Elliptic Curves and Public Key Cryptography (3rd VDS Summer School)

Discussion/Problem Session II

Since we have not discussed most of the exercises proposed in Session I, I will just suggest some calculations. If you do not like computers, two of thme are small enough to be done by hand, but the idea is to use Sage (or any other software).

Exercise 12. Let E_1 be the elliptic curve defined over $\mathbb{F}_{11}$ by the equation $y^2 = x^3 + x + 6$ and $P_1 := (2, 7) \in E_1(\mathbb{F}_{11})$

a) Find $|E_1(\mathbb{F}_{11})| = 13$ and deduce (without calculating) that $< P_1 >= E_1(\mathbb{F}_{11})$.

We consider the *Elgamal cryptosystem* over $< P_1 >= E_1(\mathbb{F}_{11})$. The curve E_1 and the point P_1 are public data of the system and we suppose that messages have already been translated to points $M \in E_1(\mathbb{F}_{11})$. Private keys are $d \in \mathbb{Z}$ and the corresponding public keys are $dP_1 \in E_1(\mathbb{F}_{11})$. As usual, if Q is the public key of a user to whom we want to transmit a message M, we choose a random $n \in \mathbb{Z}$ and what we actually send is $(nP_1, nQ + M) \in E_1(\mathbb{F}_{11}) \times E_1(\mathbb{F}_{11})$.

b) If $d = 7$ is the private key of A, what's his/her public key?
c) If A receives $((8, 3), (10, 2))$, what message M was transmitted? [Remember, messages are elements of $E_1(\mathbb{F}_{11})$, not actual words.]

Exercise 13. Anna uses the ECDSA signature algorithm on the elliptic curve E_2 defined over $\mathbb{F}_7$ by the equation $y^2 = x^3 + 2x + 6$ and the base point $P_2 = (1, 3)$. He chooses $d_A = 4$ as private key, with corresponding public key $Q_A = d_A P_A$. He then signs a message m, that has $f = HASH(m) = 3$, using the *nonce* $k = 4$.

a) Check that $|E(\mathbb{F}_7)| = 11$.
b) Find Q_A.
c) What's Anna's signature for m?
d) Assuming you have already checked that $f = HASH(m)$, verify the signature obtained in c)

Exercise 14. Consider the curve E_3 defined ove $\mathbb{F}_{8831}$ by the equation $y^2 = x^3 + 3x + 45$, and the point $P_3 = (4, 11)$.We are going to use the Elgamal cryptosystem defined by E_3 and P_3.

a) What's the size of the group $E_3(\mathbb{F}_{8831})$?
b) What's the size of the subgroup $< P_3 >$? Is $| < P_3 > |$ prime?
c) Barbara chooses as her secret key $d_B = 3$. What's her public key $Q_B = d_B P_3$?
d) Anna wants to send to Barbara the message (written as a point in E_4) $M = (5, 1743)$. For that, she chooses the random number $n = 8$. What's the encrypted message C that Anna will send to Barbara?

Exercise 15. Find a random prime p that is 30 decimal digits long, an elliptic curve E_{rand} defined over $\mathbb{F}_p$, and a point $P_{rand} \in E_{rand}(\mathbb{F}_p)$ such that the order of the subgroup $< P_{rand} >$ is prime and at least 20 decimal digits long.

EXTRA (introduced after H. Schoutens' lecture): Use Sage to find a Weierstraß equation for the Fermat curve $x^3 + y^3 + z^3 = 0$ defined over $\mathbb{Q}$.

12) Let E_1 be the elliptic curve defined over $\mathbb{F}_{11}$ by the equation $y^2 = x^3 + x + 6$ and $P_1 := (2, 7) \in E_1(\mathbb{F}_{11})$

a) Find $|E_1(\mathbb{F}_{11})| = 13$ and deduce (without calculating) that $< P_1 >= E_1(\mathbb{F}_{11})$.

We consider the Elgamal cryptosystem over $< P_1 >= E_1(\mathbb{F}_{11})$.

b) If $d = 7$ is the private key of A, what's his/her public key?

c) If A receives $((8, 3), (10, 2))$, what message M was transmitted?

