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
```

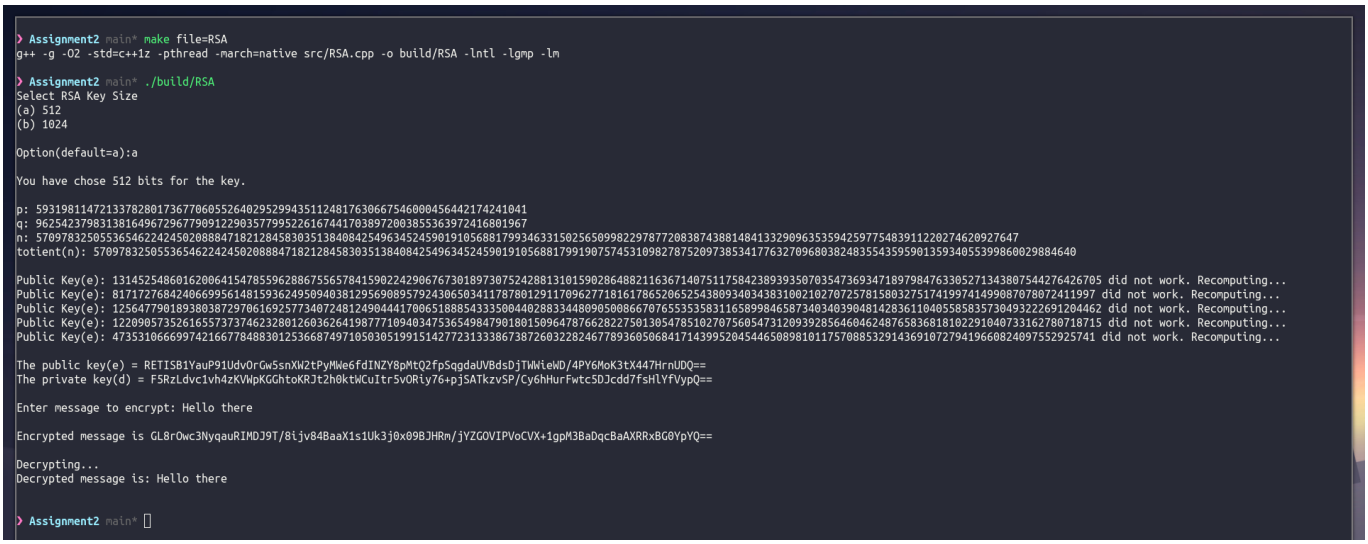
Extra Notes

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

Output Screenshots

RSA

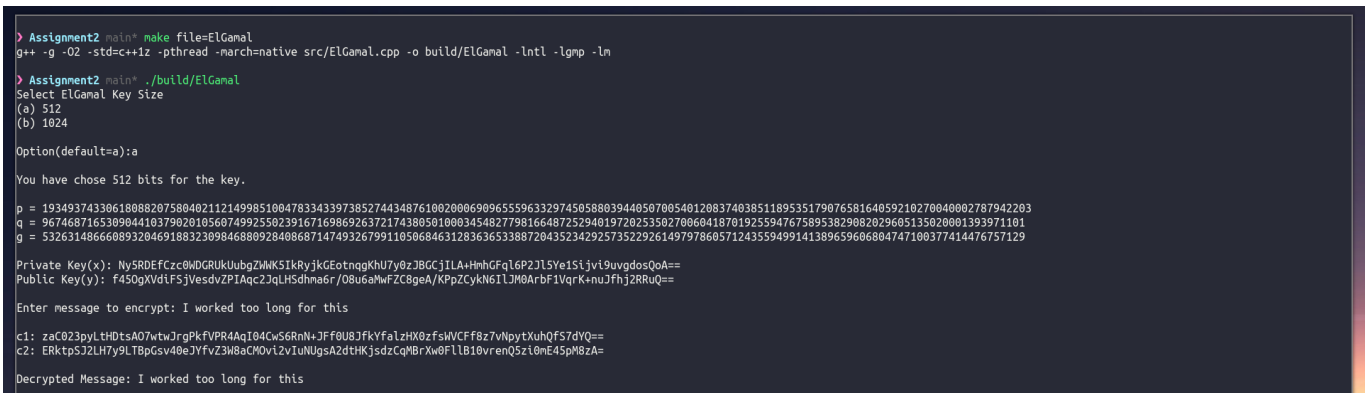
512 BITS



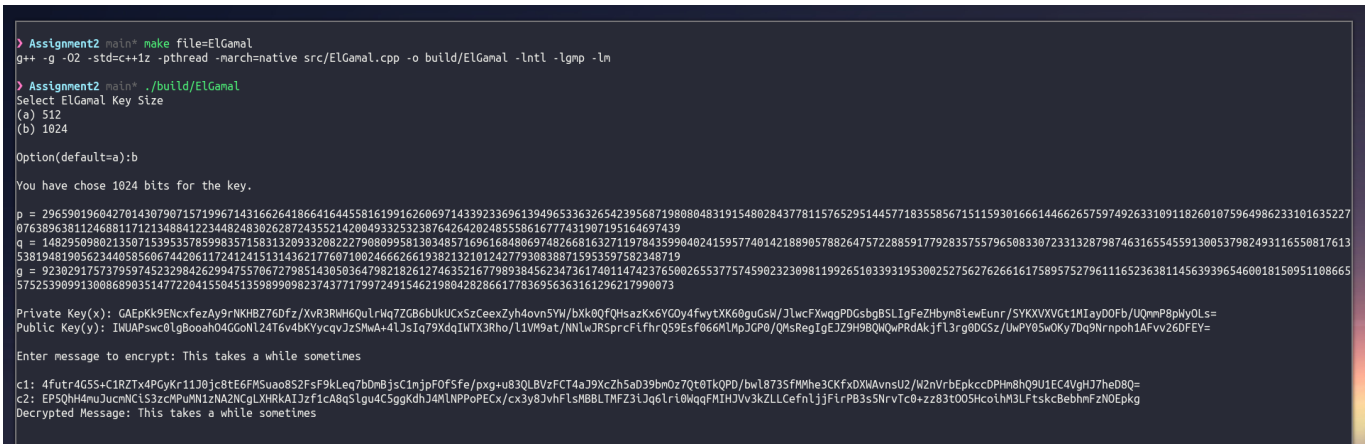
1024 BITS

El Gamal

512 BITS



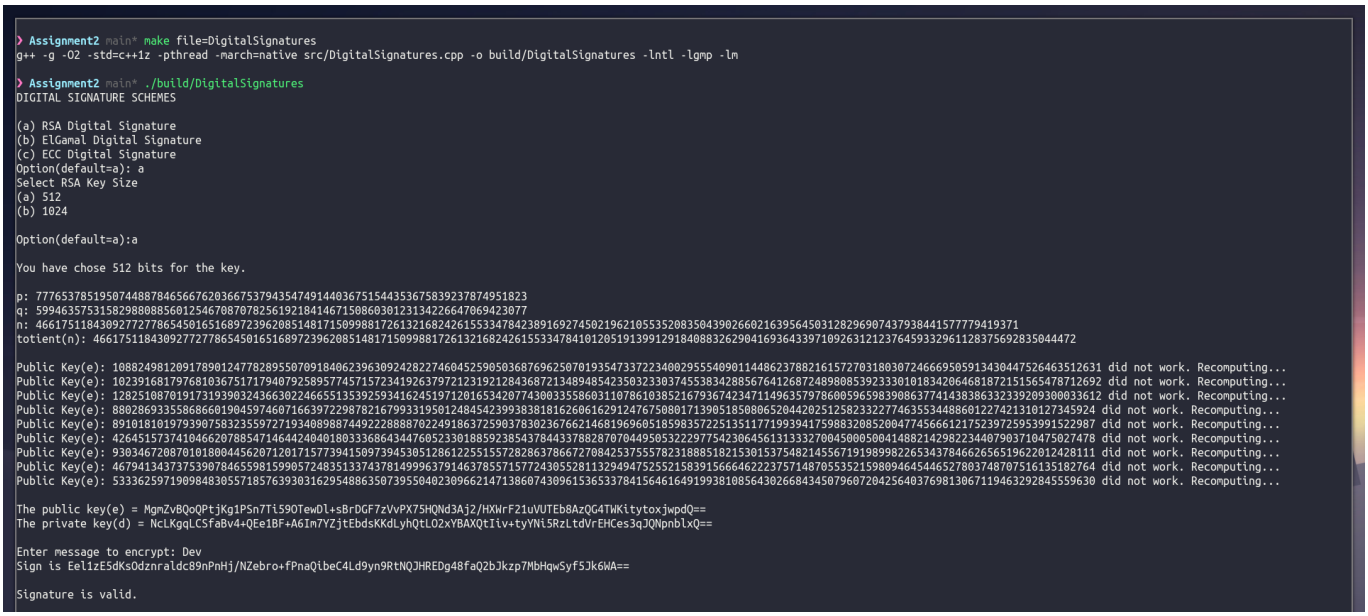
1024 BITS



ECC

