CS4062D Introduction to Information Security Assignment 2

By Dev Sony, B180297CS

[Github Repo](#)

The main source code is in `/src/`

Compile

To compile a .cpp file from `src/`, 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
```

Extra Notes

Utility files have been added in the `ultils/` folder. They contain necessary functions to facilitate parameter Generation and Convertions.

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): 5709783250553654622424502088847182128458303513840842549634524590191056881799190757453109827875209738534177632709680382483554353959013593405539986002988464

Public Key(e): 13145254860162006415478559628867556578415902242906767301897307524288131015902864882116367140751175842389393507035473693471897984763305271343807544276426705 did not work. Recomputing...
Public Key(e): 8171727684240066995614815936249509403812956908957924306503411787801291170962771816178652065254380934034383100210270725781580327517419974149908707807241997 did not work. Recomputing...
Public Key(e): 125647790189380387297061692577340724812490444170065188854333500440288334480905008667076553535831165899846587340340390481428361104055858357304932226912044462 did not work. Recomputing...
Public Key(e): 12209057352616557373746232801260362641987771094373536549847901801509647876068227501305478510270756054731209392856460462487658368181022910407331626780718715 did not work. Recomputing...
Public Key(e): 473531066997421667784883012536687497105030519915142772313338673872603228246778936050684171439952045446508980101175708853291436910727941966082409755292557241 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: 12518335120576807633052845203474369825326290873862649780491289373689310898627617479878988957362525823152751057567703744755705140901809670992469497991478393
q: 12388428838851177748320125955088441400253811257465341709776766602833191235627232795746932724718340300671424346856819325777072060047238715161702466239976079
n: 155082503822157259175939709065395156352106417175929292707435223721264553085214619580897606351304945586756020948334098554707730214855372677023895126160677810820565162131829605332158997397694535924656769659598018606203551216302951660865272338491857286116618290722083187967563117018943396419667889104981653161047
totient(n): 155082503822157259175939709065395156352106417175929292707435223721264553085214619580897606351304945586756020948334098554707730214855372677023895126160677785913801202703844223959187838834856310344554638331606527792564378599128160911236251607755138004896803894273685778924693390593358063473853393906576

Public Key(e): 144848498999091580797734340495290664421049323172377622144403541334764280709038752252884938171782891813099609398435568697580006959573727293442413101593678868461037527442351499026537844881050134841386917529684003439644151230901407643506927585461232660171429289230143610454581769555424111599156832825511322525233544 did not work. Recomputing...
Public Key(e): 84124300813767508084925886875312191302729675441764516865594771730946848382411558376118672796077934922299429221541929428792271841140347614681130774515628508151934209055241193631445101448178049932228531832991115618802459701228360573455212262801708787845733163990650053558183027431823612635686970653271529867460 did not work. Recomputing...
Public Key(e): 58844648127628919584051760202553625735253224350766686945992029606030545987551620628662994136913108518307065351176836234983456738909952821397704351728145921516652714080494356453904999215078309766990054994995452672266012977065694456234138140310186875240042723946768421658347342178697223034829800605762873394754 did not work. Recomputing...
Public Key(e): 12740749703313690932285478608510565053533639359628284466573018108709626053561597671542950204940120099982140045867141618752815988366435757734882035585870407681004540319623659793945569377174775555565069274475840886121681151136008023711813667609360766113853304888585762174933753413379864844021285268064344753572 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 = 29659019604270143079071571996714316626418664164455816199162606971433923336961394965336326542395687198080483191548028437781157652951445771835558567151159301666144662657597492633109118260107596498623310163522707638963811246881171213488412234482483026287243552142004933253238764264202485558616777431907195164697439
q = 14829509802135071539535785998357158313209332082227908099581303485716961684806974826681632711978435990402415957740142188905788264757228859177928357557965083307233132879874631655455913005379824931165508176135381948190562344058560674420611724124151314362177607100246662661938213210124277930838871595359575823487 19
g = 92302917573795974523298426299475570672798514305036478821826127463521677989384562347361740114742376500265537574590232309811992651033931953002527562762661617589575279611165236381145639396546001815095110866557525390991300868903514772204155045135989909823743771799724915462198042828661778369563631612962179900073

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+zz83tOO5HcoihM3LFtskcBebhnFzNOEpkg
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,
4735426855612688157150536069327009319670526556452190591893)

Encrypted Points on ECC:
C1: (3116419985064910705181698949362899155557566126325660768583,
2316287417141645863493737476206775607933907772439623853743)
C2: (3074801721176786251972480126733265022006398894084743575426,
