Test cases:

Big Test Cases

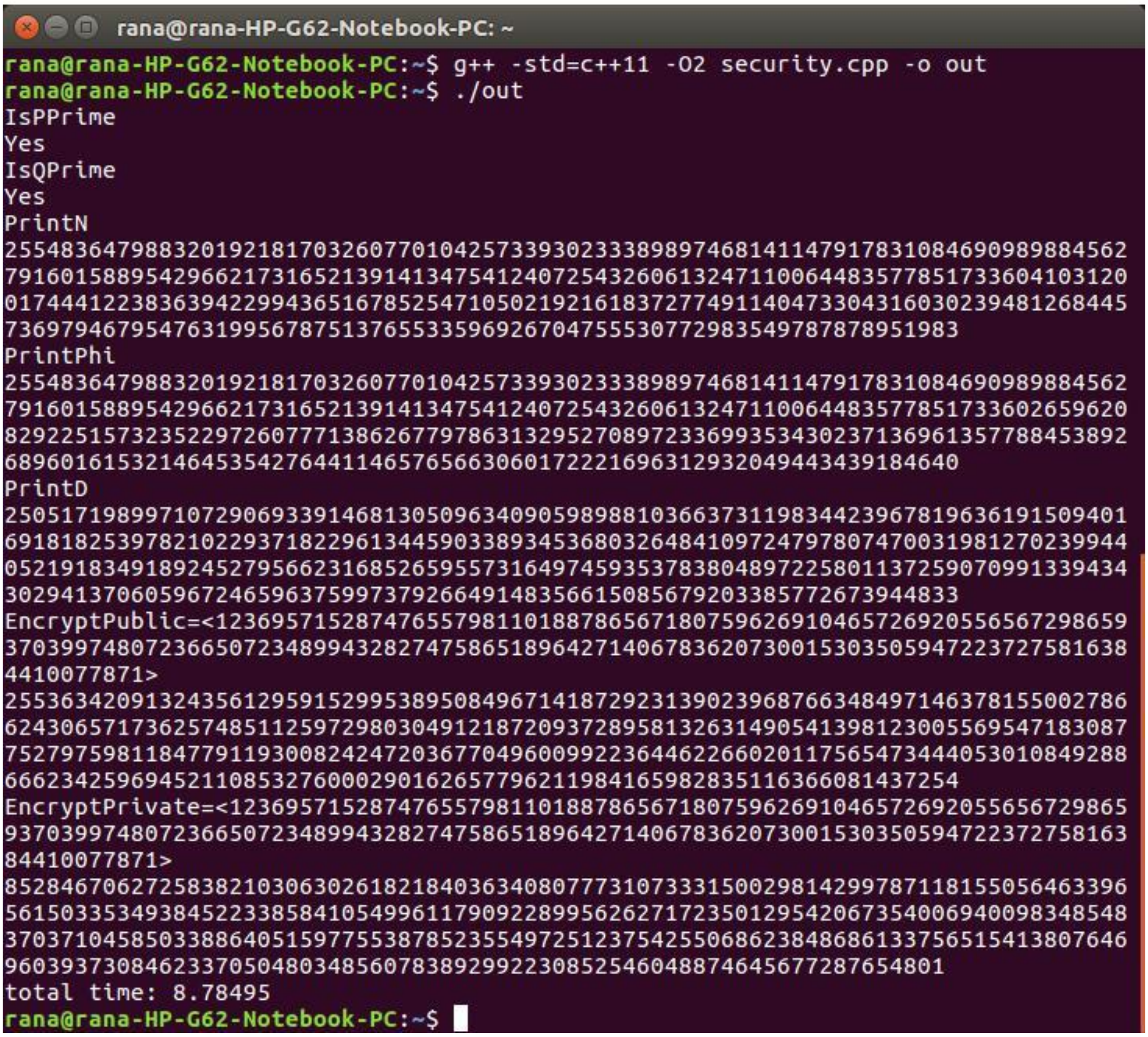
1)example1
P=123695715287476557981101887865671807596269104657269205565672986593703997480723
66507234899432827475865189642714067836207300153035059472237275816384410077871

Q=20654203534419948030543150793706350878655084239621734478118800449363181588158
02774220405304957787464676771309034463560633713497474362222775683960029689473