In [65]:
```
E1=EllipticCurve(GF(11),[1,6])
E1
```

Out[65]:
```
Elliptic Curve defined by y^2 = x^3 + x + 6 over Finite Field of s
ize 11
```

In [66]:
```
P1=E1(2,7)
P1
```

Out[66]:
```
(2 : 7 : 1)
```

In [67]:
```
#a)

order(E1)
```

Out[67]:
```
13
```

In [68]:
```
#b)

d=7
Q=d*P1
Q
```

Out[68]:
```
(7 : 2 : 1)
```

In [69]:
```
#c)
[(n, n*P1)for n in [1..12]]
```

Out[69]:
```
[(1, (2 : 7 : 1)),
 (2, (5 : 2 : 1)),
 (3, (8 : 3 : 1)),
 (4, (10 : 2 : 1)),
 (5, (3 : 6 : 1)),
 (6, (7 : 9 : 1)),
 (7, (7 : 2 : 1)),
 (8, (3 : 5 : 1)),
 (9, (10 : 9 : 1)),
 (10, (8 : 8 : 1)),
 (11, (5 : 9 : 1)),
 (12, (2 : 4 : 1))]
```

In [70]:
```
#THE SECRET n IS
n=3

#THE MESSAGE IS
M=E1(10,2)-n*Q
M
```

Out[70]:
```
(10 : 9 : 1)
```

13) Anna uses the ECDSA signature algorithm on the elliptic curve E_2 defined over $\mathbb{F}_7$ by the equation $y^2 = x^3 + 2x + 6$ and the base point $P_2 = (1, 3)$. He chooses $d_A = 4$ as private key, with corresponding public key $Q_A = d_A P_A$. He then signs a message m, that has $f = HASH(m) = 3$, using the nonce $k = 4$.

a) Check that $|E(\mathbb{F}_7)| = 11$.

b) Find Q_A.

c) What's Anna's signature for m?

d) Assuming you have already checked that $f = HASH(m)$, verify the signature in c)

In [71]:
```
E2=EllipticCurve(GF(7),[2,6])
P2=E2(1,3)
dA=4
f=6
k=4
```

In [72]:
```
#a)

order(E2)
```

Out[72]: 11

In [73]:
```
#b)

QA=dA*P2
QA
```

Out[73]: (3 : 5 : 1)

REMEMBER: SIGNATURE

- $n = | < P > |$
- $f = HASH(M), \quad (x_0, y_0) = kP,$
- $0 \neq r = x_0 \mod n, \quad 0 \neq s = k^{-1}(f + rd_A) \mod n,$
- Signature (r, s).

In [74]:
```
#b)
n=order(P2)
PP=k*P2
n, PP
```

Out[74]: (11, (3 : 5 : 1))

In [75]:
```
r=3
s=((f+r*dA)/k)%n
r, s
```

Out[75]: (3, 10)

REMEMBER: VERIFICATION

- $u_1 = s^{-1}f \mod n$ and $u_2 = s^{-1}r \mod n$.
- $(x_1, y_1) = u_1 P + u_2 Q_A$. If this point is O, signature is not valid.
- Signature is accepted as valid $\iff x_1 = r(= x_0) \mod n$. $[u_1 P + u_2 Q_A = kP]$

In [76]:
```
u1, u2=(f/s)%n, (r/s)%n
u1,u2
```

Out[76]: (5, 8)

In [77]:
```
R=u1*P2+u2*QA
R
```

Out[77]:
```
(3 : 5 : 1)
```

In [78]:
```
R[0]==r
```

Out[78]:
```
True
```

14) Consider the curve E_3 defined ove $\mathbb{F}_{8831}$ by the equation $y^2 = x^3 + 3x + 45$, and the point $P_3 = (4, 11)$.We are going to use the Elgamal cryptosystem defined by E_3 and P_3.

a) What's the size of the group $E_3(\mathbb{F}_{8831})$?

b) What's the size of the subgroup $< P_3 >$? Is $| < P_3 > |$ prime?

c) Barbara chooses as her secret key $d_B = 3$. What's her public key $Q_B = d_B P$?

d) Anna wants to send to Barbara the message (written as a point in E_4) $M = (5, 1743)$. For that, she chooses the random number $n = 8$. What's the encrypted message C that Anna will send to Barbara?

