

# 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 Conversions.

## Output Screenshots

RSA

**512 BITS**

```
> Assignment2 main* make filesRSA
g++ -g -O2 -std=c++1z -pthread -march=native src/RSA.cpp -o build/RSA -lnl -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: 96254237983138164967296779891229035779952261674417038972003855363972416801967
n: 5709783250553654622424502088847182128458303513840842549634524590191056881799346331502565099822978772083874388148413329096353594259775483911220274620927647
totient(n): 5709783250553654622424502088847182128458303513840842549634524590191056881799190754531098278752097385341776327096808382483554359590135934055399860029884640

Public Key(e): 13145254869162066415478559672866755657841590224290667673010973075242088131015902864082116367140751175842289393507035473693471897984763305271343807544276426705 did not work. Recomputing...
Public Key(e): 81747276842406699561481593624950940381295690895792430650341178700129117096277181617865206525438093403438310021027075781508327517419974149908707807411997 did not work. Recomputing...
Public Key(e): 12564779018938038729706169257734072481249444417006518885433350044028833448099508066707655353583116589984658734034039048142836110405585835730493222691204462 did not work. Recomputing...
Public Key(e): 12299057352616557373746232801260362641987771094034753654984790180150964787662822758130547851027075605473120939285646046248765836818102291040733162780718715 did not work. Recomputing...
Public Key(e): 47353106669974216677848830125366874971059305199151427723133863782760322824677893605060417143995204546508981011757088532914369107279419660824097552925741 did not work. Recomputing...

The public key(e) = RETISB1YauP91UdvOrGwSxnXw2tPyMw6FdINZYBmQtQ2fPsggdaUVBdsJtMwIeWd/4PY6MoK3tX447HrnUDQ==
The private key(d) = F5R2ldvc1vh4zKVmPKGhtokRJTzH0ktWcuItr5vOrYig76+pJ5ATkzv5P/Cy6hHurFwtc5DjcdJ7fshLVfVypQ==

Enter message to encrypt: Hello there

Encrypted message is GL8rOwc3NyquarIMDJ9T/8ijv84BaaX1s1Uk3j0x09BJHRm/jyZGOVIPVoCVX+1gpM3BaDqCbaAXRRxB09YpVQ==

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: 12518335120576807633052845203474396825326290873862649780491289373689310898627617479878988957362525823152751057567703744755785140901809670992469497991478393
q: 123884288388511774832012595508844140025381125746534170977676660283319123562723279574693272471834030067142434685681932577072060047238715161702466239976079
n: 1550825038221572591759397090653951563521064171759292927074352237212645530852146195808976063513049455867560209483340985547077302148553726770238951261606778108205651621318296053321589973976945359246567659599
8018060620355121630295166086527233849185728611661829072208318796756311701894339641966788910498165361047
totient(n): 1550825038221572591759397090653951563521064171759292927074352237212645530852146195808976063513049455867560209483340985547077302148553726770238951261606778591380120270384422395918783883485631034455
4638331606527792564378599128160911236251607927503647745538004896803894273685778924693390593580634738533933906576

Public Key(e): 144848498999991580797734340495290664421049323172377622144403541334764280709038752252884938171782891813099660939843556869758000695957372729344241310159367886846103752744235149902653784488105013484
1386917529684003439644151230901407643506927585461232660171429289230143610454581769555424111599156832825513225253544 did not work. Recomputing...
Public Key(e): 84124308813767580884925886875312191302729675441764516865594771730946848382411558376118672796077934922299429221541929428792271841140347614681130774515628508151934209055241193631445101448178049932
2285318329911561880245970122836057345521226280170878784573316399065005355818302743182361263568697065327152986746 did not work. Recomputing...
Public Key(e): 588446481276289159884051760202553625739253224350766686945992029606305459875516206286629941369131085183070653511768362349834567389099528213977043517281459215166527140804943564539049921507830976
69900549949545267226601297706569445623413814031018687524004272394676842165834734217869722303482980605762873394754 did not work. Recomputing...
Public Key(e): 1274074970331369093228547860851056505352533693596282446657301810870962605356159767154295020494012009998214004586714161875281598836643575773488203585870407681004540319623659793945569377174775555
56650692744758408861216811511360808237118136676093607661138533048885857621749337531337986484402128526806434753572 did not work. Recomputing...

The public key(e) = eYQnCa+PAYVP09NMVtLP+jnsjdHwORp1lVyOX/yfGkAI2E1SS1RvamCyWE+zVzZneJMKMYbb69fIEkin+Fa81FQuNi8yEMs9o58GgiZiWBBNXSj4nLJeqYi4ABpuHj4b/dQhVr7rWfSD/wexKug1vgUg150HC+nK6FSVem20SSE=
The private key(d) = UD30b/ep0CxBa+cc46R2/zZqXEXsN6/rhhJ11uub5YRILAU0qU6GALjFwK6r qX/RRgcce0KAc+zzgJnauevqBEH2v42dvZ3IAm9lJ6Lg6f+L7FCQAX3Vlt30uDuUgnaJpnNP2TaYr8M6BwLP12Zu+n7I2aFkVa5FQxk4g45hE=

Enter message to encrypt: Hello again

Encrypted message is e0hZch0SA/WACeRJIftf5Nc38Y1M1aFPnRzGd3nokV2Giy1FLLRdnzVozdtPj6yQkNkZ+4Gg5UlnxmzqTERERfu84eVDm2vUbyGdzNYRMfzRgnALiTLnaBT36aAaGXZD4nbLgYPCGFs+qzX/BsAgwOHmCuVhEQc0e0LfK=

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

## El Gamal

## 512 BITS