E=65537

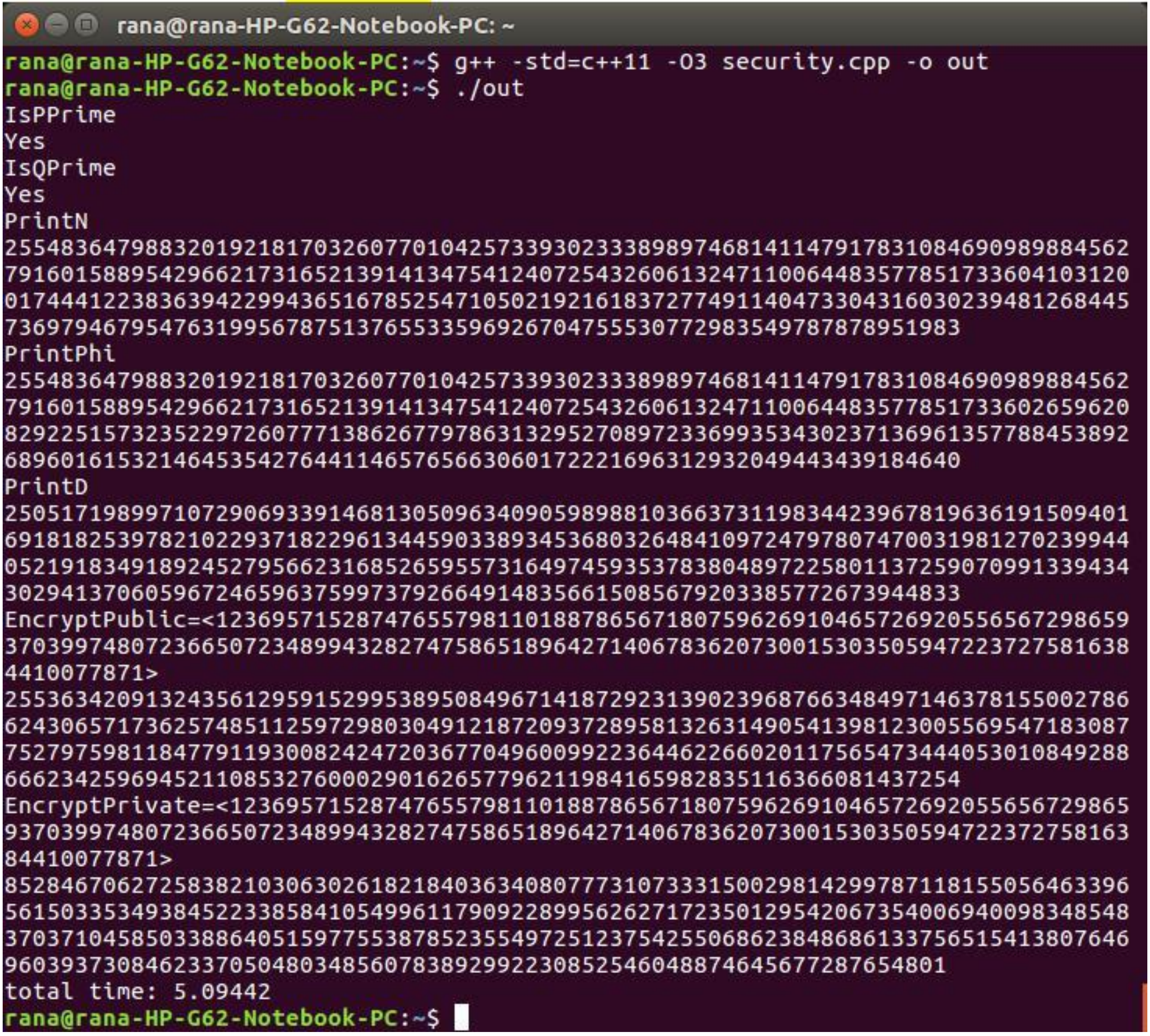
message=P=1236957152874765579811018878656718075962691046572692055656729865937039
97480723665072348994328274758651896427140678362073001530350594722372758163844100
77871

if optimization 2 is used, it takes 8.7 sec



```
rana@rana-HP-G62-Notebook-PC:~$ g++ -std=c++11 -O2 security.cpp -o out
rana@rana-HP-G62-Notebook-PC:~$ ./out
IsPPrime
Yes
IsQPrime
Yes
PrintN
25548364798832019218170326077010425733930233389897468141147917831084690989884562
79160158895429662173165213914134754124072543260613247110064483577851733604103120
01744412238363942299436516785254710502192161837277491140473304316030239481268445
73697946795476319956787513765533596926704755530772983549787878951983
PrintPhi
25548364798832019218170326077010425733930233389897468141147917831084690989884562
79160158895429662173165213914134754124072543260613247110064483577851733602659620
82922515732352297260777138626779786313295270897233699353430237136961357788453892
68960161532146453542764411465765663060172221696312932049443439184640
PrintD
25051719899710729069339146813050963409059898810366373119834423967819636191509401
69181825397821022937182296134459033893453680326484109724797807470031981270239944
05219183491892452795662316852659557316497459353783804897225801137259070991339434
30294137060596724659637599737926649148356615085679203385772673944833
EncryptPublic=<12369571528747655798110188786567180759626910465726920556567298659
37039974807236650723489943282747586518964271406783620730015303505947223727581638
4410077871>
25536342091324356129591529953895084967141872923139023968766348497146378155002786
62430657173625748511259729803049121872093728958132631490541398123005569547183087
75279759811847791193008242472036770496009922364462266020117565473444053010849288
66623425969452110853276000290162657796211984165982835116366081437254
EncryptPrivate=<1236957152874765579811018878656718075962691046572692055656729865
93703997480723665072348994328274758651896427140678362073001530350594722372758163
84410077871>
85284670627258382103063026182184036340807773107333150029814299787118155056463396
56150335349384522338584105499611790922899562627172350129542067354006940098348548
37037104585033886405159775538785235549725123754255068623848686133756515413807646
9603937308462337050480348560783892992230852546048874645677287654801
total time: 8.78495
rana@rana-HP-G62-Notebook-PC:~$ 
```

if optimization 3 is used it takes 5 sec



```
rana@rana-HP-G62-Notebook-PC:~$ g++ -std=c++11 -O3 security.cpp -o out
rana@rana-HP-G62-Notebook-PC:~$ ./out
IsPPrime
Yes
IsQPrime
Yes
PrintN
25548364798832019218170326077010425733930233389897468141147917831084690989884562
79160158895429662173165213914134754124072543260613247110064483577851733604103120
01744412238363942299436516785254710502192161837277491140473304316030239481268445
73697946795476319956787513765533596926704755530772983549787878951983
PrintPhi
25548364798832019218170326077010425733930233389897468141147917831084690989884562
79160158895429662173165213914134754124072543260613247110064483577851733602659620
82922515732352297260777138626779786313295270897233699353430237136961357788453892
68960161532146453542764411465765663060172221696312932049443439184640
PrintD
25051719899710729069339146813050963409059898810366373119834423967819636191509401
69181825397821022937182296134459033893453680326484109724797807470031981270239944
05219183491892452795662316852659557316497459353783804897225801137259070991339434
30294137060596724659637599737926649148356615085679203385772673944833
EncryptPublic=<1236957152874765579811018878656718075962691046572692055567298659
37039974807236650723489943282747586518964271406783620730015303505947223727581638
4410077871>
25536342091324356129591529953895084967141872923139023968766348497146378155002786
62430657173625748511259729803049121872093728958132631490541398123005569547183087
75279759811847791193008242472036770496009922364462266020117565473444053010849288
66623425969452110853276000290162657796211984165982835116366081437254
EncryptPrivate=<1236957152874765579811018878656718075962691046572692055656729865
93703997480723665072348994328274758651896427140678362073001530350594722372758163
84410077871>
85284670627258382103063026182184036340807773107333150029814299787118155056463396
56150335349384522338584105499611790922899562627172350129542067354006940098348548
37037104585033886405159775538785235549725123754255068623848686133756515413807646
9603937308462337050480348560783892992230852546048874645677287654801
total time: 5.09442
rana@rana-HP-G62-Notebook-PC:~$ 
```

