CS4062D Introduction to Information Security Assignment 2

By Dev Sony, B180297CS

Github Repo

Compile

To compile a .cpp file from the source directory, use the make command as follows and pass the filename without the extension. The output file will be stored in the `build/` folder.

```
// make file=<filename>
make file=RSA
```

Running the Code

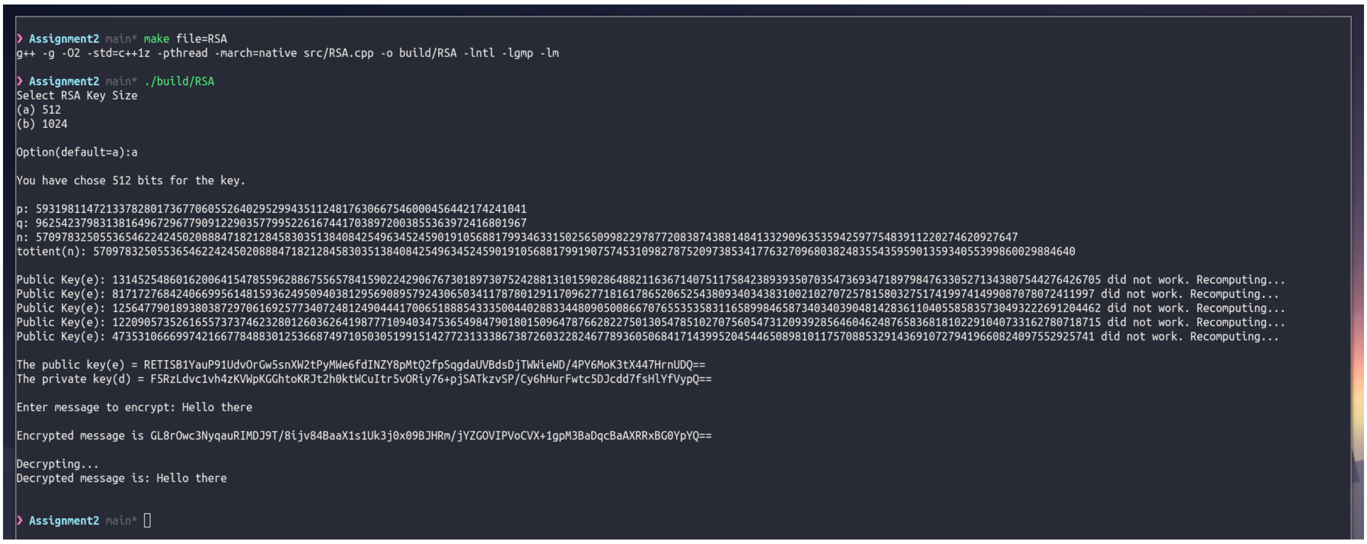
To run the code, simply run the output file as per the example given below.

```
// ./build/<filename>
./build/RSA
```

