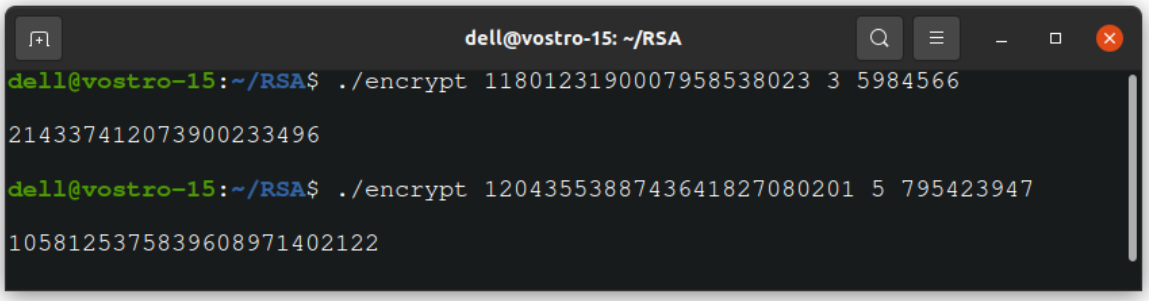


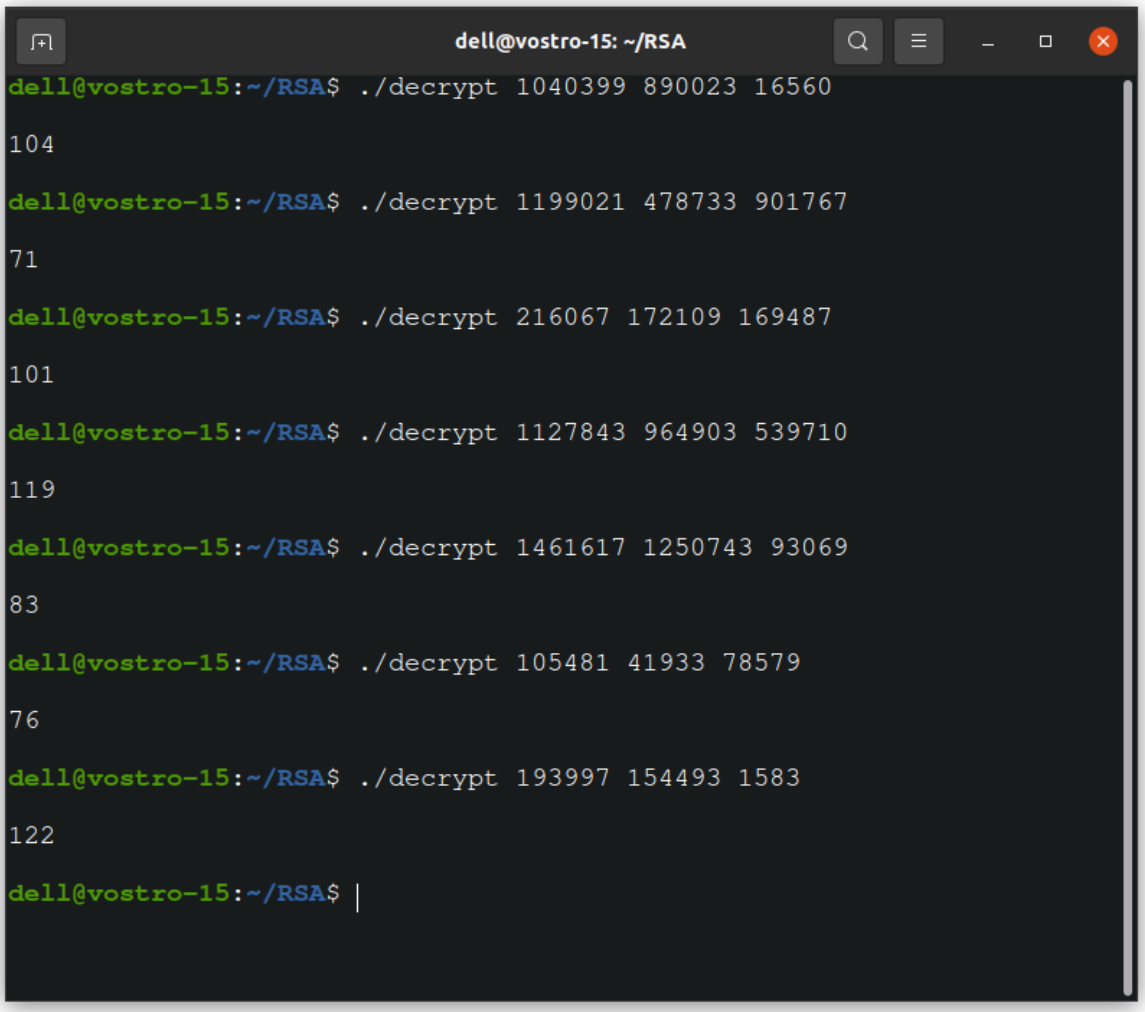

dell@vostro-15: ~/RSA
dell@vostro-15:~/RSA$ ./keygen 433 499
Public Key: (216067,5)
Private Key: (216067,172109)
dell@vostro-15:~/RSA$ ./keygen 1061 1063
Public Key: (1127843,7)
Private Key: (1127843,964903)
dell@vostro-15:~/RSA$ ./keygen 1217 1201
Public Key: (1461617,7)
Private Key: (1461617,1250743)
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
21433741207390023349 6
dell@vostro-15:~/RSA$ ./encrypt 1204355388743641827080201 5 795423947
105812537583960897140212 2


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$