2)example2

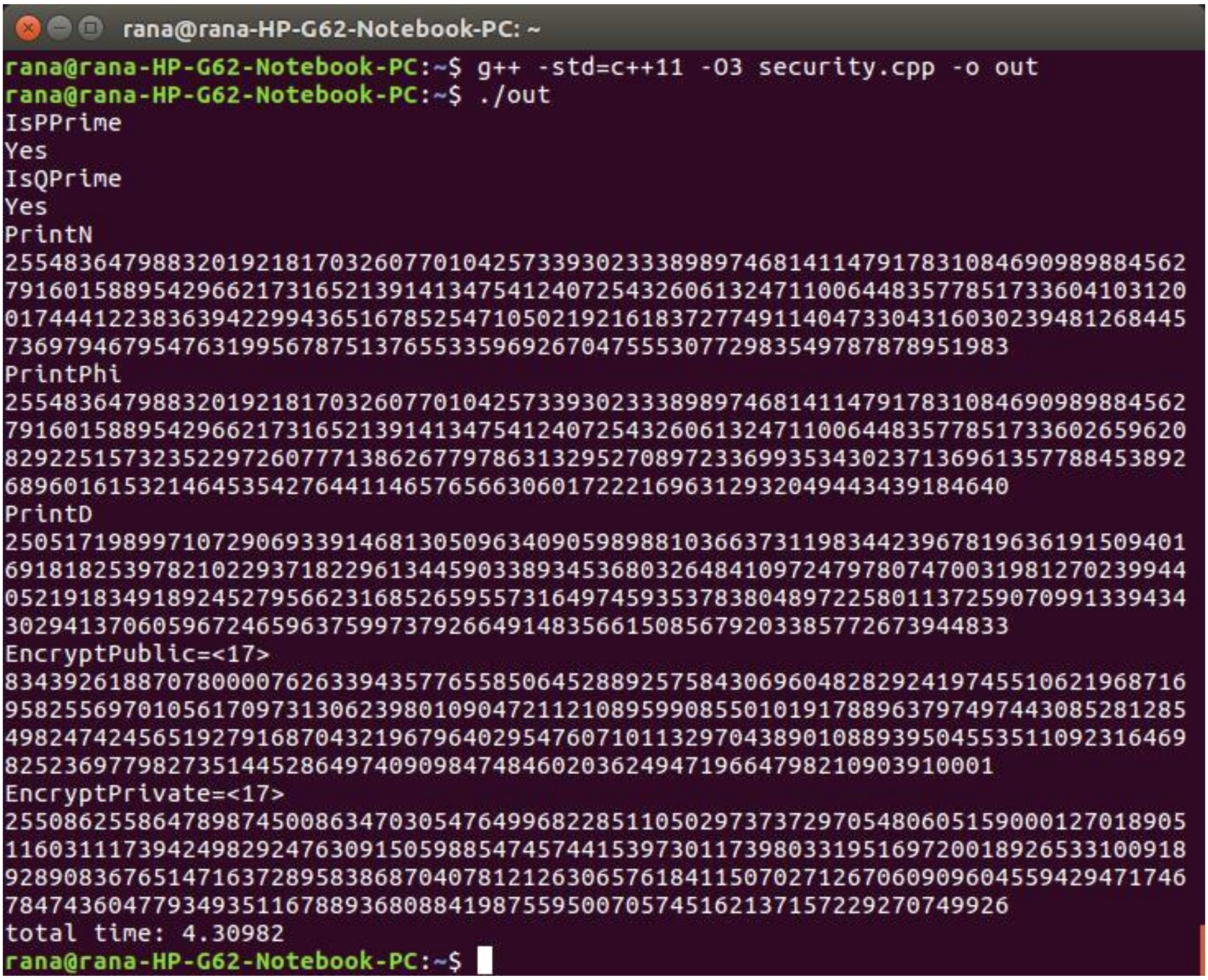
P=1236957152874765579811018878656718075962691046572692055567298659370399748072366507234899432827475865189642714067836207300153035059472237275816384410077871

Q=2065420353441994803054315079370635087865508423962173447811880044936318158815802774220405304957787464676771309034463560633713497474362222775683960029689473

E=65537

message=17

it takes 4.3 sec



```
rana@rana-HP-G62-Notebook-PC:~$ g++ -std=c++11 -O3 security.cpp -o out
rana@rana-HP-G62-Notebook-PC:~$ ./out
IsPPrime
Yes
IsQPrime
Yes
PrintN
25548364798832019218170326077010425733930233389897468141147917831084690989884562
79160158895429662173165213914134754124072543260613247110064483577851733604103120
01744412238363942299436516785254710502192161837277491140473304316030239481268445
73697946795476319956787513765533596926704755530772983549787878951983
PrintPhi
25548364798832019218170326077010425733930233389897468141147917831084690989884562
79160158895429662173165213914134754124072543260613247110064483577851733602659620
82922515732352297260777138626779786313295270897233699353430237136961357788453892
68960161532146453542764411465765663060172221696312932049443439184640
PrintD
25051719899710729069339146813050963409059898810366373119834423967819636191509401
69181825397821022937182296134459033893453680326484109724797807470031981270239944
05219183491892452795662316852659557316497459353783804897225801137259070991339434
30294137060596724659637599737926649148356615085679203385772673944833
EncryptPublic=<17>
83439261887078000076263394357765585064528892575843069604828292419745510621968716
95825569701056170973130623980109047211210895990855010191788963797497443085281285
49824742456519279168704321967964029547607101132970438901088939504553511092316469
8252369779827351445286497409098474846020362494719664798210903910001
EncryptPrivate=<17>
25508625586478987450086347030547649968228511050297373729705480605159000127018905
11603111739424982924763091505988547457441539730117398033195169720018926533100918
92890836765147163728958386870407812126306576184115070271267060909604559429471746
78474360477934935116788936808841987559500705745162137157229270749926
total time: 4.30982
rana@rana-HP-G62-Notebook-PC:~$ 
```