Output Screenshots

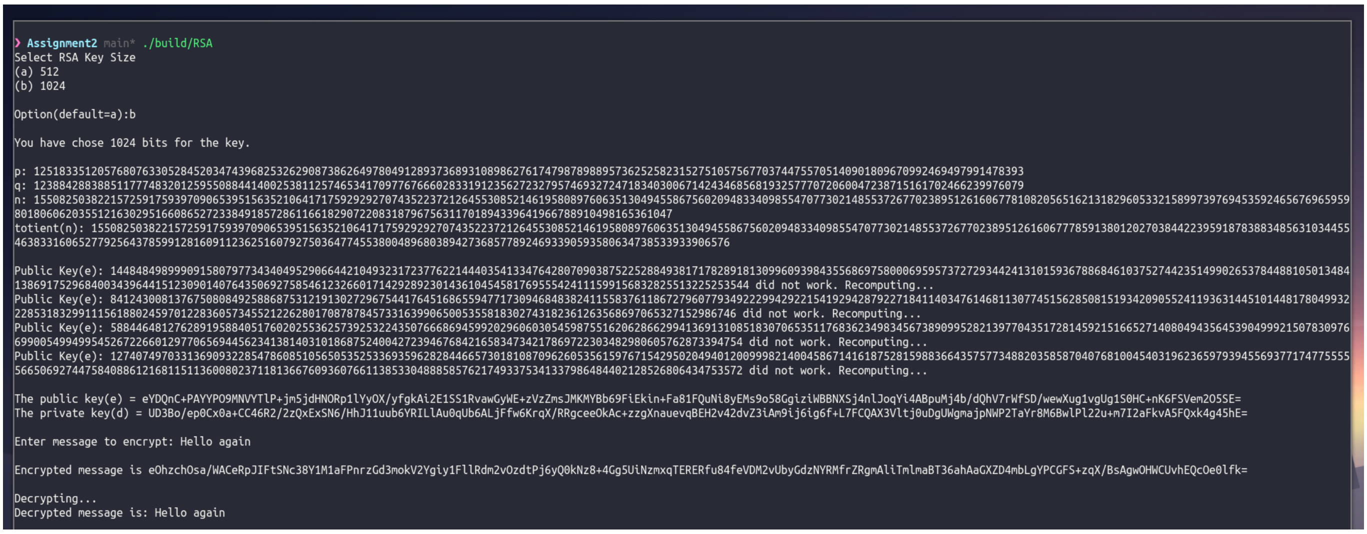
RSA

512 BITS



```
❯ Assignment2 main* make file=RSA
g++ -g -O2 -std=c++1z -pthread -march=native src/RSA.cpp -o build/RSA -lntl -lgmp -lm

❯ Assignment2 main* ./build/RSA
Select RSA Key Size
(a) 512
(b) 1024

Option(default=a):a

You have chose 512 bits for the key.

p: 59319811472133782801736770605526402952994351124817630667546000456442174241041
q: 96254237983138164967296779091229035779952261674417038972003855363972416801967
n: 5709783250553654622424502088847182128458303513840842549634524590191056881799346331502565099822978772083874388148413329096353594259775483911220274620927647
totient(n): 57097832505536546224245020888471821284583035138408425496345245901910568817991907574531098278752097385341776327096803824835543595901359340553998600029884640

Public Key(e): 13145254860162006415478559628867556578415902242906767301897307524288131015902864882116367140751175842389393507035473693471897984763305271343807544276426705 did not work. Recomputing...
Public Key(e): 8171727684240669956148159362495094038129569089579243065034117878012911709627718161786520652543809340343831002102707257815803275174199741499087078072411997 did not work. Recomputing...
Public Key(e): 12564779018938038729706169257734072481249044417006518885433350044028833448090500866707655353583116589984658734034039048142836110405585835730493222691204462 did not work. Recomputing...
Public Key(e): 12209057352616557373746232801260362641987771094034753654984790180150964787662822750130547851027075605473120939285646046248765836818102291040733162780718715 did not work. Recomputing...
Public Key(e): 4735310666997421667784883012536687497105030519915142772313338673872603228246778936050684171439952045446508981011757088532914369107279419660824097552925741 did not work. Recomputing...

The public key(e) = RETISB1YauP91UdvOrGw5snXW2tPyMWe6fdINZY8pMtQ2fpSqgdaUVBdsDjTWWieWD/4PY6MoK3tX447HrnUDQ==
The private key(d) = F5RzLdvc1vh4zKVWpKGGhtoKRJt2h0ktWCuItr5vORiy76+pjSATkzvSP/Cy6hHurFwtc5DJcdd7fsHlYfVypQ==

Enter message to encrypt: Hello there

Encrypted message is GL8rOwc3NyqauRIMDJ9T/8ijv84BaaX1s1Uk3j0x09BJHRm/jYZGOVIPVoCVX+1gpM3BaDqcBaAXRRxBG0YpYQ==

Decrypting...
Decrypted message is: Hello there

❯ Assignment2 main* 
```

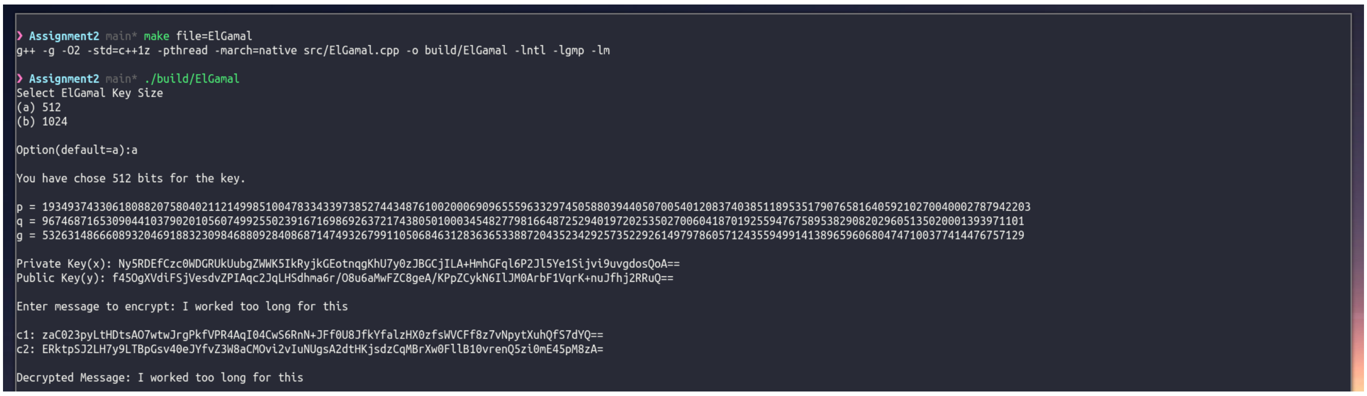
1024 BITS



```
❯ Assignment2 main* ./build/RSA
Select RSA Key Size
(a) 512
(b) 1024

Option(default=a):b

You have chose 1024 bits for the key.

p: 12518335120576807633052845203474396825326290873862649780491289373689310898627617479878988957362525823152751057567703744755705140901809670992469497991478393
q: 12388428838851177748320125955088441400253811257465341709776766602833191235627232795746932724718340300671424346856819325777072060047238715161702466239976079
n: 15508250382215725917593970906539515635210641717592929270743522372126455308521461958089760635130494558675602094833409855470773021485537267702389512616067781082056516213182960533215899739769453592465676965959
80180606203551216302951660865272338491857286116618290722083187967563117018943396419667889104981653610 47
totient(n): 15508250382215725917593970906539515635210641717592929270743522372126455308521461958089760635130494558675602094833409855470773021485537267702389512616067778591380120270384422395918783883485631034455
4638331606527792564378599128160911236251607927503647745538004896803894273685778924693390593580634738533933906576

Public Key(e): 14484849899909158079773434049529066442104932317237762214440354133476428070903875225288493817178289181309960939843556869758000695957372729344241310159367886846103752744235149902653784488105013484
138691752968400343964415123090140764350692758546123266017142928923014361045458176955542411159915683282551322525 3544 did not work. Recomputing...
Public Key(e): 84124300813767508084925886875312191302729675441764516865594771730946848382411558376118672796077934922299429221541929428792271841140347614681130774515628508151934209055241193631445101448178049932
228531832991115618802459701228360573455212262801708787845733163990650053558183027431823612635686970653271529867 46 did not work. Recomputing...
Public Key(e): 58844648127628919588405176020255362573925322435076668694599202960603054598755162062866299413691310851830706535117683623498345673890995282139770435172814592151665271408049435645390499921507830976
6990054994995452672266012977065694456234138140310186875240004272394676842165834734217869722303482980605762873394754 did not work. Recomputing...
Public Key(e): 12740749703313690932285478608510565053525336935962828446657301810870962605356159767154295020494012009998214004586714161875281598836643575773488203585870407681004540319623659793945569377174775555
56650692744758408861216811511360080237118136676093607661138533048885857621749337534133798648440212852680643475357 2 did not work. Recomputing...

The public key(e) = eYDQnC+PAYYPO9MNVYTlP+jm5jdHNORp1lYyOX/yfgkAi2E1SS1RvawGyWE+zVzZmsJMKMYBb69FiEkin+Fa81FQuNi8yEMs9o58GgiziWBBNXSj4nlJoqYi4ABpuMj4b/dQhV7rWfSD/wewXug1vgUg1S0HC+nK6FSVem2O5SE=
The private key(d) = UD3Bo/ep0Cx0a+CC46R2/2zQxExSN6/HhJ11uub6YRILlAu0qUb6ALjFfw6KrqX/RRgceeOkAc+zzgXnauevqBEH2v42dvZ3iAm9ij6ig6f+L7FCQAX3Vltj0uDgUWgmajpNWP2TaYr8M6BwlPl22u+m7I2aFkvA5FQxk4g45hE=

Enter message to encrypt: Hello again

Encrypted message is eOhzchOsa/WACeRpJIFtSNc38Y1M1aFPnrzGd3mokV2Ygiy1FllRdm2vOzdtPj6yQ0kNz8+4Gg5UiNzmxqTERERfu84feVDM2vUbyGdzNYRMfrZRgmAliTmlmaBT36ahAaGXZD4mbLgYPCGFS+zqX/BsAgwOHWCUvhEQcOe0lfk=

Decrypting...
Decrypted message is: Hello again
```