```
> Assignment2 main* make filesElGamal
g++ -g -O2 -std=c++1z -pthread -march=native src/ElGamal.cpp -o build/ElGamal -lnl -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 = 1934937433061808820758040211214998510047833433973852744348761002006090655596332974505880394405070054012083740385118953517907658164059210270040002787942203
q = 967468716530904410379020105607499255023916716986926372174380501000345482779816648725294019720253502700604187019255947675893829082029605135020001393971101
e = 53263148666089320469188323098468809284086871474932679911050684631283636533887204352342925735229261497978605712435594991413896596086084747100377414476757129

PrIvate Key(x): Ny5RDEfCzc0MDGRUuJUbGZWmKsIKrYjkEotnngKHU7y0zJBCCjTLA+HmhCFqL6P2JLSy6t1Sj1vJuvvdosQoA==
Public Key(y): f450gXvdtF5jVesvdZP1AQc2JqLH5dhn6r/O8ueaHwFzC8geA/KPpZCYkNo1LJM0Arb1VqrK+nuJThj2RRuQ==

Enter message to encrypt: I worked too long for this

c1: zaC023pylThDtsA07wtwJrgPKFvPR4Aq104Cw56RmN+JFF08JfKfYfaLzHX0zfsWVCFfBz7vNpvtXuhQf5dYQ==
c2: ERktpS3ZLH7yLTLBpGs40eJYfVz3W8aCM0vl2vIuNUGsA2dthKjsdzCqMBRw0FLlB10vrenQ5zi0mE45pM8zA=

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 = 2965981968427014307987157199671431662641866416445581619916260697143392336961394965236326542395687198080483191548028437781157652951445771835585671511593016661446626575974926331091182601075964986233101635227
07638963811246881171213488412234482483026287243552142004933253238764264202485558616777431907195164697439
q = 1482958980213507153953578599835715831320933208222790809958130348571696168488697482668163271197843599048241595774014218890578826475722885917792835755796508330723313287987463165545591300537982493116550817613
53819481985623440585606744206117241241513143621776071002466626619382132101242779308388715953597582348719
g = 9230291757379597452329842629947557067279851430503647982182612746352167798938456234736174011474237650026553775745902323098119926510339319530025275627626616175895752796111652363811456393965460018150951108665
5752539099130086890351477220415504513598990982374377179972491546219804282866177836956363161296217990073

Private Key(x): GAepKk9ENCxFeZyA9rNKH8Z76Dfz/XvR3RMH6QuLrWq7ZGB6bUKUCxSzCeexZyh4ovn5YV/bXk0QfQHsazKx6YGOy4fwytXK60guGsW/JlwcFXwqgPDCsbgBSLIgFeZbbyn8IewEunr/SYKXXVVGt1MIayD0Fb/UQmnp8pkiYOLs=
Public Key(y): IwUAPswc0LgBooah04GGoNL24T6v4BKlycqVzJzShwA+4LJsIq79XqdIWTX3Rho/L1Vh9at/NNlwJRSPrcFlfhrQ59EsF066HlmpJGP8/QMsRegIgeJZ9H9BQwQwPRdAkjFL3rg0DGSz/UwPY0SwOkY7Dq9Nrnph1AFvv26DFEY=