3)example3

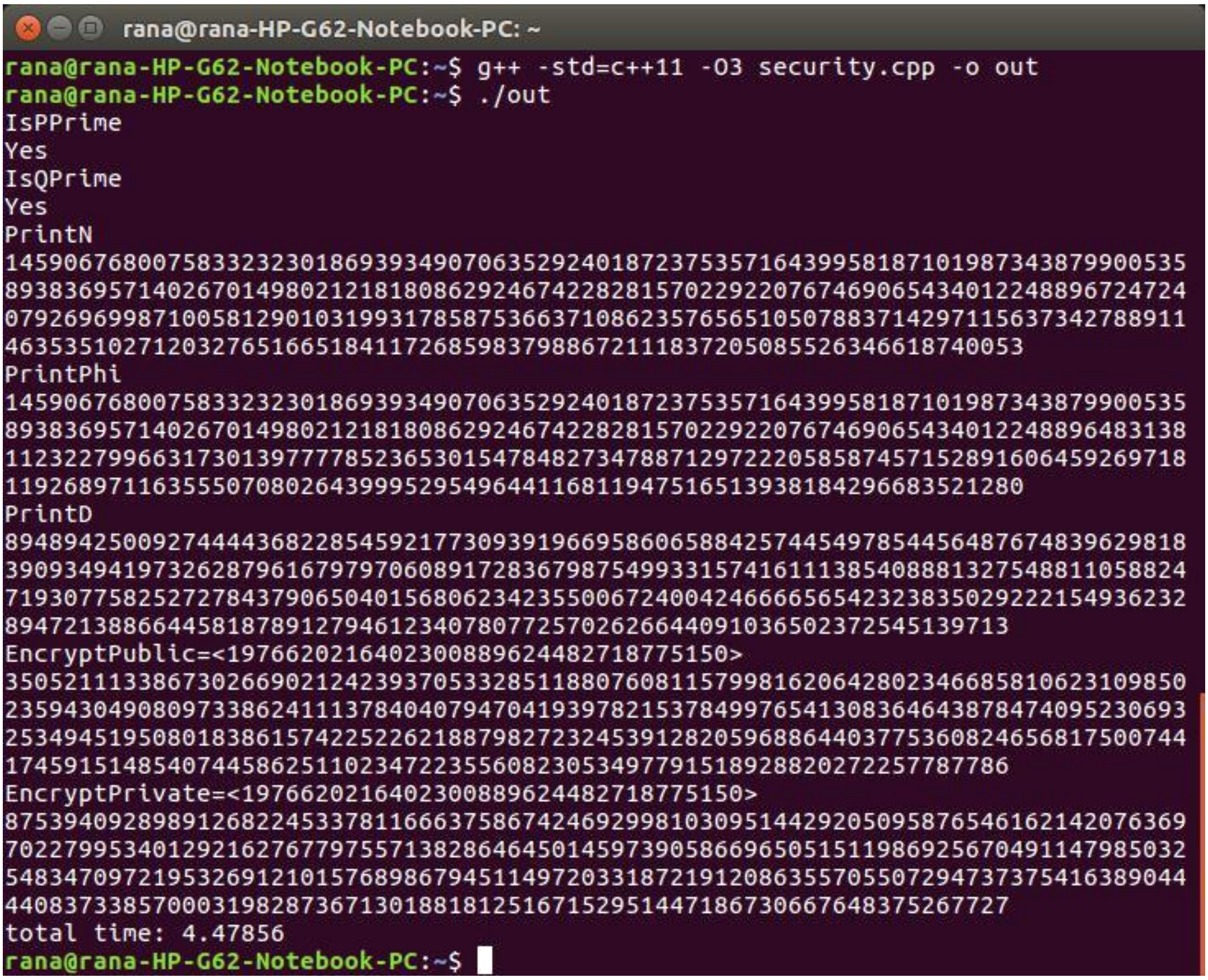
P=12131072439211271897323671531612440428472427633701410925634549312301964373042085619324197365322416866541017057361365214171711713797974299334871062829803541

Q=12027524255478748885956220793734512128733387803682075433653899983955179850988797899869146900809131611153346817050832096022160146366346391812470987105415233

E=65537

message=1976620216402300889624482718775150

it takes 4.4 sec



```
rana@rana-HP-G62-Notebook-PC:~$ g++ -std=c++11 -O3 security.cpp -o out
rana@rana-HP-G62-Notebook-PC:~$ ./out
IsPPrime
Yes
IsQPrime
Yes
PrintN
14590676800758332323018693934907063529240187237535716439958187101987343879900535
89383695714026701498021218180862924674228281570229220767469065434012248896724724
07926969987100581290103199317858753663710862357656510507883714297115637342788911
463535102712032765166518411726859837988672111837205085526346618740053
PrintPhi
14590676800758332323018693934907063529240187237535716439958187101987343879900535
89383695714026701498021218180862924674228281570229220767469065434012248896483138
11232279966317301397777852365301547848273478871297222058587457152891606459269718
119268971163555070802643999529549644116811947516513938184296683521280
PrintD
89489425009274444368228545921773093919669586065884257445497854456487674839629818
39093494197326287961679797060891728367987549933157416111385408881327548811058824
71930775825272784379065040156806234235500672400424666656542323835029222154936232
89472138866445818789127946123407807725702626644091036502372545139713
EncryptPublic=<1976620216402300889624482718775150>
35052111338673026690212423937053328511880760811579981620642802346685810623109850
23594304908097338624111378404079470419397821537849976541308364643878474095230693
25349451950801838615742252262188798272324539128205968864403775360824656817500744
17459151485407445862511023472235560823053497791518928820272257787786
EncryptPrivate=<1976620216402300889624482718775150>
87539409289891268224533781166637586742469299810309514429205095876546162142076369
70227995340129216276779755713828646450145973905866965051511986925670491147985032
54834709721953269121015768986794511497203318721912086355705507294737375416389044
44083733857000319828736713018818125167152951447186730667648375267727
total time: 4.47856
rana@rana-HP-G62-Notebook-PC:~$ █
```

