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 utils/ folder. They contain necessary functions to facilitate parameter Generation and Convertions.

Screenshots (Encryption)

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: 12581335120576807633052452034738062231722088738674078049129317368931089862751747987808895736252582315275105758770374475570814906901809670992469407991478393

p: 12581335120576809763305245203471639627317299746692783191332862731279574693277247183483806714233468865819257777072060847238171516170246623997607

p: 1558025083221572591759397909653951563521064171759279277674522372124655308521401958089766651310445586766208948334090554707730214855372677823895126160677780820551563521064171759279277674352237212645530852146195088976665131049455867560209483340905547077302148553726770238951261606777809453592455769599

ps: 155802508322157259175939790965395156532106417175927929776435223712164553085214619508895766651310940955547077302148553726770238951261606777809453392155997397694535924565676965959

ps: 15580250832215725917593979096539515653210641717592992770743522377126453308521461950895766651310940955676097809822157725917593979096539515653210649177592992707435233951565380857707433240955676695599

priblic Key(e): 144884989999915807977343404952906644210492317237762214440354133476428679903875252288493817178289181389956939584975734424119159367868646103752744235149902653784488105913484

priblic Key(e): 14488498999901580797734340495290664421049231723776221444035413347642887090388255312225353344 did not work. Recomputing...

priblic Key(e): 8184120803176761905808992580891731191302726978717171994668083512155301610877939222294722214192465121524262923721193614163476146801130774515628081519340993254760851762959180940976350977345140804974513110507695804954094747745095550494747540804943564453747148097435172891935149646454761909595808517629255166527148804943564453914993545166527148804935645379739212419695408494745408985274778913180697826945747139498315165074880943564457879919354969955477773488203558579739323149976455979739373231497656660459930676611385330896873857773093231499764658930676651138530699789669595777777
```

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
```

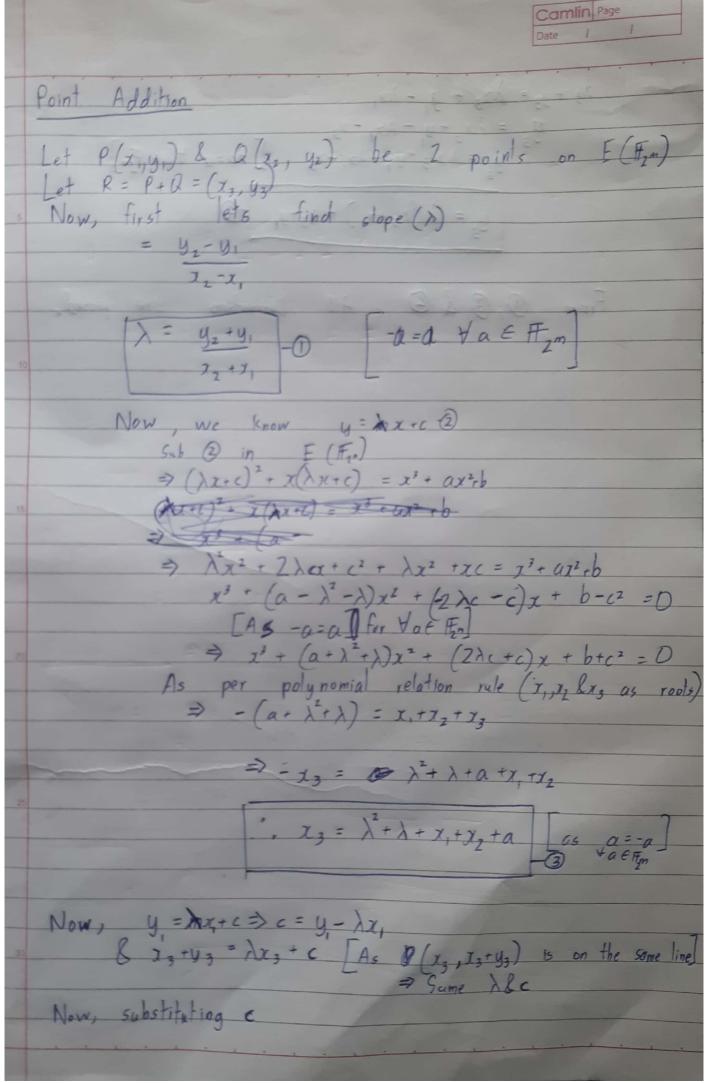
Screenshots (Digital Signatures)