In [79]:
```
is_prime(8831)
```

Out[79]:
```
True
```

In [80]:
```
E3=EllipticCurve(GF(8831),[3,45])
P3=E3(4,11)
E3,P3
```

Out[80]:
```
(Elliptic Curve defined by y^2 = x^3 + 3*x + 45 over Finite Field
of size 8831,
 (4 : 11 : 1))
```

In [81]:
```
#a)
order(E3)
```

Out[81]:
```
8854
```

In [82]:
```
#b)

N=order(P3)
N, is_prime(N)
```

Out[82]:
```
(4427, False)
```

In [83]:
```
factor(N)
```

Out[83]:
```
19 * 233
```

In [84]:
```
#c)

dB=3
QB=dB*P3
QB
```

Out[84]:
```
(413 : 1808 : 1)
```

In [85]:
```
#d)
M=E3(5,1743)
n=8
Cifer=(n*QB,n*P3+M)
Cifer
```

Out[85]:
```
((673 : 146 : 1), (3889 : 2009 : 1))
```

15) Find a random prime p that is 30 decimal digits long, an elliptic curve E_{rand} defined over $\mathbb{F}_p$, and a point $P_{rand} \in E_{rand}(\mathbb{F}_p)$ such that the order of the subgroup $< P_{rand} >$ is prime and at least 20 decimal digits long.

In [86]:
```
p=random_prime(10^30,10^29)
p
```

Out[86]:
```
278698686739544551408811437343
```

In [87]:
```
#ONE WAY TO DO IT

A, B=randint(0,p-1), randint(0,p-1)
while mod(4*A^3+27*B^2,p)==0:
    A, B=randint(0,p-1), randint(0,p-1)

A, B
```

Out[87]:
```
(243483868313156462047730871 08L, 163768912347210539107420091470L)
```

In [88]:
```
E=EllipticCurve(GF(p),[A,B])
E
```

Out[88]:
```
Elliptic Curve defined by y^2 = x^3 + 243483868313156462047730871
8*x + 16376891234721053910742009147 0 over Finite Field of size 278
6986867395445514088114373 43
```

In [89]:
```
N=E.order()
N
```

Out[89]:
```
27869868673954405130701820 2050
```

In [90]:
```
factor(N)
```

Out[90]:
```
2 * 3^2 * 5^2 * 107 * 2207 * 6791 * 26921 * 1370597 * 10466503
```

In [91]:
```
G=E.gens()
G
```

Out[91]:
```
((421031762095859024425783185 38 : 84176041517801343349637393461 :
1),)
```

In [92]:
```
#SINCE ALL OF THE ABOVE IS RANDOM, TO GO ON AND DO AN ACTUAL EXAMPL
E
#WE WILL USE THE FOLLOWING DATA, THAT WAS FOUND AT RANDOM
#ALL LETTERS FOR THIS EXAMPLE WILL BE DOUBLED

pp=33268410620006274842089806653
AA=28400815227068151851575894387
BB=18506675668079694847092201139
EE=EllipticCurve(GF(pp),[AA,BB])
EE
```

Out[92]:
```
Elliptic Curve defined by y^2 = x^3 + 284008152270681518515758943
87*x + 18506675668079694847092201139 over Finite Field of size 3326
8410620006274842089806653
```

In [93]:
```
#WE FIND THE ORDER OF THE GROUP OF GF(pp)-RATIONAL POINTS NO THE CU
RVE
#TO SEE IF IT IS =BIG PRIME*SMALL COFACTOR
NN, factor(NN)
```

Out[93]:
```
(33268410620006341705016307088, 2^4 * 207927566375039635656351919 3
)
```

In [94]:
```
#IT WORKS: OREDER = 16*BIG PRIME
#WE FIND GENERATORS FOR THE GF(pp)-RATIONAL POINTS ON THE CURVE

GG=EE.gens()
GG
```

Out[94]:
```
((449871958030604291682135926 5 : 22522509420850368078559882331 : 1
),
 (22142363148099836544586471074 : 23119620757221324601719293293 :
1))
```

In [95]:
```
#IT IS NOT A CYCLIC GROUP. CHOOSE ONE GENERATOR AND SEE IF WE CAN B
UILD A BIG SUBGROUP OUT OF IT
RR=GG[0]
RR
```

Out[95]: (449871958030604291682135926 5 : 225225094208503680785598823 31 : 1)

In [96]:
```
nn=2^4 #THE SMALL COFACTOR
PP=nn*RR
PP
```

Out[96]: (563415825578552761001835777 6 : 263146048059256798210439445 98 : 1)

In [97]:
```
#HENCE PP GENERATE A SUBGROUP OF LARGE PRIME ORDER. LET'S CHECK IT
AGAIN
order(PP), is_prime(order(PP)), order(PP)==NN/2^4
```

Out[97]: (207927566375039635656351919 3, True, True)