Enter message to encrypt: This takes a while sometimes

c1: 4futr4G55+C1RZX4PGyKr11J0jcbtE6FMSua0852Fsf9KLeq7bDmBjsC1njpfOF5fe/pxg+u83QLBVzFCT4aJ9xcZh5d39bmOz7Q0TkQPD/bwl8735FMmhe3CKfDXMAvnsU2/WznVrbEpkkcDPHm8hQ9U1EC4VgHJ7heD0Q=
c2: EP5QH4muJucmNCL53zcMPuMNIzNA2NcgLXHRkAIJzf1cA8qSLgu4C5ggKdhJ4MLNPPoPECX/cx3y8JvhFLsMBBLTMFZ3LjQ6LrI0WqgFMHJ3Vv3KZLLCefnljjFfirPB3s5NrvTc0+zz83t005HcoLhM3LftskcBebhmFzNOEpkg
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+M0tQZfyvT02fG0sg738pJJStFUMBki
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 -lmp -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: 77765378519507448878465667620366753794354749144036751544353675839237074951823
q: 599463575158298888560125467080787256192184146715086030123134226647069423077
n: 466175118438927277865450165168972396208514817150998817261321682426155334784238916927450219621055352083504390266021639564503128296907437938441577779419371
totient(n): 466175118438927277865450165168972396208514817150998817261321682426155334784101205191399129184088326290416936433971092631212376459332961128375692835044472

Public Key(e): 108824981209178901247782895507091840623963092428227460452590536876962507019354733723400295554090114486237882161572703180307246669505913430447526463512631 did not work. Recomputing...
Public Key(e): 102391681797681036751719407258957745715723419263797212319212843687213489485423503233037455383428856764126872489808539233018018342064681872151565478712692 did not work. Recomputing...
Public Key(e): 12825108701917319390324366302246655135392593416245197120165342077430033558603110786103852167936742347114963579786005965983908637741438386332339209300833612 did not work. Recomputing...
Public Key(e): 8802869335586866019045974607166397229878216799331950124845423993838181626061629124767508017139051850806520442025125823322774635534488601227421310127345924 did not work. Recomputing...
Public Key(e): 891018101979390758323559727193408980744922268807024910637259037830237662146810696085185983722513511710939417590832005200477456661217529725953991522087 did not work. Recomputing...
Public Key(e): 4264515737410466207885471464424040180333686434476052330188592385437844337882870704949053222977542306456131333270045000500414882142982234407903710475027478 did not work. Recomputing...
Public Key(e): 9303467208701018004456207120117157739415097394530512861225515728286378667270842537555782318885182153015375482145567191989982265343784662656519622012428111 did not work. Recomputing...
Public Key(e): 467941343735390784655981599057248351337437814999637914637855715772430552811329494752552158391566646222375714870553521590894645446527803748707516135182764 did not work. Recomputing...
Public Key(e): 53336259719084830557185763903162954886350739550402309662147138607430961536533784156461649199381085643026684345079607204256403769813067119463292845559630 did not work. Recomputing...

The public key(e) = MgnZvBQoQtjKg1PSn7Tl590TewDL+sBrDGFzVvPX7SHQNd3Ajz/HXWFr2iuvUTEbBAzG4TWKitytoxjwpdQ==
The private key(d) = NcLKqqlCfFaBv4+QeE1BF+A6In7VZjTEbdsKKdLyhQtL02xYBAxQtIiv+tyNlSRzLdtVrEHces3qJQnpnbLxQ==

Enter message to encrypt: Dev
Sign is Ee1tE5dKs0dznraldcB9nPhj/NZebro+FPnaQlbeC4ld9yn9RtNQHREdg48faQ2bJkzp7MbHqwSyf5jK6MA==

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: 6891194343561143347267800807158044887716327422600950483576857566533334043167016235531534625676650130255656894580128476788977145468503711962370000296082857
q: 695486275697050850099308923529832836240846586674656399720286162249732404563534426857570238178542407937515146792537823816414027228471953185047069039430137
n: 47926789907839016419870302792901108425622417612165895769752083499479225743309931052885255085448816776635118161245683004992445084752017711657781038011119511515324338573396646842394507688440224828973601504451
99659970931478202669849971958677820266191044032404538753211356134258297712649047671768635532118061409
totient(n): 47926789907839016419870302792901108425622417612165895769752083499479225743309931052885255085448816776635118161245683004992445084752017711657781038011119497669342147246773811122524464774307373648874
99249779251503916193556956281703295130373885835872896182277373039070584942730519790873725347386551463048948416