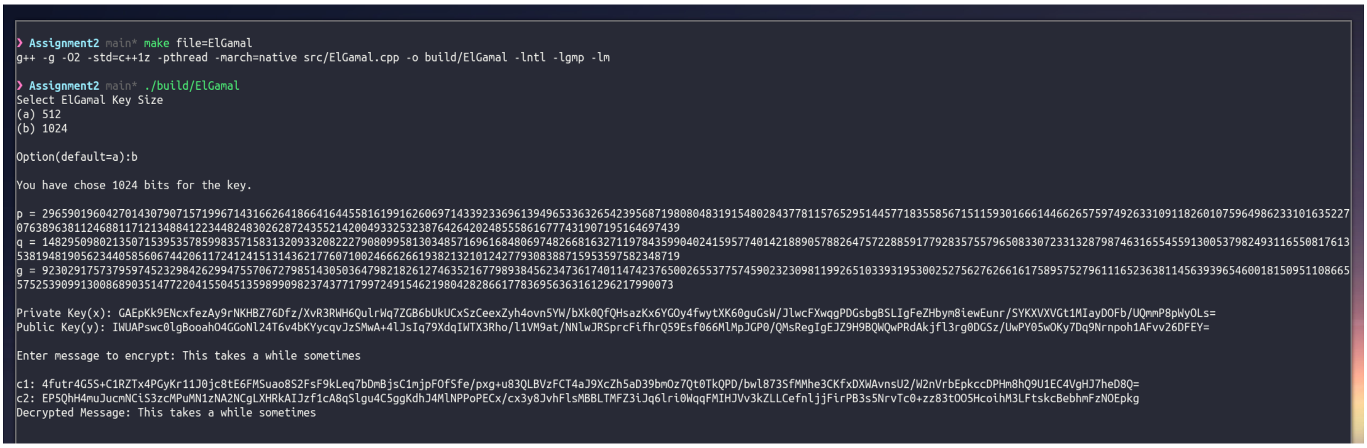
El Gamal

512 BITS



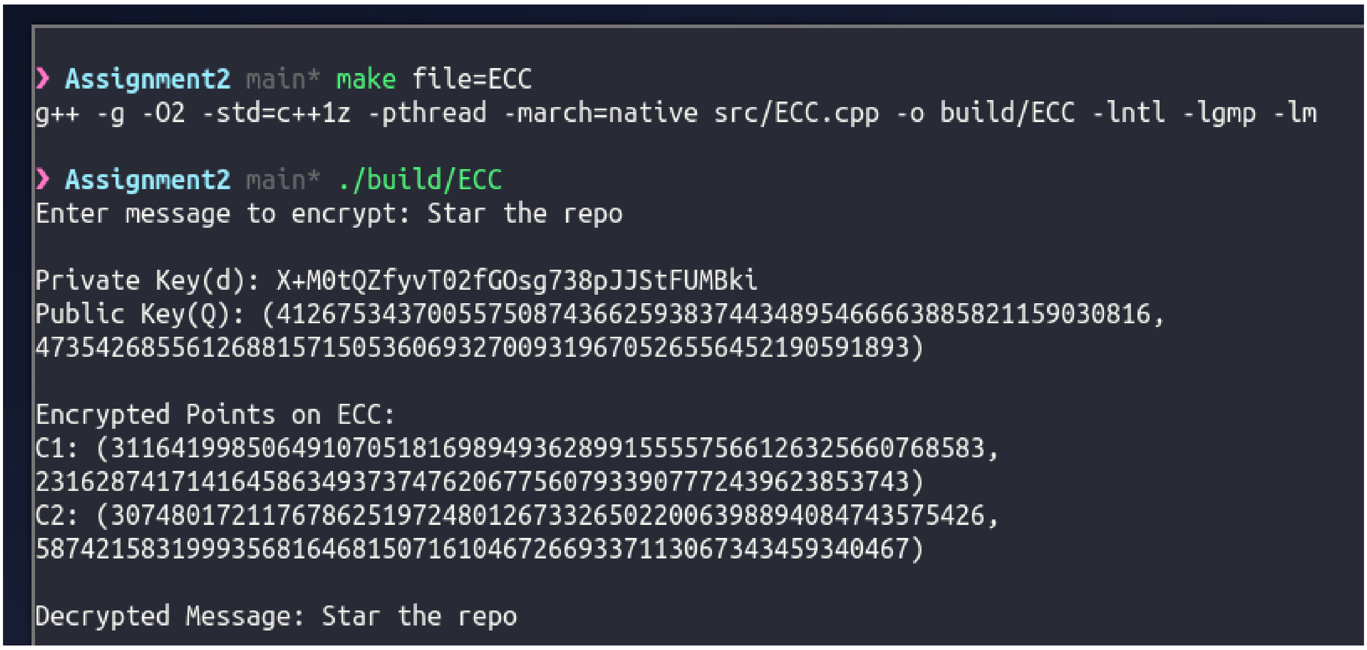
```
❯ Assignment2 main* make file=ElGamal
g++ -g -O2 -std=c++1z -pthread -march=native src/ElGamal.cpp -o build/ElGamal -lntl -lgmp -lm

❯ Assignment2 main* ./build/ElGamal
Select ElGamal Key Size
(a) 512
(b) 1024

Option(default=a):a

You have chose 512 bits for the key.

p = 19349374330618088207580402112149985100478334339738527443487610020006909655596332974505880394405070054012083740385118953517907658164059210270040002787942203
q = 9674687165309044103790201056074992550239167169869263721743805010003454827798166487252940197202535027006041870192559476758953829082029605135020001393971101
g = 5326314866608932046918832309846880928408687147493267991105068463128363653388720435234292573522926149797860571243559499141389659606804747100377414476757129

Private Key(x): Ny5RDEfCzc0WDGRUkUubgZWWK5IkRyjkGEotnqgKhU7y0zJBGCjILA+HmhGFql6P2Jl5Ye1Sijvi9uvgdosQoA==
Public Key(y): f45OgXVdiFSjVesdvZPIAqc2JqLHSdhma6r/O8u6aMwFZC8geA/KPpZCykN6IlJM0ArbF1VqrK+nuJfhj2RRuQ==

Enter message to encrypt: I worked too long for this

c1: zaC023pyLtHDtsAO7wtwJrgPkfVPR4AqI04CwS6RnN+JFf0U8JfkYfalzHX0zfsWVCFf8z7vNpytXuhQfS7dYQ==
c2: ERktpSJ2LH7y9LTBpGsv40eJYfvZ3W8aCMOvi2vIuNUgsA2dtHKjsdzCqMBrXw0FllB10vrenQ5zi0mE45pM8zA=

Decrypted Message: I worked too long for this
```

