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
```

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

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: 1258133512057680763305245203473806223172208873867240780491293173689310898627517479878088957362525823152751057587703744755708149081809670992469407991478393

p: 125813351205768097633052452034716396273172997480991293173689310898627617479878088957362525823152751057587703744755708149081809670992469407991478393

p: 1258123581858117774830219595988844180925381127746524178977466602833191238627731279574693277247183489380671423346865691925777707240608472381715161762466239976879

p: 12581258125125195957999599665995516635196417175929927674552237126455308521461958089766651310445586766969599

ps180660269551251252699516668622727228818187976503117891849393641967695959959769451595979797645159299279774352237712645530852146195808976665131089695587677302148553726770238995126166677785913801202708384422395918783883485631034455

de3833166652772566345990124595165695977343840952966442104922317237762214440354133476428679903875252588493817178289181389956939843556859758006695957372729344241310159367886846103752744235149902653784488105913484

problic Key(e): 1448844989999015807977343484952966442104923172377622144403541334764286799038752522884938171782891813899569395849759597772934424131015936788684610375274423514990395244193631445146418849932

Public Key(e): 1448844989999015807977343484952966442149923172377622144403541334764286799038752522884938171782891813899569395436510453153069975345104510451045105905893825512225353544 did not work. Recomputing...

Public Key(e): 1448844989999014807643046971319130272699243814510464518763049932451465271488049435644537619919146946545119130699258471193051446545165057148804935644517629919146947618051746989369777392149769458117636655971497890189549697894678108947899324794789418969547874789818993149647869999789669559777279382299455698797747755555656999674475808862176299155166678936676611385330489858576271493337798648492182552686443753739153180676656994674651185330598838557627149337
```

El Gamal

512 BITS

```
    Assignment2 main* make file=ElGamal
g++ g -02 -std=c++12 -pthread -march=native src/ElGamal.cpp -o build/ElGamal -lntl -lgmp -ln

    Assignment2 main* ./build/ElGamal
    Select ElGamal Key Size
    (a) 512
    (b) 1824

Option(default=a):a

You have chose 512 bits for the key.
p = 1934937433061888828758040211214998518047833439738527443487618020086999655596332974595888394405078054012083740385118953517967658164059218278040002787942203
q = 967668716530904410837902018560749925592391671698692637217438050180804548277981664872579401972025350270860418701925594767589538290820296051350200019393971101
g = 5326314866668932046918832309846888028408687147493267991105068463128363653388720435234292573522926149797860571243559499141389659606804747100377414476757129

Private Key(x): MySRDEFTcze0MDCRUKUbubgzMKYSIKRyjKGcotnogkhUrJvgzJBCCjILA+HhKrGqlGe2JLSvelSi_jvi@uvgdosQoA==
Public Key(y): f450gXvdiF5jVesdvzPIAqc2JqLHSdhma6r/08u6dAmFZC8geA/KPZCykKGIJM0ArbF1VqrK+nuJfhj2RRuQ==
Enter message to encrypt: I worked too long for this
c1: zac@23pyLtHDtsAO7xtwJrgPkfVPR4Ad104CwSGRnN-JFF0UBJfkYfalzHX0gzfsHVCFf8z7vNpytXuhQfS7dYQ==
c2: ERKtpSJ2LHTy9LTBpGsv40eJYfvZ3H8aCMOvi2vIuNugsA2dtHKjsdzCqMBrXw0FllB10vrenQSzl@mE45pMBzA=

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

1024 BITS

ECC

```
Assignment2 main* make file=ECC
g++ -g -02 -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+M0tQZfyvT02fG0sg738pJJStFUMBki
Public Key(Q): (4126753437005575087436625938374434895466663885821159030816,
4735426855612688157150536069327009319670526556452190591893)