4) example4

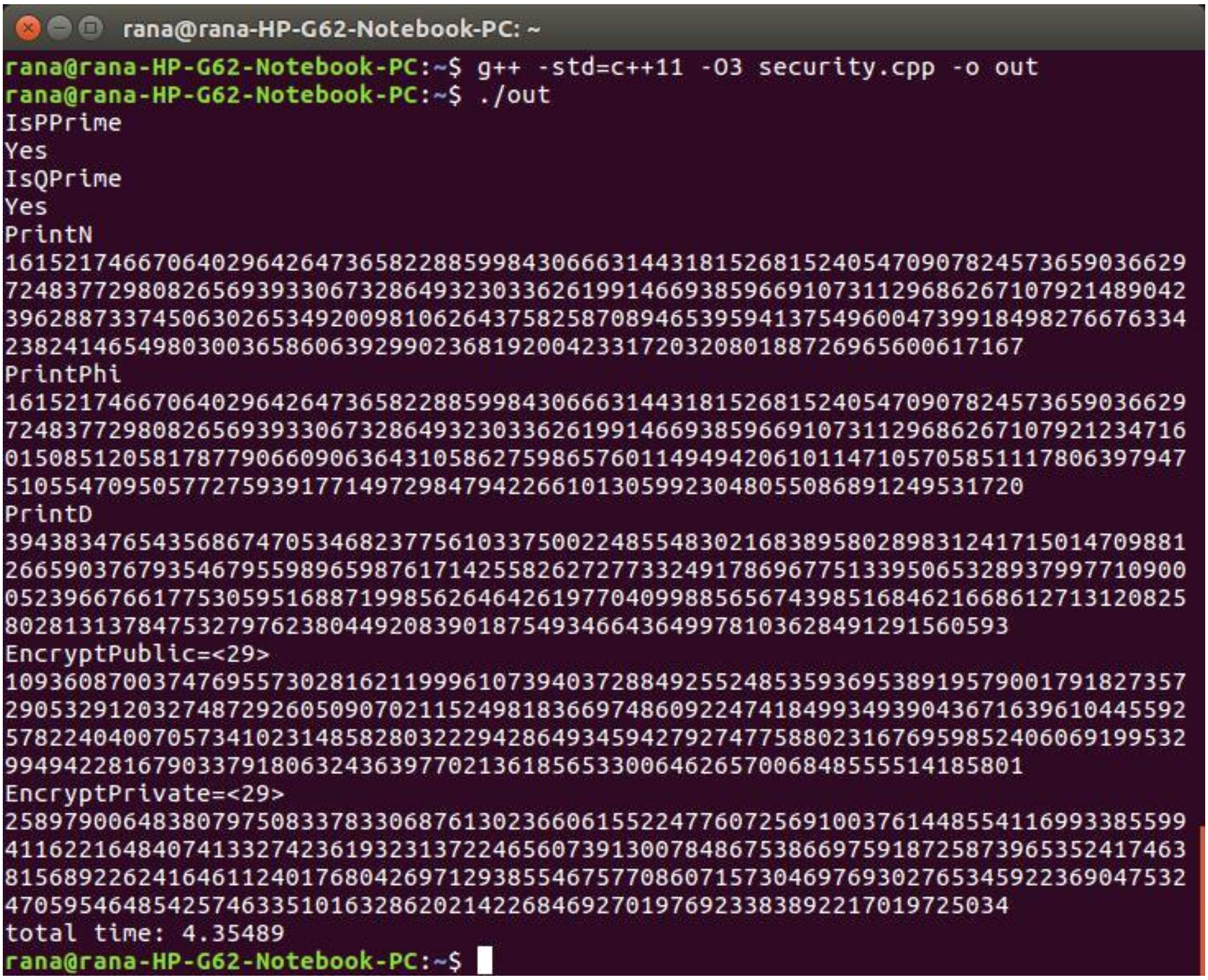
P=131441318342695122192609419937146696050066257431720060305295046455278009515236 97620149903055663251854220067020503783524785523675819158836547734770656069477

Q=122885062860918041082626454076587099628033581863163098712057697033712331158567 726582368246310927404030571272719288203639838195442929501955585905303695015971

E=65537

message=29

it takes 4.3 sec



```
rana@rana-HP-G62-Notebook-PC:~$ g++ -std=c++11 -O3 security.cpp -o out
rana@rana-HP-G62-Notebook-PC:~$ ./out
IsPPrime
Yes
IsQPrime
Yes
PrintN
161521746670640296426473658228859984306663144318152681524054709078245736590366629
724837729808265693933067328649323033626199146693859669107311296862671079214890 42
396288733745063026534920098106264375825870894653959413754960047399184982766763 34
23824146549803003658606392990236819200423317203208018872696560061 7167
PrintPhi
161521746670640296426473658228859984306663144318152681524054709078245736590366629
724837729808265693933067328649323033626199146693859669107311296862671079212347 16
015085120581787790660906364310586275986576011494942061011471057058511178063979 47
51055470950577275939177149729847942266101305992304805508689124953172 0
PrintD
394383476543568674705346823775610337500224855483021683895802898312417150147098 81
266590376793546795598965987617142558262727733249178696775133950653289379977109 00
052396676617753059516887199856264642619770409988565674398516846216686127131208 25
80281313784753279762380449208390187549346643649978103628491291560593
EncryptPublic=<29>
109360870037476955730281621199961073940372884925524853593695389195790017918273 57
290532912032748729260509070211524981836697486092247418499349390436716396104455 92
578224040070573410231485828032229428649345942792747758802316769598524060691995 32
99494228167903379180632436397702136185653300646265700684855551418580 1
EncryptPrivate=<29>
258979006483807975083378330687613023660615522477607256910037614485541169933855 99
411622164840741332742361932313722465607391300784867538669759187258739653524174 63
815689226241646112401768042697129385546757708607157304697693027653459223690475 32
47059546485425746335101632862021422684692701976923383892217019725034
total time: 4.35489
rana@rana-HP-G62-Notebook-PC:~$
```