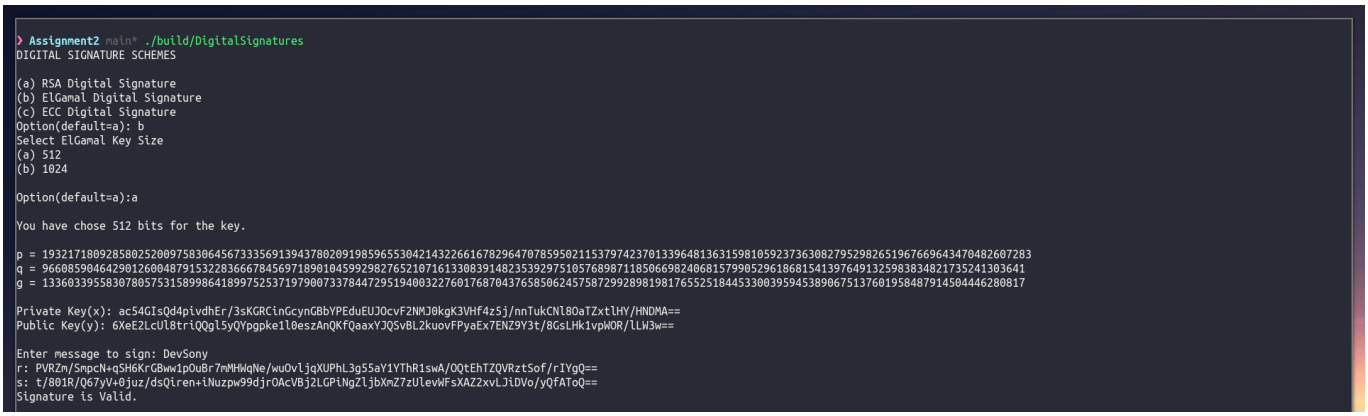
Digital Signatures

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: 7776537851950744887846566762036675379435474914403675154435367583923787491823
q: 5994635753158298808856012546708707825619218414671508603012313422664706942307 7
n: 4661751184309277277865450165168972396208514817150998817261321682426155334784238916927450219621055352083504390266021639564503128296907437938441577779419371
totient(n): 4661751184309277277865450165168972396208514817150998817261321682426155334784101205191399129184088326290416936433971092631212376459332961128375692835044472
Public Key(e): 1088249812091789012477828955070918406239630924282274604525905036876962507019354733722340029555409011448623788216157270318030724666950591343044752646351263 1 did not work. Recomputing...
