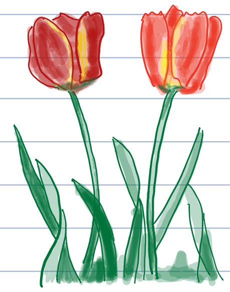
Secure Distributed Systems

CompSci 661 / 461



This video

- RSA is often explained in C.S. classes
  but is fairly old now
- Elliptic Curve crypto is increasingly common
  - used in all blockchains
- ECC is secure because of the
  discrete log problem
- we want to understand the internals
- no mathematical proofs.
- we'll return to Diffie-Helman Key Exchange

Diffie-Hellman Key Exchange

Goals:

- Alice and Bob want to exchange a secret
  - across a network
  - despite an observer
  - the secret is a shared key K_{AB}
- Diffie-Helman is the protocol they'll use

- DH is a general method, the engine
  - Elliptic Curves are what we'll plug-in as the fuel

- DH requires
  - a group based on prime p
  - the group must have a generator $\alpha \in \{2, \dots, p-2\}$

Two phases:

A. Setup (Phase 1)

1. choose a large prime p
2. choose an integer $\alpha \in \{2, 3, \dots, p-2\}$.
3. publish p and α

Assume that Alice & Bob each know p and α

B. KEY Exchange (Phase 2)

1. Alice : chooses $a = K_{A-} \in \{2, \ldots, p-2\}$ private

   compute $A = K_{A+} = \alpha^a \bmod p$ public

2. Bob : choose $b = K_{B-} \in \{2, \ldots, p-2\}$

   compute $B = K_{B+} = \alpha^b \bmod p$

α^a means $\underbrace{\alpha \circ \alpha \cdots \circ \alpha}_{a \text{ times}}$

3. $A \to B : A$

   $B \to A : B$

4. Alice computes $K_{AB} = B^a \bmod p = (\alpha^b)^a \bmod p = \alpha^{ab} \bmod p$

   Bob computes $K_{AB} = A^b \bmod p = (\alpha^a)^b \bmod p = \alpha^{ab} \bmod p$

5. K_{AB} can be used in any symmetric key protocol.
   - we have $\log_2(p)$ bits
   - if we need a shorter key, take fewer bits

Before we get into why this is secure, lets look at how this works.

1) A collection of properties of groups
2) an easier example that isn't secure
3) a more complicated example that is
4) an example using Elliptic curves

A group means that we have a set of elements G and a group operator $\circ$, such that

1. $a \circ b = c \in G$ the operator is closed
2. $a \circ (b \circ c) = (a \circ b) \circ c$ associativity
3. there exists an identity element $\mathbb{1} \in G$

   $a \circ \mathbb{1} = \mathbb{1} \circ a = a$ for all $a \in G$
4. for all $a \in G$, there exists an inverse a^{-1} such that

   $a \circ a^{-1} = a^{-1} \circ a = \mathbb{1}$
5. "Abelian" groups also have an operator such that

   $a \circ b = b \circ a$ for all $a, b \in G$ commutative

Here is one group!

Let $\mathbb{Z}_p^*$ represent a set (or subset) of integers within $i = 0, 1, \ldots, p-1$

for which: p is prime

the $\gcd(i, p) = 1$ no common factors with p

this forms a group under multiplication mod p *

with identity element $\mathbb{1}$.

We are going to see that Elliptic curves are groups, too!!

Here is an example of a group.

$\mathbb{Z}_9^*$ where $G = \{1, 2, 4, 5, 7, 8\}$

there are six elements in this group.

$*$ means multiplication

Here is a table of all pairs of values in the group as input to the operator

* mod 9	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	1	2
8	8	7	5	4	2	1

Do we have a group? Yes! This not a proof! Just examples.

1. closed?
   yes all instances of $x * y$ are in the group (mod 9)
2. associative? yes:
   $$\left.\begin{aligned} 2*(4*5) &= (2*4)*5 \\ 2*2 &= 8*5 \\ 4 &= 4 \end{aligned}\right\} \text{mod } 9$$
3. 1 is in every row
4. 1 is in every row
5. For example $2 \times 4 = 8$ and $4 \times 2 = 8$

Here is another example of a group. This group fits our definition, but we'll see it's not good for cryptography.

Example 2:

Our group will be $\mathbb{Z}_{11}^{+}$.

$p=11$

addition is our operator

$G=\{0,1,2,3,4,5,6,7,8,9,10\}$

Recall I mentioned the generator? For this group, the generator is $\alpha=2$. That means, with 2 and our operator, we can generate all the elements in the group.

Let's generate our group from $\alpha=2$ for $i=1 \ldots 11$

Keep in mind the operator:

$\underbrace{\alpha \circ \alpha \circ \alpha \circ \alpha}_{4 \text{ times}}$

So 4α for this group?

$\alpha+\alpha+\alpha+\alpha=4\alpha$

i	$i\alpha \bmod 11$
1	2
2	4
3	6
4	8
5	10
6	1
7	3
8	5
9	7
10	9
11	0

Exciting!!

Recall that Diffie-Helman Key Exchange is our engine. And groups are our fuel. Let's feed this group to DHKE.