Small Test Cases

5) example5

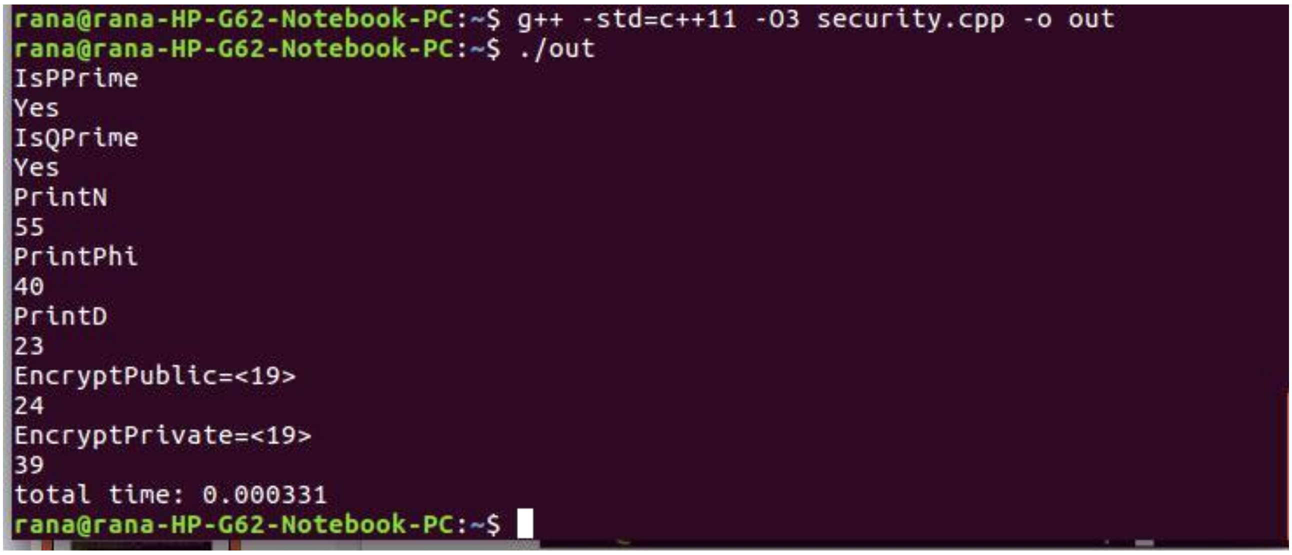
p=5

Q=11

E=7

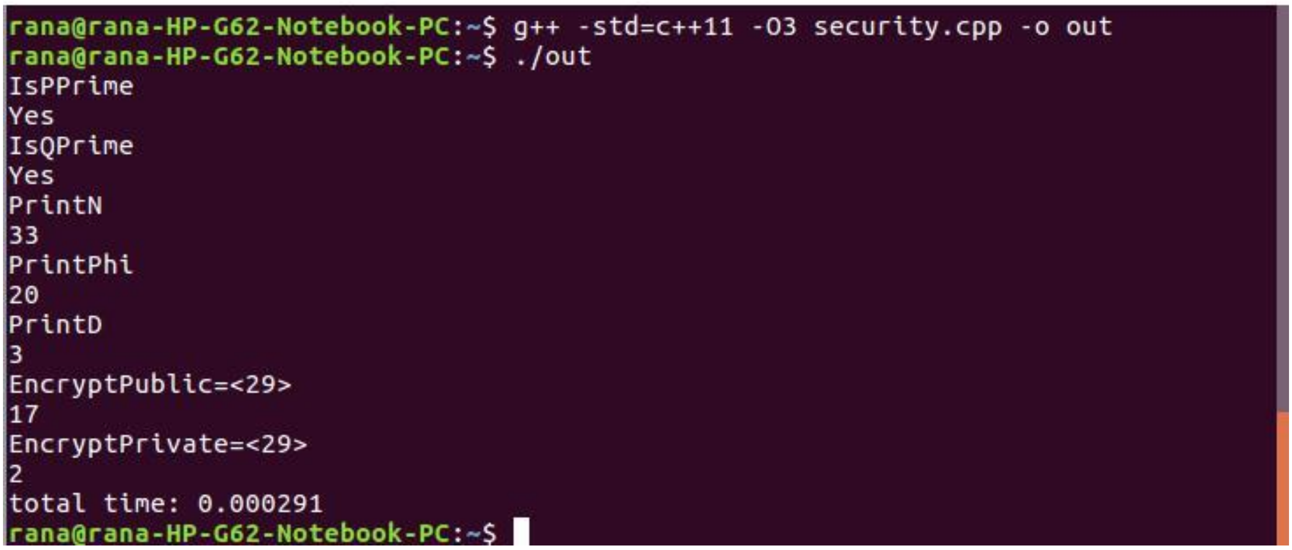
message=19

it takes around 0 sec



```
rana@rana-HP-G62-Notebook-PC:~$ g++ -std=c++11 -O3 security.cpp -o out
rana@rana-HP-G62-Notebook-PC:~$ ./out
IsPPrime
Yes
IsQPrime
Yes
PrintN
55
PrintPhi
40
PrintD
23
EncryptPublic=<19>
24
EncryptPrivate=<19>
39
total time: 0.000331
rana@rana-HP-G62-Notebook-PC:~$ 
```

6) example3
P=3
Q=11
E=7
message=29
it takes around 0 sec



```
rana@rana-HP-G62-Notebook-PC:~$ g++ -std=c++11 -O3 security.cpp -o out
rana@rana-HP-G62-Notebook-PC:~$ ./out
IsPPrime
Yes
IsQPrime
Yes
PrintN
33
PrintPhi
20
PrintD
3
EncryptPublic=<29>
17
EncryptPrivate=<29>
2
total time: 0.000291
rana@rana-HP-G62-Notebook-PC:~$ 
```

Notes

the data structure used in this code is vector of data type long long , every 9 digits are put in one element of the vector.