Public Key(e): 1023916817976810367517179407925895774571572341926379721231921284368721348948542350323303745538342885676412687248980853923330101834206468187215156547871269 2 did not work. Recomputing...
Public Key(e): 1282510870191731939032436630224665513539259341624519712016534207743003355860311078610385216793674234711496357978600596598390863774143838633233920930003361 2 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 EelIzE5dKsOdznraldc89nPnHj/NZebro+fPnaQibeC4Ld9yn9RtNQJHREDg48faQ2bJkzp7MbHqwSyf5Jk6WA==
Signature is valid.

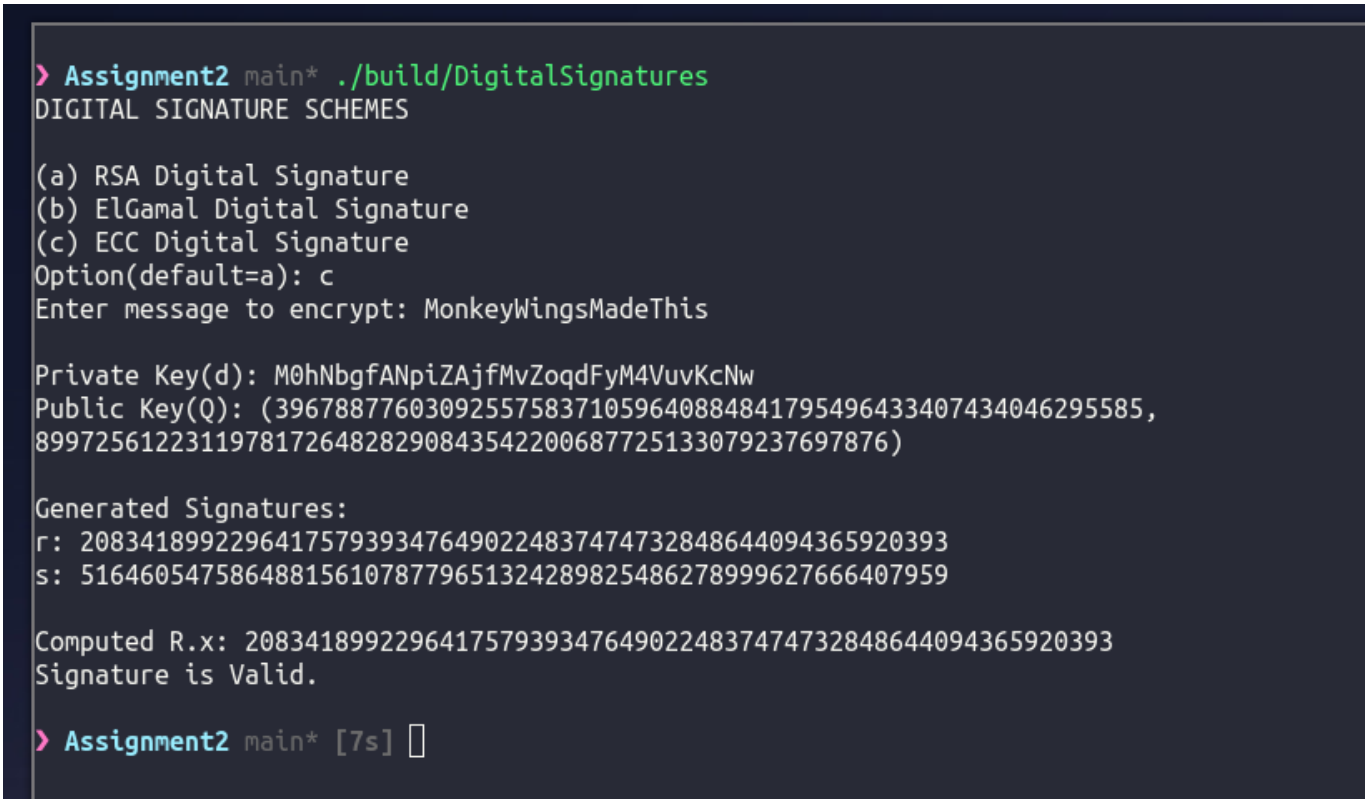

Assignment2 main* ./build/DigitalSignatures
DIGITAL SIGNATURE SCHEMES
(a) RSA Digital Signature
(b) ElGamal Digital Signature
(c) ECC Digital Signature
Option(default=a): a
Select RSA Key Size
(a) 512
(b) 1024
Option(default=a):b
You have chose 1024 bits for the key.