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

Decrypted Message: Star the repo
```

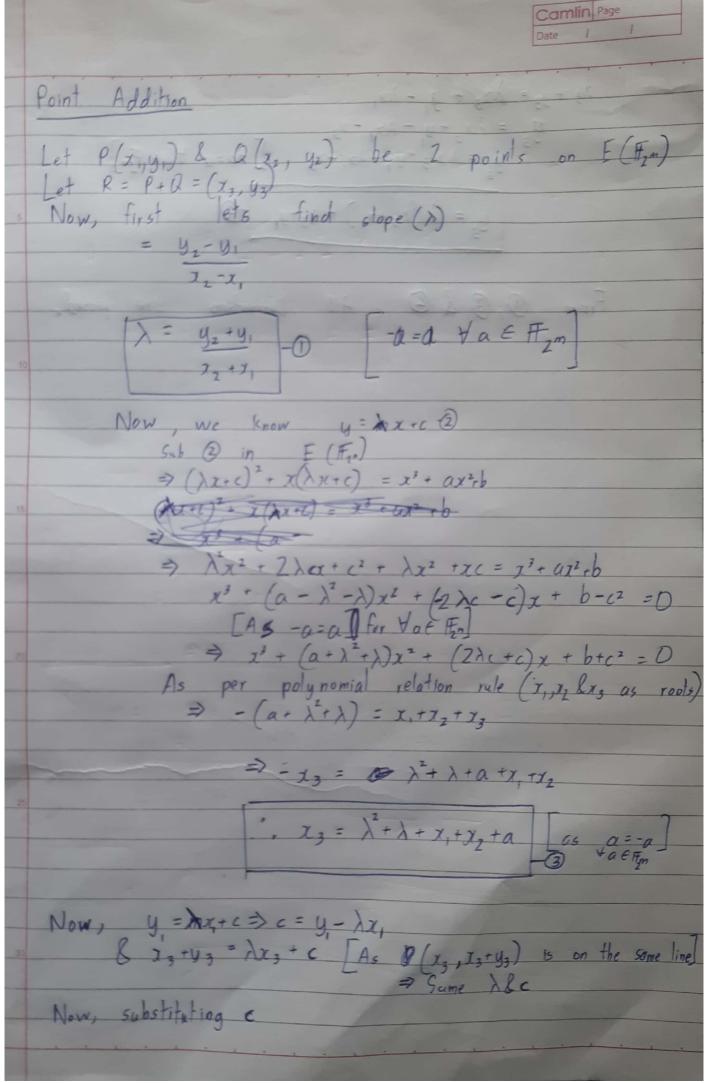
Digital Signatures