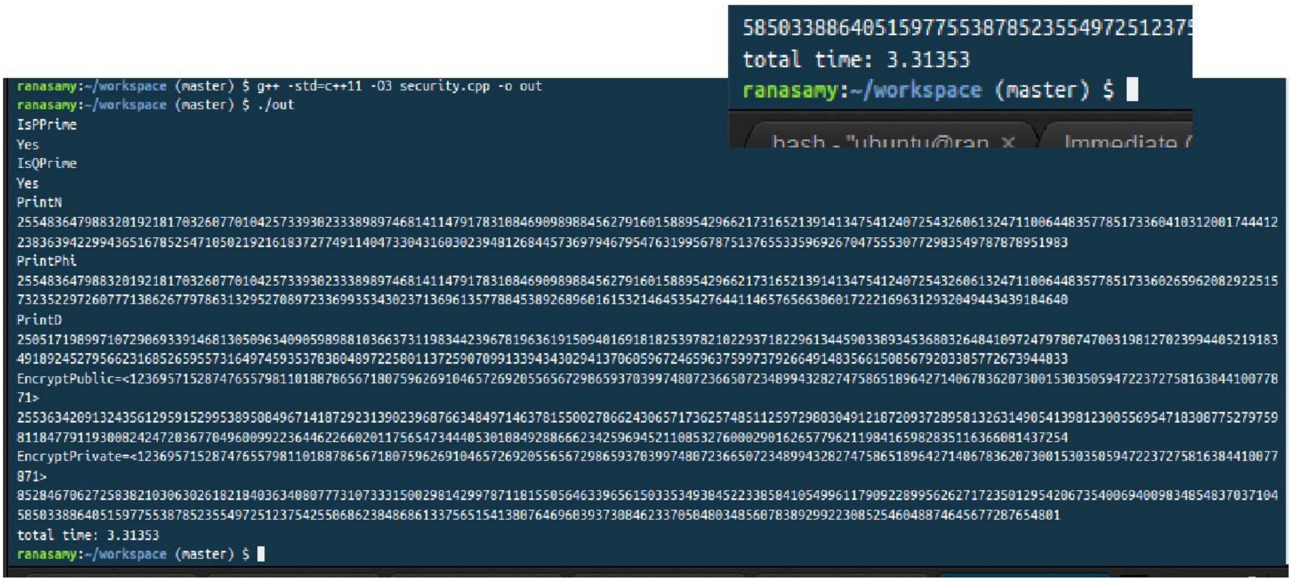
Division algorithm is Double Division , the Power function is recursive.

Some quick things I made to optimize the code:

using of add function instead of multiplication in double division, long division by 2 in the power function of O(log n) , add function isn’t used in multiplication function.

Encrypt Private is the function that takes most of the time , Except this functions all other Functions together run in approximately 1 sec.

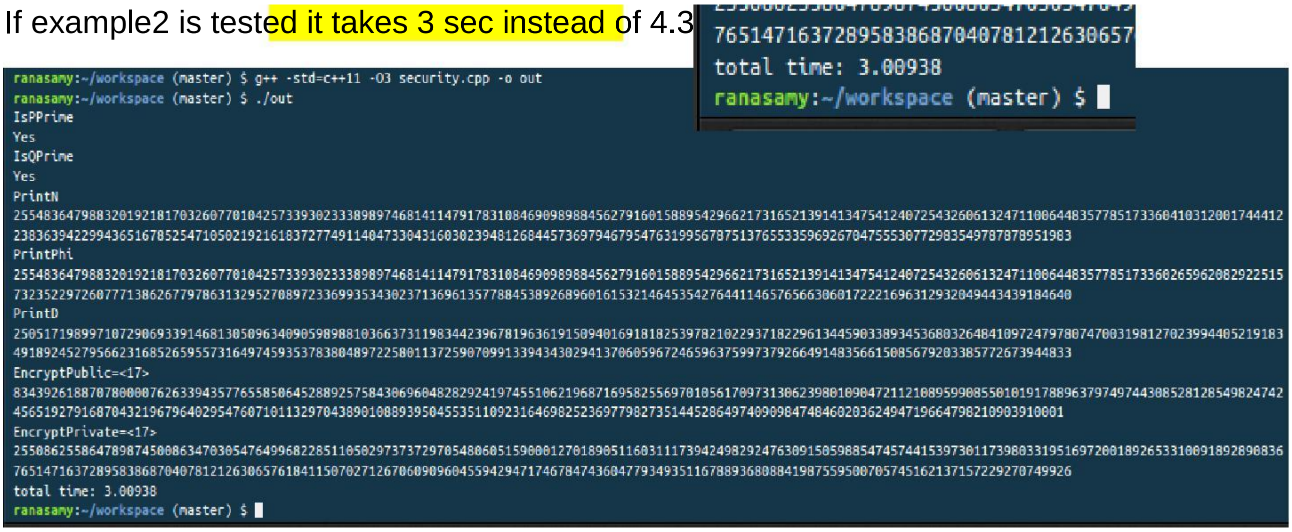
All test cases are run on my personal laptop , which slow down the runtime , when example 1 is tested on cloud 9 server , it takes 3.3 sec instead of 5sec.



```
5850338864051597755387852355497251237
total time: 3.31353
ranasamy:~/workspace (master) $ 
```

```
ranasamy:~/workspace (master) $ g++ -std=c++11 -O3 security.cpp -o out
ranasamy:~/workspace (master) $ ./out
IsPPrime
Yes
IsQPrime
Yes
PrintN
255483647988320192181703260770104257339302333898974681411479178310846909898845627916015889542966217316521391413475412407254326061324711006448357785173360410312001744412
2383639422994365167852547105021921618372774911404733043160302394812684457369794679547631995678751376553359692670475553077298354978787895198 3
PrintPhi
255483647988320192181703260770104257339302333898974681411479178310846909898845627916015889542966217316521391413475412407254326061324711006448357785173360265962082922515
7323522972607771386267797863132952708972336993534302371369613577884538926896016153214645354276441146576566306017222169631293204944343918464 0
PrintD
250517198997107290693391468130509634090598988103663731198344239678196361915094016918182539782102293718229613445903389345368032648410972479780747003198127023994405219183
4918924527956623168526595573164974593537838048972258011372590709913394343029413706059672465963759973792664914835661508567920338577267394483 3
EncryptPublic=<123695715287476557981101887865671807596269104657269205565672986593703997480723665072348994328274758651896427140678362073001530350594722372758163844100778
71>
255363420913243561295915299538950849671418729231390239687663484971463781550027866243065717362574851125972980304912187209372895813263149054139812300556954718308775279759
8118477911930082424720367704960099223644622660201175654734440530108492886662342596945211085327600029016265779621198416598283511636608 1437254
EncryptPrivate=<123695715287476557981101887865671807596269104657269205565672986593703997480723665072348994328274758651896427140678362073001530350594722372758163844100777
871>
852846706272583821030630261821840363408077731073331500298142997871181550564633965615033353493845223385841054996117909228995626271723501295420673540069400983485483703710 4
585033886405159775538785235549725123754255068623848686133756515413807646960393730846233705048034856078389299223085254604887464567728765480 1
total time: 3.31353
ranasamy:~/workspace (master) $ 
```