Public Key(e): 11763484218464609146227837822571174763095505655811036711940806853899233555013890153031821142987448484564733244558239116925613177709326311783348277954486472678500241911369424596884667380802698
1647792378137120027819658078202477703780014909598202305908827977043325653279274071660269845480878413713190093702 did not work. Recomputing...
Public Key(e): 125727137795048950775168456616018160584055467968469078444277869594428060594312451514800155095985497167747228220403521767397334084830111328494258675406790937823931855088373457543684503775843
58608436032884852845637133412713013360091294721068502145195349961310076021725073722189825537914634375181337863114 did not work. Recomputing...

The public key(e) = SR8+FRZ6fh6LpIgt5EVhpGYL+6DkfpZwZo/LL4jFbPgWYN0fIPUB+4d1m0t7gIR1oaybDSL/C3v3Uug24K9gxanqfXaK+d/Hy3S4ypXUVw+83KwFTLLJvkOFXMaicKbJzfLaThrr12+itktbp/fzHd7W+RneLvczGEga7ep8BNA=
The private key(d) = GOZVCA3zLVuwRH+ilejjiH9AeJhBRfNZqeHGL+M/SpQyeYu24Y0812F0Wex4spTVoLIqocwHPGna3AqJ/yWeAZxKbA3YzoP2T71NZch2HxNRptgWneGdj49ONNMARWZR2reZ5qdAJ/U+ZpSP917ug+OE4ESTVeyqz+7XzU=

Enter message to encrypt: MonkeyWings
Sign is PEeHJcNwJUs3FBAfADlGKM7l1cZctjw9jXiUOCs9uitziB2SiUegVdagEexGFCavfzUm6dZ1nh0Sn3j4x3ZF/s9n4PREF/dDu/eJohJeLe+VrLxoj0PzY2qNjEjdtJZ1jaKZ/g839d0K16/AZ5vCk34AQf5T+84WweA1w=

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 = 193217180928502520097583064567335691394378020919859655304214322661678296470785950211537974237013396481363159810592373630827952982651967669643470482607283
q = 9660859046429012600487915322836667845697189010459929827652107161330839148235392975105768987118506698240681579905296186815413976491325983834821735241303641
g = 1336033955830780575315899864189975253719790073378447295194003227601768704376585062457587299289819817655251844533803959453890675137601958487914504446280817

Private Key(x): ac54G1sQd4pvdhEr/3sKGRcInCynCBbYPEDuEUJ0cvF2NWJ0KqK3VHF4z5j/nnTukCNl80aTZxtLhY/HNDMA==
Public Key(y): 6XeZLcU8trlQQglsyQYppke10eszAnQkFQaaxYJQ5vBL2kuovFPyaExTENZ9Y3t/8GsLhk1vpW0R/LLW3w==

Enter message to sign: DevSony
r: PVRZn/SnncN+qSH6KrGBww1pDuBr7mMHwQNe/wuOvLjqXUPhL3g55aY1YThR1swA/OQtEhTZQVRzt5of/rIVgQ==
s: t/80IR/Q67yV+0juz/dsQIren+INuzpw99djroAcVBj2LGP1NgZLjbXmZ7zUlevWfSXA2zxvL3iDVo/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 = 177034747028745477866842536682600900977789649007998363506907922766018921634615480940121238071586527094396777491709335773239986303342957338225808966552099
q = 8851737351437273738933421268341300450488894824503999181753453961383009460817307740470060619035793263547198388745854667886619993151671478669112904483276049
g = 44281139884923835302474169561328695235319922895172021170008327676841882304047246051107903051231921741680649976167597954227666777405348084055359704156859

Private Key(x): H3KBucQB0vxk8BmFp5V38Ljx6qYrKnB36i2QMw3V3w50g1q5XRzXw5/zxb/BkYocRtR/KlAady+CUwHPQ==
Public Key(y): jL/Ndf7m7ITWzCH/YLF06tLRFx1LK7gHkxRyAFpnKnxL/p8/YQELAdiW7Sgiuyj/945jAx1XtVwr5EHiklonA==