5874215831999356816468150716104672669337113067343459340467)

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: 7776537851950744887846566762036675379435474914403675154435367583923787495 1823
q: 5994635753158298808856012546708707825619218414671508603012313422664706942 3077
n: 4661751184309277277865450165168972396208514817150998817261321682426155334784238916927450219621055352083504390266021639564503128296907437938441577779419371
totient(n): 4661751184309277277865450165168972396208514817150998817261321682426155334784101205191399129184088326290416936433971092631212376459332961128375692835044472

Public Key(e): 108824981209178901247782895507091840623963092428227460452590503687696250701935473372234002955540901144862378821615727031803072466695059134304475264635 12631 did not work. Recomputing...
Public Key(e): 102391681797680103675171794079258957745715723419263797212319212843687213489485423503233037455383428856764126872489800539233301018342064681872151565478712692 did not work. Recomputing...
Public Key(e): 128251087019173193903243663022466551353925934162451971201653420774300335586031107861038521679367423471149635797860059659839086377414383863323392093000033612 did not work. Recomputing...
Public Key(e): 880286933558686601904597460716639722978782167993319501248454239938381816260616291247675080171390518508065204420251258233227746355344886012274213101273 45924 did not work. Recomputing...
Public Key(e): 89101810197939075832355972719340898744922288887022491863725903783023676621468196960518598357225135117719939417598832085200477456666121752397259539915 22987 did not work. Recomputing...
Public Key(e): 42645157374104662078854714644240401803336864344760523301885923854378443378828707044950532229775423064561313332700450005004148821429822344079037104750 27478 did not work. Recomputing...
Public Key(e): 9303467208701018004456207120171577394150973945305128612255155728286378667270842537555782318885182153015375482145567191989982265343784662656519622012428111 did not work. Recomputing...
Public Key(e): 467941343737539078465598159905724835133743781499963791463785571577243055281132949475255215839156664622237571487055352159809464544652780374870751613518 2764 did not work. Recomputing...
Public Key(e): 53336259719098483055718576393031629548863507395504023096621471386074309615365337841564616491993810856430266843450796072042564037698130671194632928455 59630 did not work. Recomputing...

The public key(e) = MgmZvBQoQPtjKg1PSn7Ti590TewDl+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: 6954862756970508500993089235298328362408465866746563997202861622497324043544265875770238178542407937515146792537823016414027228471953185847069639430137
n: 47926789907839016419870302792901108425622417612165895769752083499479225743309931052885255085448816776635118161245683004992445084752017711657781038011119511515324338573396646842394507688440224828973601504451996599709314720220266984997195867782026619104403240453875321135613425829712649047671768635532118061409
totient(n): 47926789907839016419870302792901108425622417612165895769752083499479225743309931052885255085448816776635118161245683004992445084752017711657781038011119497669342147246773811122524464774307373648874992497792151039161935569562817032951303738858325872896182277373039070584942730517970873725347386551463048948416

Public Key(e): 11763484218464609146227837822571174763095505655811036711940006853899233555013890153033182114298744848456447332444598239116925613177709326311703348277954486472678500241911369424596884667380802698164779233781371200278196558778282477703730014909598282385908827977043332565327927487166026905484807841371319909378 2 did not work. Recomputing...
Public Key(e): 125727153795940950775164566160101605840555467960496907844427786995944320605043124515140801550995985549716774722822040352176739733408483011132849425867540679093782393185508837345754368450377584358608436032884885284563713341217301333609912947210685021451953496613100760217250737221898253791463437518133786311 4 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 = 966085904642901260048791532283666784569718901045992982765210716133083914823539297510576898711850669824068157990529618681541397649132598383482173524130364
g = 133603395583078057531589986418997525371979007337844729519400322760176870437658506245758729928981981765525184453300395945389067513760195848791450444628081

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 = 177034747028745474778668425366826009009777896490079983635069079227660189216346154809401212380715865270943967774917093357732399863033429573382258089966552099
q = 8851737351437273738933421268341300450488894824503999181753453961383009460817307740470060619035793263547198388745854667886619993151671478669112904483276049
g = 44281139884923835302474169561328695235319922895172021170008327676841882304047246051107903051231921741680649976167597954227666777740534808405535970415685

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/nKz6X7Dk6EHQl/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): (39678877603092557583710596408848417954964334074340462955585,
8997256122311978172648282908435422006877251330792376978876)

Generated Signatures:
r: 20834189922964175793934764902248374747328486440943659203 93
s: 51646054758648815610787796513242898254862789996276664079 59

Computed R.x: 2083418992296417579393476490224837474732848644094365920 393
Signature is Valid.

> Assignment2 main* [7s] 
```