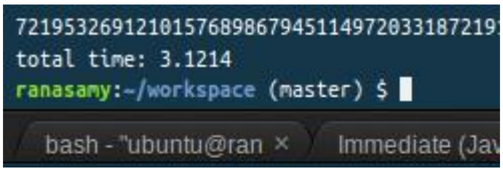
If example2 is tested it takes 3 sec instead of 4.3



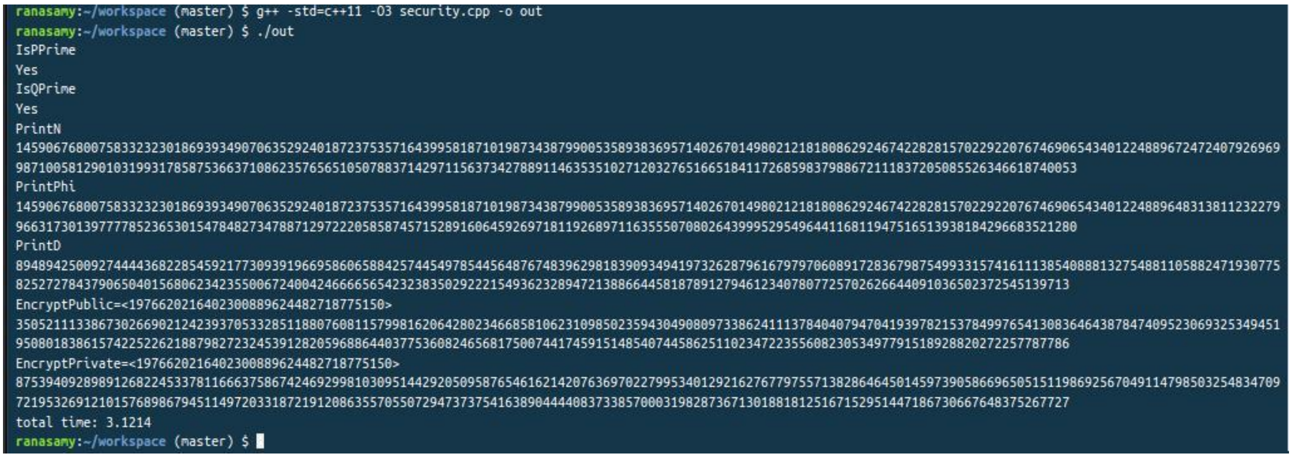
```
76514716372895838687040781212630657
total time: 3.00938
ranasamy:~/workspace (master) $ 
```

```
ranasamy:~/workspace (master) $ g++ -std=c++11 -O3 security.cpp -o out
ranasamy:~/workspace (master) $ ./out
IsPPrime
Yes
IsQPrime
Yes
PrintN
255483647988320192181703260770104257339302333898974681411479178310846909898845627916015889542966217316521391413475412407254326061324711006448357785173360410312001744412
2383639422994365167852547105021921618372774911404733043160302394812684457369794679547631995678751376553359692670475553077298354978787895198 3
PrintPhi
255483647988320192181703260770104257339302333898974681411479178310846909898845627916015889542966217316521391413475412407254326061324711006448357785173360265962082922515
7323522972607771386267797863132952708972336993534302371369613577884538926896016153214645354276441146576566306017222169631293204944343918464 0
PrintD
250517198997107290693391468130509634090598988103663731198344239678196361915094016918182539782102293718229613445903389345368032648410972479780747003198127023994405219183
4918924527956623168526595573164974593537838048972258011372590709913394343029413706059672465963759973792664914835661508567920338577267394483 3
EncryptPublic=<17>
834392618870780000762633943577655850645288925758430696048282924197455106219687169582556970105617097313062398010904721121089599085501019178896379749744308528128549824742
45651927916870432196796402954760710113297043890108893950455351109231646982523697798273514452864974090984748460203624947196647982109039100 01
EncryptPrivate=<17>
255086255864789874500863470305476499682285110502973737297054806051590001270189051160311173942498292476309150598854745744153973011739803319516972001892653310091892890836
7651471637289583868704078121263065761841150702712670609096045594294717467847436047793493511678893680884198755950070574516213715722927074992 6
total time: 3.00938
ranasamy:~/workspace (master) $ 
```

when example 3 is tested it takes 3.1 sec instead of 4.4



```
7219532691210157689867945114972033187219
total time: 3.1214
ranasamy:~/workspace (master) $ 
```



```
ranasamy:~/workspace (master) $ g++ -std=c++11 -O3 security.cpp -o out
ranasamy:~/workspace (master) $ ./out
IsPPrime
Yes
IsQPrime
Yes
PrintN
145906768007583323230186939349070635292401872375357164399581871019873438799005358938369571402670149802121818086292467422828157022922076746906543401224889672472407926969
987100581290103199317858753663710862357656510507883714297115637342788911463535102712032765166518411726859837988672111837205085526346618740053
PrintPhi
145906768007583323230186939349070635292401872375357164399581871019873438799005358938369571402670149802121818086292467422828157022922076746906543401224889648313811232279
9663173013977778523653015478482734788712972220585874571528916064592697181119268971163555070802643999529549644116811947516513938184296683521280
PrintD
894894250092744443682285459217730939196695860658842574454978544564876748396298183909349419732628796167979706089172836798754993315741611138540888132754881105882471930775
82527278437906504015680623423550067240042466665654232383502922215493623289472138866445818789127946123407807725702626644091036502372545139713
EncryptPublic=<1976620216402300889624482718775150>
350521113386730266902124239370533285118807608115799816206428023466858106231098502359430490809733862411137840407947041939782153784997654130836464387847409523069325349451
95080183861574225226218879827232453912820596886440377536082465681750074417459151485407445862511023472235560823053497791518928820272257787786
EncryptPrivate=<1976620216402300889624482718775150>
875394092898912682245337811666375867424692998103095144292050958765461621420763697022799534012921627677975571382864645014597390586696505151198692567049114798503254834709
72195326912101576898679451149720331872191208635570550729473737541638904444083733857000319828736713018818125167152951447186730667648375267727
total time: 3.1214
ranasamy:~/workspace (master) $ 
```