1024 BITS



```
❯ Assignment2 main* make file=ElGamal
g++ -g -O2 -std=c++1z -pthread -march=native src/ElGamal.cpp -o build/ElGamal -lntl -lgmp -lm

❯ Assignment2 main* ./build/ElGamal
Select ElGamal Key Size
(a) 512
(b) 1024

Option(default=a):b

You have chose 1024 bits for the key.

p = 2965901960427014307907157199671431662641866416445581619916260697143392336961394965336326542395687198080483191548028437781157652951445771835585671511593016661446626575974926331091182601075964986233101635227
07638963811246881171213488412234482483026287243552142004933253238764264202485558616777431907195164697439
q = 1482950980213507153953578599835715831320933208222790809958130348571696168480697482668163271197843599040241595774014218890578826475722885917792835755796508330723313287987463165545591300537982493116550817613
53819481905623440585606744206117241241513143621776071002466626619382132101242779308388715953597582348719
g = 9230291757379597452329842629947557067279851430503647982182612746352167798938456234736174011474237650026553775745902323098119926510339319530025275627626616175895752796111652363811456393965460018150951108665
5752539099130086890351477220415504513598990982374377179972491546219804282866177836956363161296217990073

Private Key(x): GAEpKk9ENcxfezAy9rNKHBZ76Dfz/XvR3RWH6QulrWq7ZGB6bUkUCxSzCeexZyh4ovn5YW/bXk0QfQHsazKx6YGOy4fwytXK60guGsW/JlwcFXwqgPDGsbgBSLIgFeZHbym8iewEunr/SYKXVXVGt1MIayDOFb/UQmmP8pWyOLs=
Public Key(y): IWUAPswc0lgBooahO4GGoNl24T6v4bKYycqvJzSMwA+4lJsIq79XdqIWTX3Rho/l1VM9at/NNlwJRSprcFifhrQ59Esf066MlMpJGP0/QMsRegIgEJZ9H9BQWQwPRdAkjfl3rg0DGSz/UwPY05wOKy7Dq9Nrnpoh1AFvv26DFEY=

Enter message to encrypt: This takes a while sometimes

c1: 4futr4G5S+C1RZTx4PGyKr11J0jc8tE6FMSuao8S2FsF9kLeq7bDmBjsC1mjpFOfSfe/pxg+u83QLBVzFCT4aJ9XcZh5aD39bmOz7Qt0TkQPD/bwl873SfMMhe3CKfxDXWAvnsU2/W2nVrbEpkccDPHm8hQ9U1EC4VgHJ7heD8Q=
c2: EP5QhH4muJucmNCiS3zcMPuMN1zNA2NCgLXHRkAIJzf1cA8qSlgu4C5ggKdhJ4MlNPPoPECx/cx3y8JvhFlsMBBLTMFZ3iJq6lri0WqqFMIHJVv3kZLLCefnljjFirPB3s5NrvTc0+zz83tOO5HcoihM3LFtskcBebhmFzNOEpkg
Decrypted Message: This takes a while sometimes
```