p: 6891119434356114334726780807615804488771632742260095848357685756653333404316701623553153462567665813025565689458012847678897714546850371196237000029682857
q: 6954862756970508509930892352983283624084658667465639972028616224973240456353442685757702381785424079375151467925378230164140272284719531858470690393401 37
n: 4792678990783901641987030279290110842562241761216589576975208349947922574330993105288525508544881677663511816124568300499244508475201771165778103801111951151532433857339664684239450768844022482897360150445199659970931472022026669849971958677820266191044032404538753211356134258297126490476717686355321180614 09
totient(n): 4792678990783901641987030279290110842562241761216589576975208349947922574330993105288525508544881677663511816124568300499244508475201771165778103801111954971669342147246773811122524464774307373648874992497792151039161935569562817032951303738858325872896182277373039070584942730517970873725347386551463048948416
Public Key(e): 1176348421846460914622783782257117476309550565581103671194000685389923355501389015303318211429874484845644733244459823911692561317770932631170334827795448647267850024191136942459688466738080269816477923378137120027819655877828247770373001490959828238590882797704333256532792748716602690548480784137131990937 82 did not work. Recomputing...
Public Key(e): 1257271537959409507751684566160101605840555467960496907844427786995944320605043124515140801550995985549716774722822040352176739733408483011132849425867540679093782393185508837345754368450377584358608436032884885284563713341217301333609912947210685021451953496913100760217250737221898255379146343751813378631 14 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/SpQyeYu24Y0B12F0Wex4spTYolIqocWHWPGna3AqJ/yWeAZxKBal3YzoP2T71MZch2HxNRPtgWneGdj49ONNMArWZR2re2ZSqdAJ/U+ZpSP917ug+OE4ES7Evyqz+7XzU=
Enter message to encrypt: MonkeyWings
Sign is PEEoHJcNwjU3sFBFAfd1GKM7lIcZctjw9jiXUOC1Pos9uitziB2SniUegvVdagEexGFCavfzU6mOdZimh0Sm3j4x3ZF/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.
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.
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): (396788776030925575837105964088484179549643340743404629558 5,
899725612231197817264828290843542200687725133079237697876)
Generated Signatures:
r: 208341899229641757939347649022483747473284864409436592039 3
s: 516460547586488156107877965132428982548627899962766640795 9
Computed R.x: 208341899229641757939347649022483747473284864409436592039 3
Signature is Valid.
Assignment2 main* [7s]

Camlin Page
Date / /

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 lets find slope (λ) =

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

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

Now, we know $y = \lambda x + c$ ②
Sub ② in $E(\mathbb{F}_{2^m})$

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

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

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

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

[As $-a = a$ 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)

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

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

$$\boxed{\therefore x_3 = \lambda^2 + \lambda + x_1 + x_2 + a} \quad ③ \qquad \left[\text{as } \underset{\forall a \in \mathbb{F}_{2^m}}{a = -a}\right]$$

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 λ & c

Now, substituting c

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

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

$$y_3 = \lambda x_3 + y_1 + \lambda x_1 + x_3 \qquad [-a = a \ \forall a \in \mathbb{F}_{2^m}]$$

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

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

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

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

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

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

$$\boxed{x_2 = \lambda^2 + \lambda + 2x_1 + a}$$

& $$\boxed{y_2 = \lambda(x_2 + x_1) + x_2 + y_1}$$