ECC_Final

December 8, 2022

1 Base_Change

[80]:
```
a=next_prime(175981698561051928659134961523704512879589723149871239887698698123456789 01)
a
```

[80]:
```
1759816985610519286591349615237045128795897231498712398876986981234567 9103
```

[81]:
```
l=a.digits(2^8)
print(l)
```

```
[255, 44, 249, 55, 23, 98, 207, 252, 179, 45, 142, 121, 87, 141, 190, 164, 117,
186, 176, 100, 226, 51, 90, 112, 205, 237, 17, 102, 208, 245, 9]
```

[82]:
```
len(l)
```

[82]:
```
31
```

[83]:
```
sourav=a.digits(2^30)
print(sourav)
```

```
[939076863, 859670620, 417520447, 799233502, 817526180, 684689810, 517789445,
1031018884, 9]
```

2 ADDITION, Subtraction & Multiplication

[84]:
```
A=next_prime(45189659162359861238795618270564615224876123951230756123875461 2390)
```

[85]:
```
L=A.digits(2^8)
print(L)
```

```
[243, 212, 5, 39, 33, 146, 119, 117, 245, 85, 53, 42, 42, 143, 71, 204, 119,
202, 235, 101, 223, 162, 119, 122, 240, 127, 74, 4]
```

[86]:
```
B=next_prime(23839659813265879613278562387561238795681273658791236571236 40982)
```

[87]:
```
S=B.digits(2^8)
print(S)
```

```
[109, 56, 115, 155, 240, 27, 194, 45, 201, 191, 243, 86, 84, 232, 251, 142, 52,
202, 249, 186, 3, 54, 47, 177, 139, 203, 5]
```

[88]:
```
print((A+B).digits(2^30))
```

```
[41487712, 216447047, 311516138, 282976160, 630500443, 459508867, 79151802, 276]
```

[89]:
```
print((A-B).digits(2^30))
```

```
[194157702, 517331138, 874078916, 317306228, 838878013, 565407403, 189156500,
273]
```

[90]:
```
print((A*B).digits(2^30))
```

```
[775541623, 904082450, 674284498, 698383547, 407923945, 227102914, 915866975,
271470896, 747622078, 249545757, 245533198, 814244225, 269765456, 933906280,
397]
```

3 Barrett Reduction

[91]:
```
Prime=0xffffffff00000001000000000000000000000000ffffffffffffffffffffffff
Prime
```

[91]:
```
115792089210356248762697446949407573530086143415290314195533631308867097853951
```

[92]:
```
p=115792089210356248762697446949407573530086143415290314195533631308867097853951
```

[93]:
```
p.digits(2^30)
```

[93]:
```
[1073741823, 1073741823, 1073741823, 63, 0, 0, 4096, 1073725440, 65535]
```

[94]:
```
print((((A*B)%p)).digits(2^30))
```

```
[151314446, 876022499, 88379576, 774376329, 357410509, 150572782, 857764354,
422283974, 40802]
```

4 Square & Multiply

[95]:
```
print(power_mod(A,B,Prime).digits(2^30))
```

```
[1061603227, 1012144664, 186596871, 906118858, 301667929, 882279835, 346394509,
382190261, 34690]
```

5 ECC ADDITION

[96]:
```
###### NIST P-256
p256 = 2^256-2^224+2^192+2^96-1
a256 = p256 - 3
```

```
b256 =␣
 ↪41058363725152142129326129780047268409114441015993725554835256314039467401291
## Base point
gx =␣
 ↪48439561293906451759052585252797914202762949526041747995844080717082404635286
gy =␣
 ↪36134250956749795798585127919587881956611106672985015071877198253568414405109
## Curve order
qq =␣
 ↪11579208921035624876269744694940757352999695522413576034242225906106851204436 9
FF = GF(p256)
EC = EllipticCurve([FF(a256), FF(b256)])
EC.set_order(qq)
# Base point
G = EC(FF(gx), FF(gy))
## Alice's private key
a = 545456567897987
## Alice's public key
A_prime = a*G
print (A_prime)
```

```
(85843274658334699305043628116802730568687465077193738908167644400996701448582 :
11271858291997268460882033468865739363157271298180036868936389185425453937674 7 :
1)
```

[97]:
```
print(85843274658334699305043628116802730568687465077193738908167644400996701448582.
 ↪digits(2^30))
```

```
[822618502, 839769931, 1026660504, 406381500, 813785078, 904312073, 299183961,
613803269, 48585]
```

[98]:
```
print(11271858291997268460882033468865739363157271298180036868936389185425453937674 7.
 ↪digits(2^30))
```

```
[413763691, 1072626329, 790597169, 524569649, 465465364, 885174302, 230441977,
490776745, 63796]
```

[99]:
```
b=54545656789798986
b*G
```

[99]:
```
(24488783781291031289044693414742267011758631797059251508710471768703341781691 :
40226669629065347600844197469478495199919812062201795325281959960505552766687 :
1)
```