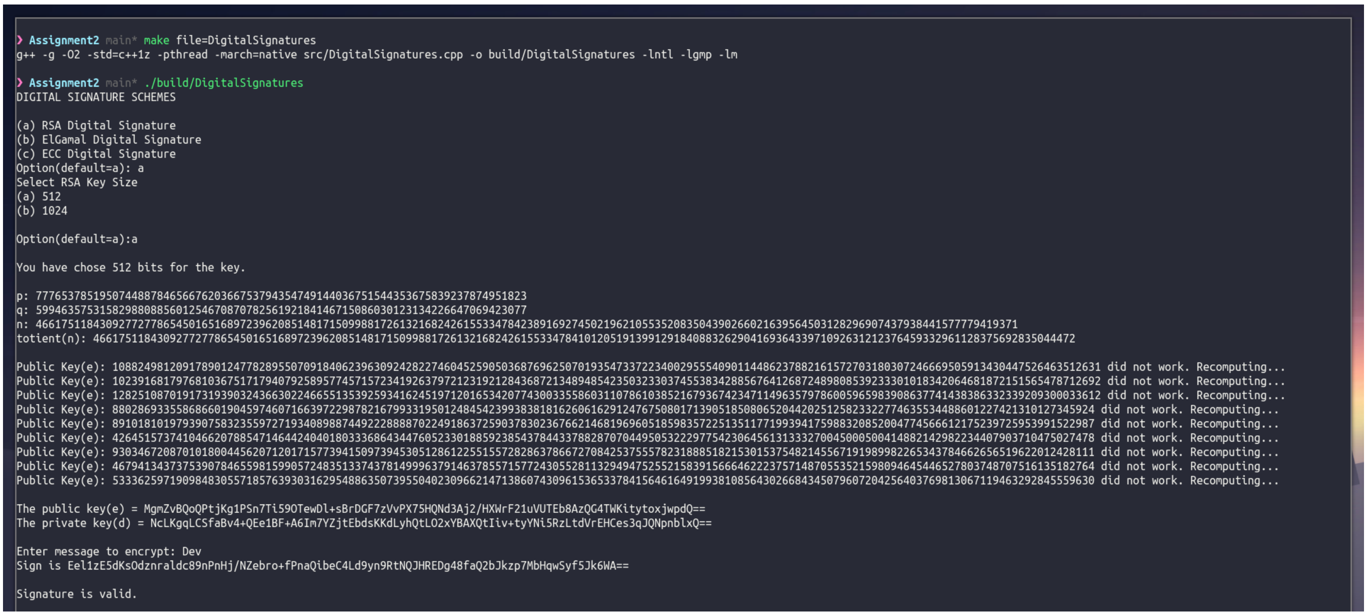
ECC



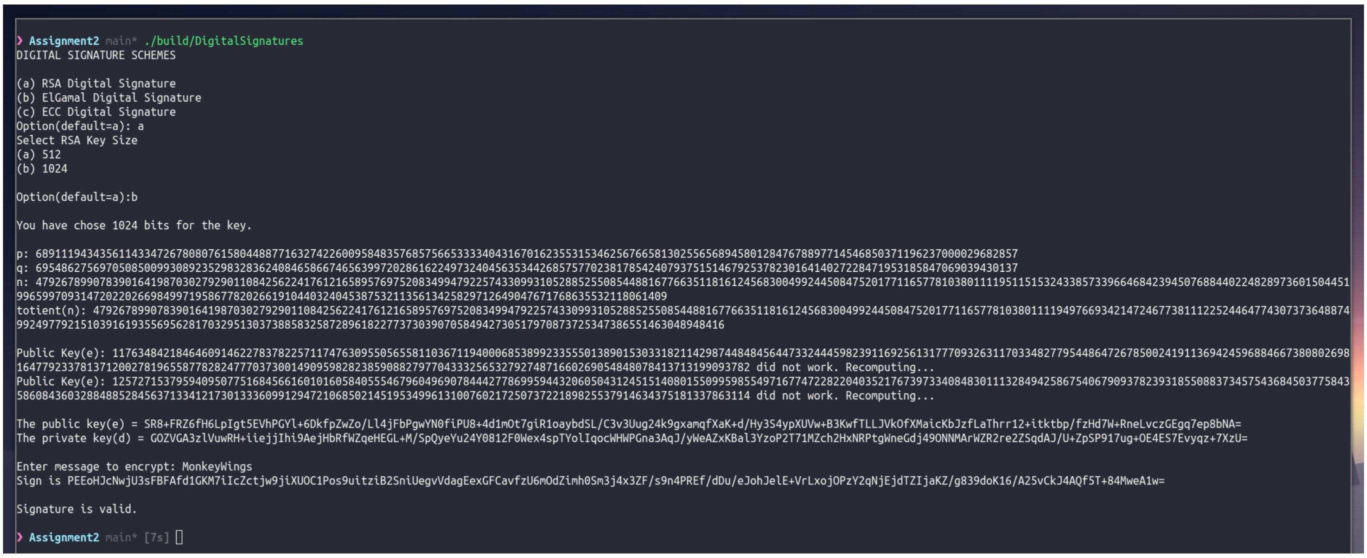
```
❯ Assignment2 main* make file=ECC
g++ -g -O2 -std=c++1z -pthread -march=native src/ECC.cpp -o build/ECC -lntl -lgmp -lm

❯ Assignment2 main* ./build/ECC
Enter message to encrypt: Star the repo

Private Key(d): X+M0tQZfyvT02fGOsg738pJJStFUMBki
Public Key(Q): (4126753437005575087436625938374434895466663885821159030816,
47354268556126881571505360693270093196705265556452190591893)

Encrypted Points on ECC:
C1: (3116419985064910705181698949362899155557566126325660768583,
23162874171416458634937374762067756079339077724396238537 43)
C2: (3074801721176786251972480126733265022006398894084743575426,
58742158319993568164681507161046726693371130673434593404 67)

Decrypted Message: Star the repo
```