In [98]:
```
#AN ALTERNATIVE WAY TO DO IT
```

In [99]:
```
A, xx, yy= randint(0,p-1), randint(0,p-1), randint(0,p-1)
B=mod(yy^2-xx^3-A*xx,p)
while mod(4*A^3+27*B^2,p)==0:
    A, xx, yy= randint(0,p-1), randint(0,p-1), randint(0,p-1)
    B=mod(yy^2-xx^3-A*xx,p)

A, B
```

Out[99]: (16364396922754573890126876355 9L, 22996975423464077981723910066 8)

In [100]:
```
E=EllipticCurve(GF(p),[A,B])
P=E(xx,yy)
E,P
```

Out[100]:
```
(Elliptic Curve defined by y^2 = x^3 + 16364396922754573890126876
559*x + 22996975423464077981723910066 8 over Finite Field of size 2
78698686739544551408811437343,
 (50552952415623245342652055125 : 27059108330742116297342987484 9 :
1))
```

In [101]:
```
N=E.order()
N
```

Out[101]: 27869868673954514659292379672 0

In [102]:
```
print factor(N)
E.gens()
```

```
2^4 * 3 * 5 * 7 * 97 * 4153 * 411805341164889979919
```

Out[102]:
```
((781294697361218490398343390 3 : 69280072100091898874926484826 : 1
),)
```

In [103]:
```
#AGAIN, WE USE AN EXAMPLE THAT WE FOUND RANDOMPLY BEFORE
#WE USE TRIPLE LETTERS FOR THIS EXAMPLE

ppp=77587016130986195369821448269
AAA=49882897950459941873978495 12
xxx, yyy=37095542502328139453335677028, 636727477324782685952008766
06
BBB=mod(yyy^2-xxx^3-AAA*xxx,ppp)
AAA, BBB, xxx, yyy
```

Out[103]:
```
(49882897950459941873978495 12,
 70956734508047934109942886526,
 37095542502328139453335677028,
 63672747732478268595200876606)
```

In [104]:
```
#IT IS NOT REALLYY NECESSARY, BUT LET'S CHECK THAT THE DISCRIMINANT
IS NOT 0

mod(4*AAA^3+27*BBB^2,ppp)==0
```

Out[104]:
```
False
```

In [105]:
```
#WE DEFINE THE ELLIPTIC CURVE AND THE BASE POINT
EEE=EllipticCurve(GF(ppp),[AAA,BBB])
PPP=EEE(xxx,yyy)
EEE,PPP
```

Out[105]:
```
(Elliptic Curve defined by y^2 = x^3 + 49882897950459941873978495 1
2*x + 70956734508047934109942886526 over Finite Field of size 7758
70161309861953698214482 69,
 (37095542502328139453335677028 : 63672747732478268595200876606 :
1))
```

In [106]:
```
#LETS FIND THE ORDER OF THE GROUP OF POINTS
NNN=EEE.order()
NNN, factor(NNN)
```

Out[106]:
```
(77587016130986140833535526700, 2^2 * 3 * 5^2 * 258623387103287136
111785089)
```

In [107]:
```
#THE SMALL COFACTOR IS
nnn=2^2*3*5^2
#IS THE REMAING PRIME BIG ENOUGH AT LEAST 20 DIGITS)?

qqq=NNN/nnn
qqq, log(qqq,10).n()
```

Out[107]:
```
(25862338710328713611178 5089, 26.4126677952182)
```

In [108]:
```
#YES, qqq HAS 27 DIGITS. LET'S FIND A POINT OF PRIME ORDER qqq

GoodPPP=nnn*PPP

GoodPPP, order(GoodPPP)==qqq
```

Out[108]:
```
((3947877083788885377898994804 1 : 2186240366409261008924334005 8 :
1), True)
```

EXTRA: Find a Weierstrass equation for the Fermat Cubic

In [117]:
```
var('x y z')
R.<x,y,z>=QQ[]
Fermat=R(x^3+y^3+z^3)
P=[1,-1,0]
E=EllipticCurve_from_cubic(Fermat,P)
E
```

Out[117]:
```
Scheme morphism:
  From: Projective Plane Curve over Rational Field defined by x^3
+ y^3 + z^3
  To:   Elliptic Curve defined by y^2 - 9*y = x^3 - 27 over Ration
al Field
  Defn: Defined on coordinates by sending (x : y : z) to
        (-z : 3*x : 1/3*x + 1/3*y)
```

$y^2 - 9y = x^3 - 27$

$y^2 - 9y = (y - \frac{9}{2})^2 - \frac{81}{4}$

Curve: $Y^2 = X^3 - \left(27 + \frac{81}{4}\right)$