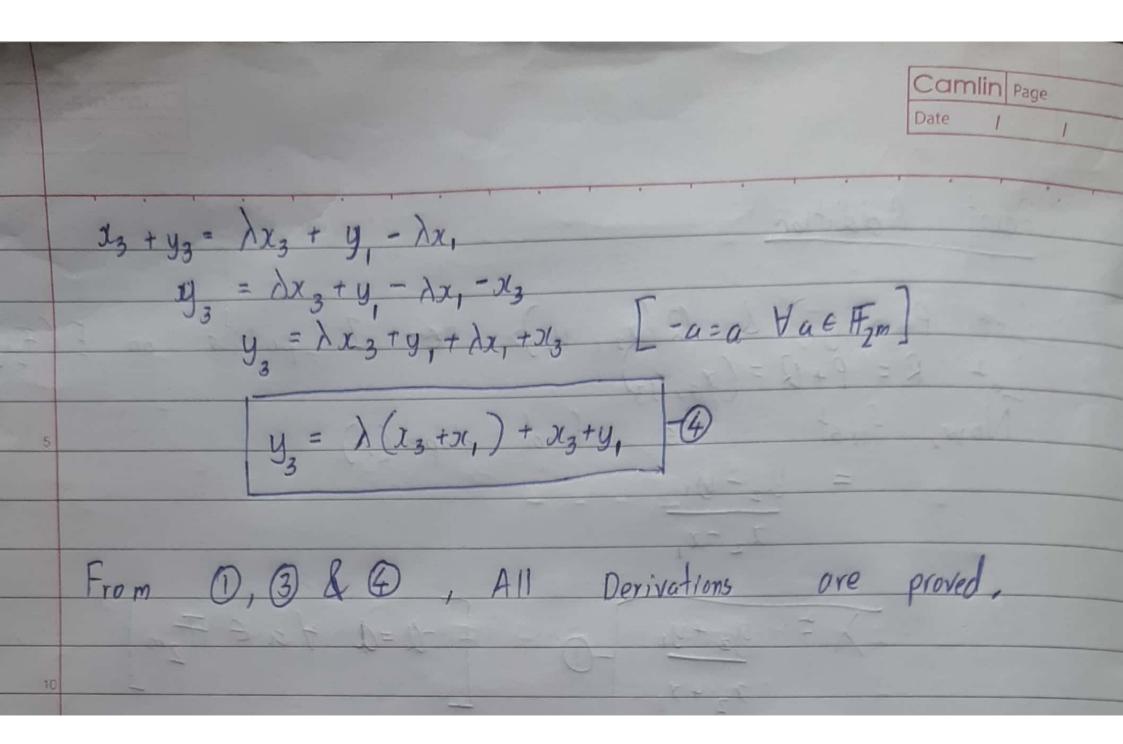
RSA

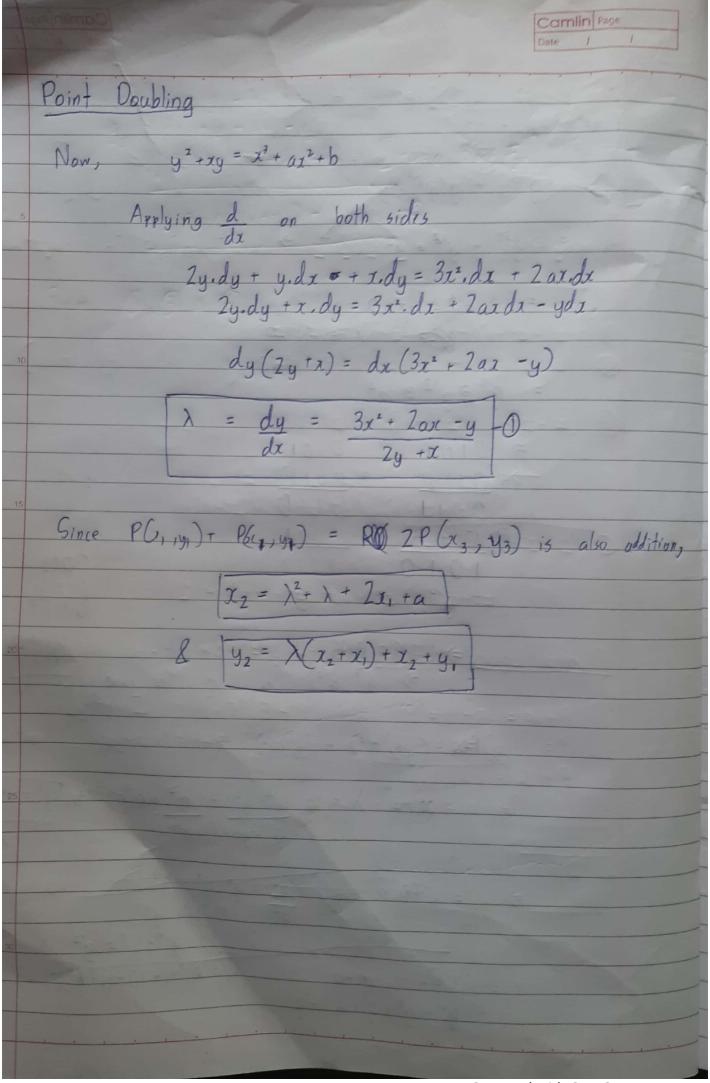
El Gamal

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): M0hNbqfANpiZAjfMvZoqdFyM4VuvKcNw
Public Key(Q): (3967887760309255758371059640884841795496433407434046295585,
899725612231197817264828290843542200687725133079237697876)
Generated Signatures:
r: 2083418992296417579393476490224837474732848644094365920393
s: 5164605475864881561078779651324289825486278999627666407959
Computed R.x: 2083418992296417579393476490224837474732848644094365920393
Signature is Valid.
Assignment2 main* [7s]
```







Scanned with CamScanner