Digital Signatures

RSA

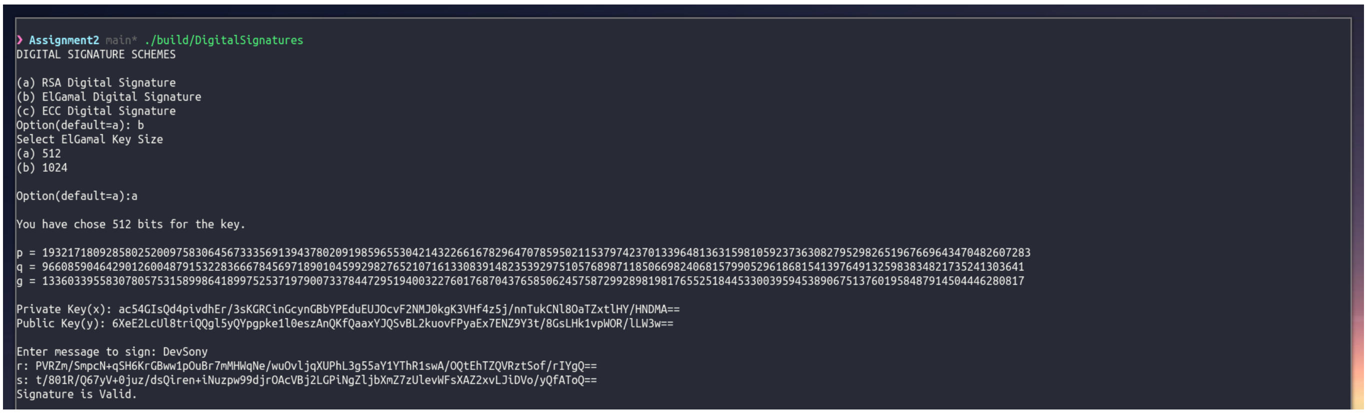


```
❯ Assignment2 main* make file=DigitalSignatures
g++ -g -O2 -std=c++1z -pthread -march=native src/DigitalSignatures.cpp -o build/DigitalSignatures -lntl -lgmp -lm

❯ Assignment2 main* ./build/DigitalSignatures
DIGITAL SIGNATURE SCHEMES

(a) RSA Digital Signature
(b) ElGamal Digital Signature
(c) ECC Digital Signature
Option(default=a): a
Select RSA Key Size
(a) 512
(b) 1024

Option(default=a):a

You have chose 512 bits for the key.

p: 77765378519507448878465667620366753794354749144036751544353675839237874951823
q: 59946357531582988088560125467087078256192184146715086030123134226647069423077
n: 4661751184309277277865450165168972396208514817150998817261321682426155334784238916927450219621055352083504390266021639564503128296907437938441577779419371
totient(n): 4661751184309277277865450165168972396208514817150998817261321682426155334784101205191399129184088326290416936433971092631212376459332961128375692835044472

Public Key(e): 10882498120917890124778289550709184062396309242822746045259050368769625070193547337223400295554090114486237882161572703180307246669505913430447526463512631 did not work. Recomputing...
Public Key(e): 10239168179768103675171794079258957745715723419263797212319212843687213489485423503233037455383428856764126872489808539233301018342064681872151565478712692 did not work. Recomputing...
Public Key(e): 12825108701917319390324366302246655135392593416245197120165342077430033558603110786103852167936742347114963579786005965983908637741438386332339209300033612 did not work. Recomputing...
Public Key(e): 8802869335586866019045974607166397229878216799331950124845423993838181626061629124767508017139051850806520442025125823322774635534488601227421310127345924 did not work. Recomputing...
Public Key(e): 8910181019793907583235597271934089887449222888870224918637259037830236766214681969605185983572251351177199394175988320852004774566612175239725953991522987 did not work. Recomputing...
Public Key(e): 4264515737410466207885471464424040180333686434476052330188592385437844337882870704495053222977542306456131333270045000500414882142982234407903710475027478 did not work. Recomputing...
Public Key(e): 9303467208701018004456207120171577394150973945305128612255155728286378667270842537555782318885182153015375482145567191989982265343784662656519622012428111 did not work. Recomputing...
Public Key(e): 4679413437375390784655981599057248351337437814999637914637855715772430552811329494752552158391566646222375714870553521598094645446527803748707516135182764 did not work. Recomputing...
Public Key(e): 5333625971909848305571857639303162954886350739550402309662147138607430961536533784156461649199381085643026684345079607204256403769813067119463292845559630 did not work. Recomputing...

The public key(e) = MgmZvBQoQPtjKg1PSn7Ti59OTewDl+sBrDGF7zVvPX75HQNd3Aj2/HXWrF21uVUTEb8AzQG4TWKitytoxjwpdQ==
The private key(d) = NcLKgqLCSfaBv4+QEe1BF+A6Im7YZjtEbdsKKdLyhQtLO2xYBAXQtIiv+tyYNi5RzLtdVrEHCes3qJQNpnblxQ==

Enter message to encrypt: Dev
Sign is Eel1zE5dKsOdznraldc89nPnHj/NZebro+fPnaQibeC4Ld9yn9RtNQJHREDg48faQ2bJkzp7MbHqwSyf5Jk6WA==

Signature is valid.
```