[100]:
```
print(24488783781291031289044693414742267011758631797059251508710471768703341781691.
 ↪digits(2^30))
```

```
[850223803, 164210561, 32244799, 704277377, 1017435543, 478851327, 879500052,
172265376, 13860]
```

[101]:
```
print(40226669629065347600844197469478495199919812062201795325281959960505552766687.
↪digits(2^30))
```

```
[616859359, 1031785013, 520361210, 738402539, 162460059, 22895108, 692511935,
524158533, 22767]
```

[102]:
```
c=a+b
```

[103]:
```
c*G
```

[103]:
```
(42427664082208496657344607185247955735952951178621074248329131382117233343 6 :
26905321244620271162745029002783338378226335762420493407339252786313472686587 :
1)
```

[104]:
```
print(42427664082208496657344607185247955735952951178621074248329131382117233343 6.
↪digits(2^30))
```

```
[881818492, 1023820762, 820256646, 659935734, 739752735, 682811376, 696138780,
141807735, 240]
```

[105]:
```
print(26905321244620271162745029002783338378226335762420493407339252786313472686587.
↪digits(2^30))
```

```
[426424827, 478459199, 182449024, 625667172, 261989006, 461626777, 232341110,
936484334, 15227]
```

6 Scalar Multiplication

[106]:
```
print(gx.digits(2^30))
```

```
[412664470, 310699287, 515062287, 14639179, 608236151, 865834382, 69500811,
880588875, 27415]
```

[107]:
```
print(gy.digits(2^30))
```

```
[935285237, 785973664, 857074924, 864867802, 262018603, 531442160, 670677230,
280543110, 20451]
```

[108]:
```
250*G
```

[108]:
```
(42816713642517519830642598718239551603454468247529013466436607916954616566201 :
13039126481485811177248838545800811647913026559060138776014452474689200219750 :
1)
```

[109]:
```
print(42816713642517519830642598718239551603454468247529013466436607916954616566201.
↪digits(2^30))
```

```
[1064014265, 521290241, 992775702, 43075731, 28569876, 883937578, 715184055,
430701780, 24233]
```

[110]:
```
print(1303912648148581117724883854580081164791302655906013877601445247468920021975
↪digits(2^30))
```

```
[102393446, 222751136, 1012228591, 173923507, 691539925, 177923810, 712638746,
949247134, 7379]
```

7 Elliptic Curve Diffie–Hellman Key Exchange

[114]:
```
A*G
```

[114]:
```
(947636917253720231731410529097182379193812871464407557491684731248685058968 16 :
421649651250258643234800538152896035741138237124605988914888470091050325706 29 :
1)
```

[118]:
```
print(947636917253720231731410529097182379193812871464407557491684731248685058968 16.
↪digits(2^30))
```

```
[812812144, 413351939, 175593752, 36621247, 348616328, 229844039, 330928752,
374507044, 53634]
```

[119]:
```
print(421649651250258643234800538152896035741138237124605988914888470091050325706 29.
↪digits(2^30))
```

```
[1048372997, 837446331, 735075336, 938204959, 522143284, 304556449, 77464032,
563213970, 23864]
```

[116]:
```
print(947636917253720231731410529097182379193812871464407557491684731248685058968 16.
↪digits(2^30))
```

```
[812812144, 413351939, 175593752, 36621247, 348616328, 229844039, 330928752,
374507044, 53634]
```

[111]:
```
B*G
```

[111]:
```
(419315569659611225427974473957777259309338556754626357323770699277904076143 56 :
232956475518198086075349884274175178213135863967878569146418881526906407468 33 :
1)
```

[112]:
```
print(419315569659611225427974473957777259309338556754626357323770699277904076143 56.
↪digits(2^30))
```

```
[300973972, 97194001, 299744040, 264020083, 639732053, 284336951, 88827051,
451183582, 23732]
```

[113]:
```
print(232956475518198086075349884274175178213135863967878569146418881526906407468 33.
↪digits(2^30))
```

```
[680982865, 883972688, 735672104, 325441668, 807874354, 408655276, 533915784,
933361001, 13184]
```

[124]:
```
(A*B)*G
```

[124]:
```
(202235024698994927831646775306639296615074645453877232285561753934840367387 91 :
265628745379422119219751861006145254012416208176526566231581032473538901445 4 :
1)
```

[126]:
```
print(202235024698994927831646775306639296615074645453877232285561753934840367387
↪digits(2^30))
```

```
[110989031, 982503481, 701980360, 1001413779, 655806820, 1029467079, 171723775,
103899102, 11446]
```

[127]:
```
print(265628745379422119219751861006145254012416208176526566231581032473538901445
↪digits(2^30))
```

```
[274667958, 314429414, 239905683, 455132376, 859819234, 955703339, 804258419,
435316589, 1503]
```

8 Thank You