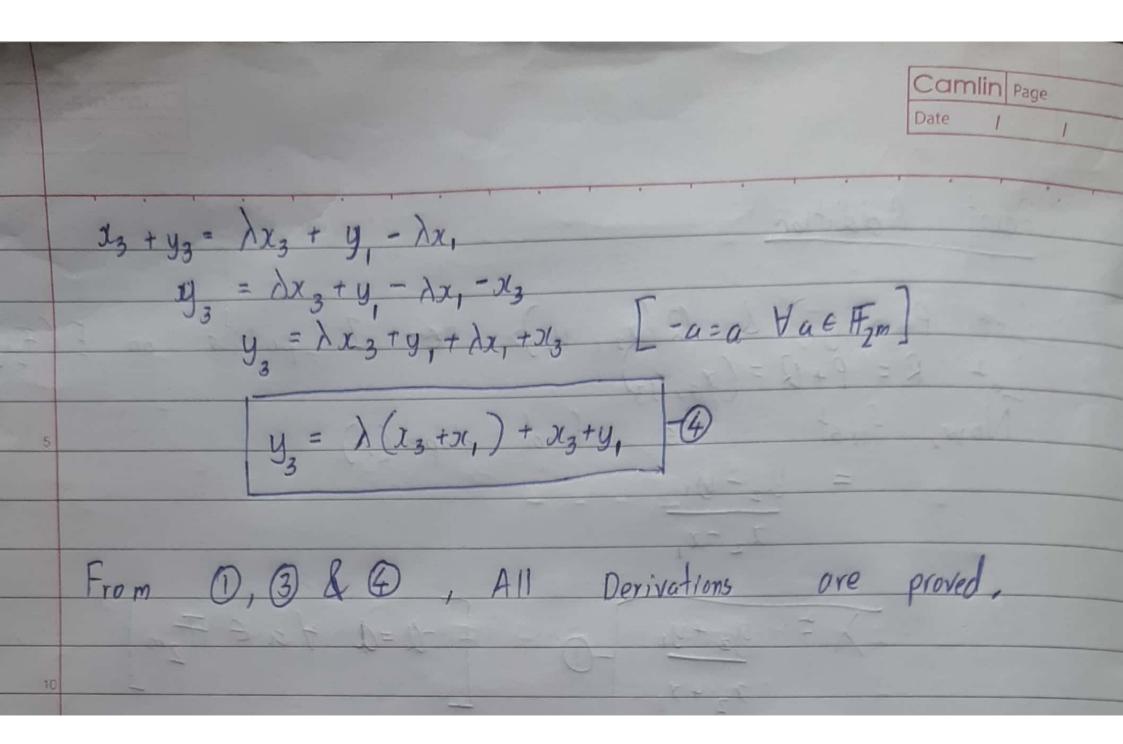
RSA

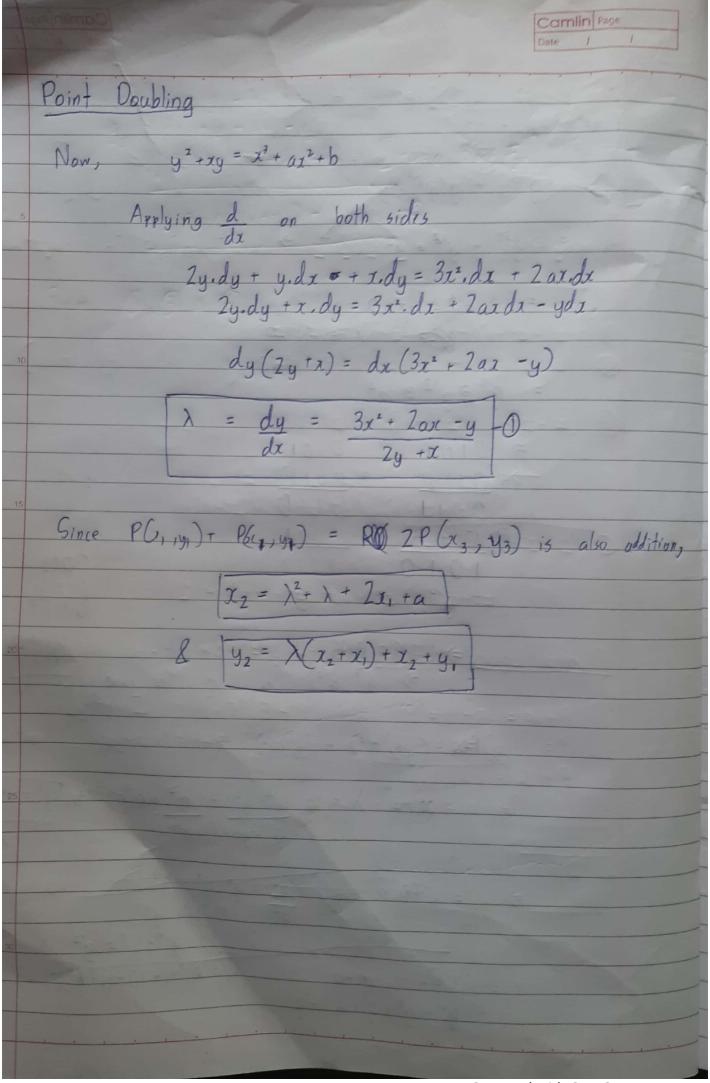
El Gamal

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] ☐
```







Scanned with CamScanner