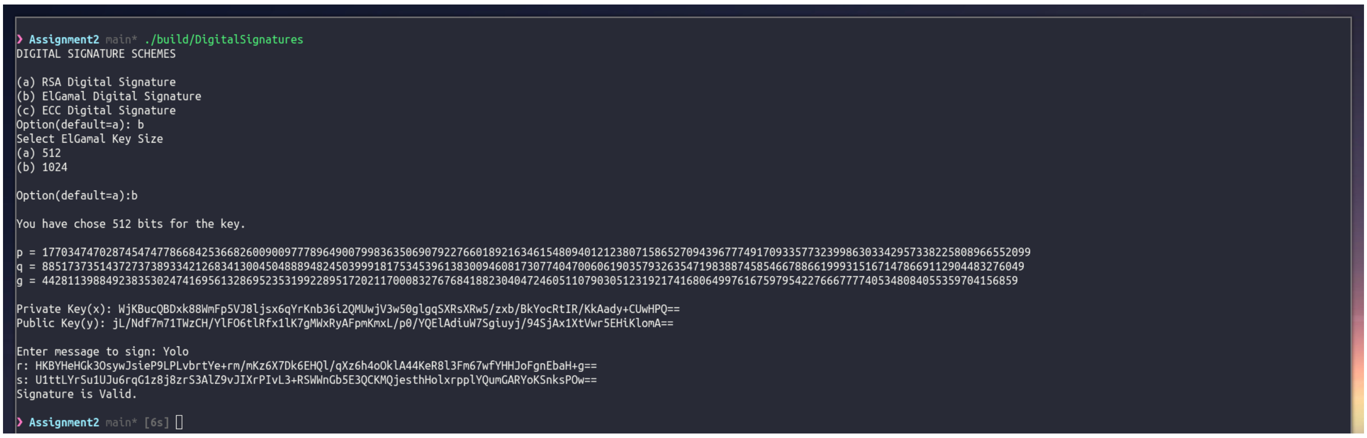


```
❯ Assignment2 main* ./build/DigitalSignatures
DIGITAL SIGNATURE SCHEMES

(a) RSA Digital Signature
(b) ElGamal Digital Signature
(c) ECC Digital Signature
Option(default=a): a
Select RSA Key Size
(a) 512
(b) 1024

Option(default=a):b

You have chose 1024 bits for the key.

p: 6891119434356114334726780807615804488771632742260095848357685756653333404316701623553153462567665813025565689458012847678897714546850371196237000029682857
q: 6954862756970508500993089235298328362408465866746563997202861622497324045635344268575770238178542407937515146792537823016414027228471953185847069039430137
n: 4792678990783901641987030279290110842562241761216589576975208349947922574330993105288525508544881677663511816124568300499244508475201771165778103801111951151532433857339664684239450768844022482897360150445 1
9965997093147202202669849971958677820266191044032404538753211356134258297126490476717686355321180614 09
totient(n): 4792678990783901641987030279290110842562241761216589576975208349947922574330993105288525508544881677663511816124568300499244508475201771165778103801111949766934214724677381112252446477430737364887 4
99249779215103916193556956281703295130373885832587289618227737303907058494273051797087372534738655146304894841 6

Public Key(e): 11763484218464609146227837822571174763095505655811036711940006853899233555013890153033182114298744848456447332444598239116925613177709326311703348277954486472678500241911369424596884667380802698
1647792337813712002781965587782824777037300149095982823859088279770433325653279274871660269054848078413713199093782 did not work. Recomputing...
Public Key(e): 12572715379594095077516845661601016058405554679604969078444277869959443206050431245151408015509959855497167747228220403521767397334084830111328494258675406790937823931855088373457543684503775843
5860843603288488528456371334121730133360991294721068502145195349961310076021725073722189825537914634375181337863114 did not work. Recomputing...

The public key(e) = SR8+FRZ6fH6LpIgt5EVhPGYl+6DkfpZwZo/Ll4jFbPgwYN0fiPU8+4d1mOt7giR1oaybdSL/C3v3Uug24k9gxamqfXaK+d/Hy3S4ypXUVw+B3KwfTLLJVkOfXMaicKbJzfLaThrr12+itktbp/fzHd7W+RneLvczGEgq7ep8bNA=
The private key(d) = GOZVGA3zlVuwRH+iiejjIhi9AejHbRfWZqeHEGL+M/SpQyeYu24Y0812F0Wex4spTYolIqocWHWPGna3AqJ/yWeAZxKBal3YzoP2T71MZch2HxNRPtgWneGdj49ONNMArWZR2re2ZSqdAJ/U+ZpSP917ug+OE4ES7Evyqz+7XzU=

Enter message to encrypt: MonkeyWings
Sign is PEEoHJcNwjU3sFBFAfd1GKM7iIcZctjw9jiXUOC1Pos9uitziB2SniUegvVdagEexGFCavfzU6mOdZimh0Sm3j4x3ZF/s9n4PREf/dDu/eJohJelE+VrLxojOPzY2qNjEjdTZIjaKZ/g839doK16/A25vCkJ4AQf5T+84MweA1w=

Signature is valid.

❯ Assignment2 main* [7s] ▯
```