Enter message to sign: YoLo
r: HKBYHeHkG30sywJs1eP9LPLvbrtYe+rm/nKz6X7Dk6EHQL/qxZ6h400kLA44KeR8L3Fm67wfYHJJoFgnEbaH+g==
s: UittLYrSuIU3u6rqG1z8j8zrS3ALZ9v3IXrPIvL3+R5WmNcb5E3QCKMQjesHh0LxrpplYQumGARYoKSnksPOw==
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] □
```



## Point Addition

Let  $P(x_1, y_1)$  &  $Q(x_2, y_2)$  be 2 points on  $E(\mathbb{F}_{2^m})$

Let  $R = P + Q = (x_3, y_3)$

Now, first let's find slope ( $\lambda$ ) =

$$= \frac{y_2 - y_1}{x_2 - x_1}$$

$$\boxed{\lambda = \frac{y_2 + y_1}{x_2 + x_1}} \quad \text{--- (1)} \quad \left[ -a = a \quad \forall a \in \mathbb{F}_{2^m} \right]$$

Now, we know  $y = \lambda x + c$  (2)

Sub (2) in  $E(\mathbb{F}_{2^m})$

$$\Rightarrow (\lambda x + c)^2 + x(\lambda x + c) = x^3 + ax^2 + b$$

$$\cancel{(\lambda x + c)^2 + x(\lambda x + c)} = \cancel{x^3 + ax^2 + b}$$

$$\Rightarrow \cancel{x^3 + (a - \lambda^2 - \lambda)x^2 + (2\lambda c - c)x + b - c^2} = 0$$

$$\Rightarrow \lambda^2 x^2 + 2\lambda c x + c^2 + \lambda x^2 + xc = x^3 + ax^2 + b$$

$$x^3 + (a - \lambda^2 - \lambda)x^2 + (2\lambda c - c)x + b - c^2 = 0$$

$$[As -a = a \text{ for } \forall a \in \mathbb{F}_{2^m}]$$

$$\Rightarrow x^3 + (a + \lambda^2 + \lambda)x^2 + (2\lambda c + c)x + b + c^2 = 0$$

As per polynomial relation rule ( $x_1, x_2$  &  $x_3$  as roots)

$$\Rightarrow -(a + \lambda^2 + \lambda) = x_1 + x_2 + x_3$$

$$\Rightarrow -x_3 = \lambda^2 + \lambda + a + x_1 + x_2$$

$$\boxed{\therefore x_3 = \lambda^2 + \lambda + x_1 + x_2 + a} \quad \text{--- (3)} \quad \left[ \begin{array}{l} as \\ \forall a \in \mathbb{F}_{2^m} \end{array} \right]$$

Now,  $y_1 = \lambda x_1 + c \Rightarrow c = y_1 - \lambda x_1$

&  $x_3 + y_3 = \lambda x_3 + c$  [As  $P(x_3, x_3 + y_3)$  is on the same line]  
 $\Rightarrow$  Same  $\lambda$  &  $c$

Now, substituting  $c$

$$x_3 + y_3 = \lambda x_3 + y_1 - \lambda x_1$$

$$y_3 = \lambda x_3 + y_1 - \lambda x_1 - x_3$$

$$y_3 = \lambda x_3 + y_1 + \lambda x_1 + x_3$$

$$[-a = a \quad \forall a \in \mathbb{F}_{2^m}]$$

$$y_3 = \lambda(x_3 + x_1) + x_3 + y_1 \quad \text{--- (4)}$$

From ①, ③ & ④, All Derivations are proved.

## Point Doubling

Now,  $y^2 + xy = x^3 + ax^2 + b$

Applying  $\frac{d}{dx}$  on both sides

$$2y \cdot dy + y \cdot dx + x \cdot dy = 3x^2 \cdot dx + 2ax \cdot dx$$

$$2y \cdot dy + x \cdot dy = 3x^2 \cdot dx + 2ax \cdot dx - y \cdot dx$$

$$dy(2y + x) = dx(3x^2 + 2ax - y)$$

$$\lambda = \frac{dy}{dx} = \frac{3x^2 + 2ax - y}{2y + x} \quad \text{--- (1)}$$

Since  $P(x_1, y_1) + P(x_2, y_2) = R$  ~~2P~~  $2P(x_3, y_3)$  is also addition,

$$x_2 = \lambda^2 + \lambda + 2x_1 + a$$

$$\& \quad y_2 = \lambda(x_2 + x_1) + x_2 + y_1$$