El Gamal

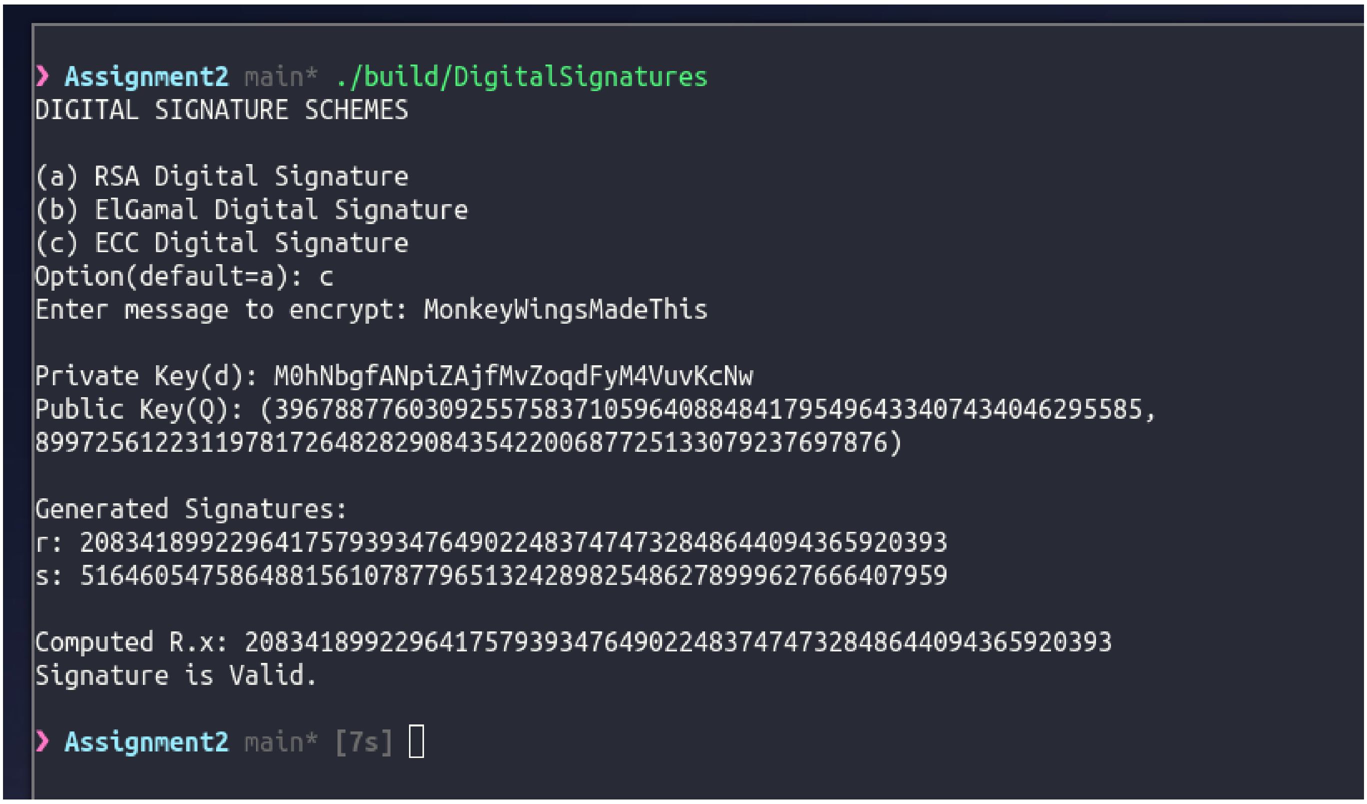


```
❯ Assignment2 main* ./build/DigitalSignatures
DIGITAL SIGNATURE SCHEMES

(a) RSA Digital Signature
(b) ElGamal Digital Signature
(c) ECC Digital Signature
Option(default=a): b
Select ElGamal Key Size
(a) 512
(b) 1024

Option(default=a):a

You have chose 512 bits for the key.

p = 19321718092858025200975830645673335691394378020919859655304214322661678296470785950211537974237013396481363159810592373630827952982651967669643470482607283
q = 9660859046429012600487915322836667845697189010459929827652107161330839148235392975105768987118506698240681579905296186815413976491325983834821735241303641
g = 13360339558307805753158998641899752537197900733784472951940032276017687043765850624575872992898198176555251844533003959453890675137601958487914504446280817

Private Key(x): ac54GIsQd4pivdhEr/3sKGRCinGcynGBbYPEduEUJOcvF2NMJ0kgK3VHf4z5j/nnTukCNl8OaTZxtlHY/HNDMA==
Public Key(y): 6XeE2LcUl8triQQgl5yQYpgpke1l0eszAnQKfQaaxYJQSvBL2kuovFPyaEx7ENZ9Y3t/8GsLHk1vpWOR/lLW3w==

Enter message to sign: DevSony
r: PVRZm/SmpcN+qSH6KrGBww1pOuBr7mMHWqNe/wuOvljqXUPhL3g55aY1YThR1swA/OQtEhTZQVRztSof/rIYgQ==
s: t/801R/Q67yV+0juz/dsQiren+iNuzpw99djrOAcVBj2LGPiNgZljbXmZ7zUlevWFsXAZ2xvLJiDVo/yQfAToQ==
Signature is Valid.
```



```
❯ Assignment2 main* ./build/DigitalSignatures
DIGITAL SIGNATURE SCHEMES

(a) RSA Digital Signature
(b) ElGamal Digital Signature
(c) ECC Digital Signature
Option(default=a): b
Select ElGamal Key Size
(a) 512
(b) 1024

Option(default=a):b

You have chose 512 bits for the key.

p = 17703474702874547477866842536682600900977789649007998363506907922766018921634615480940121238071586527094396777491709335773239986303342957338225808966552099
q = 8851737351437273738933421268341300450488894824503999181753453961383009460817307740470060619035793263547198388745854667886619993151671478669112904483276049
g = 442811398849238353024741695613286952353199228951720211700083276768418823040472460511079030512319217416806499761675979542276667777405348084055359704156859

Private Key(x): WjKBucQBDxk88WmFp5VJ8ljsx6qYrKnb36i2QMUwjV3w50glgqSXRsXRw5/zxb/BkYocRtIR/KkAady+CUwHPQ==
Public Key(y): jL/Ndf7m71TWzCH/YlFO6tlRfx1lK7gMWxRyAFpmKmxL/p0/YQElAdiuW7Sgiuyj/94SjAx1XtVwr5EHiKlomA==

Enter message to sign: Yolo
r: HKBYHeHGk3OsywJsieP9LPLvbrtYe+rm/mKz6X7Dk6EHQl/qXz6h4oOklA44KeR8l3Fm67wfYHHJoFgnEbaH+g==
s: U1ttLYrSu1UJu6rqG1z8j8zrS3AlZ9vJIXrPIvL3+RSWWnGb5E3QCKMQjesthHolxrpplYQumGARYoKSnksPOw==
Signature is Valid.

❯ Assignment2 main* [6s] ▯
```

ECC



```
❯ Assignment2 main* ./build/DigitalSignatures
DIGITAL SIGNATURE SCHEMES

(a) RSA Digital Signature
(b) ElGamal Digital Signature
(c) ECC Digital Signature
Option(default=a): c
Enter message to encrypt: MonkeyWingsMadeThis

Private Key(d): M0hNbgfANpiZAjfMvZoqdFyM4VuvKcNw
Public Key(Q): (3967887760309255758371059640884841795496433407434046295585,
899725612231197817264828290843542200687725133079237697876)

Generated Signatures:
r: 2083418992296417579393476490224837474732848644094365920393
s: 5164605475864881561078779651324289825486278999627666407959

Computed R.x: 2083418992296417579393476490224837474732848644094365920393
Signature is Valid.

❯ Assignment2 main* [7s] ▯
```