Example of applying $\mathbb{Z}_{11}^{+}$ to DHKE

Alice

Private key: $\underline{4}$

Public key:

$(\alpha + \alpha + \alpha + \alpha) \bmod 11$

$\alpha(4) \bmod 11$

$8 \bmod 11$

$A = 8$ ← sends to Bob

Bob

Private key: $\underline{8}$

Public key:

$\alpha(8) \bmod 11$

$16 \bmod 11$

$B = 5$ ← sends to Alice

Alice

$K_{AB} = 5 \cdot 4 \bmod 11$

$= 20 \bmod 11$

$= 9$

Bob

$K_{AB} = 8 \cdot 8 \bmod 11$

$= 64 \bmod 11$

$= 9$ ✓

Perfect, they both have the same key.

The question is: Given that an attacker

- Knows that $\mathbb{Z}_{11}^{+}$ is being used. ← Kerckhoff's principle!
- Sees that Alice sent 8
- Sees that Bob sent 5

Can the attacker learn the shared key is 9?

For <u>this group</u>? Yes!! Here's how:

Attacker finds discrete log of $\alpha x = A \bmod 11$

$\alpha x = 8 \bmod 11$

$2x = 8 \bmod 11$

$x = (2^{-1})\, 8 \bmod 11$

Even though the group operation is addition, we can express the relationship between α, A, and x using multiplication.

recall that the inverse of a number is the value whose product equals 1 (but mod 11 here...)

Looking at the table

i	$i\alpha \bmod 11$
1	2
2	4
3	6
4	8
5	10
6	1
7	3
8	5
9	7
10	9
11	0

We need a y such that

$2y = 1 \bmod 11$?

or use the extended Euclid's algorithm not discussed here.

when $y = 6$, the above is true.
and so:

$x = 6 \cdot 8 \bmod 11$
$= 48 \bmod 11$
$= 4$ ← Alice's private key

Let's find Bob's private key

$\alpha x = 5 \bmod 11$

$2x = 5 \bmod 11$

$x = (2^{-1})5 \bmod 11$

$x = 6 \cdot 5 \bmod 11$

$x = 30 \bmod 11$

$x = 8$

The shared key?

subtle point!
addition 4 times
(not exponentiation)

$K_{AB} = (2 \times 4) \times 8 \bmod 11$
$= 4 \bmod 11$

Does that mean that Diffie-Helman Key Exchange is not secure?

No! We fed it the wrong fuel.

Let's try with a different group.

Example 2:

Our group will be $\mathbb{Z}_{11}^*$ with $\alpha = 2$

That's shorthand for $p = 11$ and $*$ as our operator

Let's generate our group from $\alpha = 2$

$2^1 = 2 \mod 11 = 2$
$2^2 = 4$ — 4
$2^3 = 8$ — 8
$2^4 = 16$ — 5
$2^5 = 32$ — 10

$2^6 = 64 \mod 11 = 9$
$2^7 = 128 = 7$
$2^8 = 256 = 3$
$2^9 = 512 = 6$
$2^{10} = 1024 = 1$

cyclic!! $2^{11} = 2048 = 2$ Back!

Every element of this group is expressable with 2

How many elements in $\mathbb{Z}_{11}^*$? $\boxed{10}$

Order of $\mathbb{Z}_{11}^*$ is 10.

Alice

Private Key: 4

Public key:

$(\alpha * \alpha * \alpha * \alpha) \mod 11$

$= 2^4 \mod 11$

$= 5 \mod 11$

Bob

Private Key: 8

Public Key: $\alpha^8 \mod 11$

$= 3 \mod 11$

Alice

$K_{AB} = 3^4 \mod 11$

$= 81 \mod 11$

$= 4 \mod 11$

Bob

$K_{AB} = 5^8 \mod 11$

$= 390{,}625 \mod 11$

$= 4 \mod 11$ ✓

Attacker finds discrete log of $\alpha^x = B \bmod 11$

$$\alpha^x = 4 \bmod 11$$
$$2^x = 4 \bmod 11$$

Now we are in trouble.

This isn't a standard log.

$$\cancel{x \log(2) = \log(4) \bmod 11}$$
$$\cancel{x = \log 4 / \log 2 \bmod 11}$$
$$\cancel{x = 2 \bmod 11}$$

WRONG!

Best method is to try every value in the table above.

As p increases in size (and is prime)

Then that table gets a lot larger.

This is hard and one-way for all $\mathbb{Z}_p^*$ where p is prime

Brute force will take on average

about $\frac{p-1}{2}$ trials. $O(p)$

So if p is about 80 bits, thats about 10^{24} tries

But since there are better attacks, typically we double to 160 bit keys.

Is solving the DLP the only solution for breaking this type of crypto?

probably not.

The Generalized D.L.P.

Given: a finite, cyclic group G with operator $\circ$
and cardinality n

$$G, \circ \text{ and } |G| = n$$

take primitive element $\alpha \in G$; and $\beta \in G$

Find x such that $\alpha^x = \beta$

$$\underbrace{\alpha \circ \alpha \circ \ldots \circ \alpha}_{x \text{ times}} = \beta$$

Key result: For some groups, this is not one-way!

An example of a group that is not?

$$\mathbb{Z}_{11}^{+}$$

when is it?

For $\mathbb{Z}_p^*$

and elliptic curves.

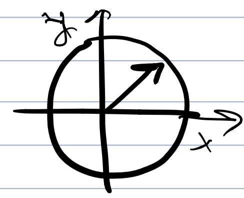
Elliptic Curve Crypto

Here is a group that is one way for the GDLP.

another

Construction is entirely engineered
Nothing natural about this.

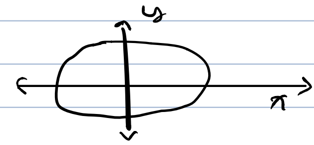
Do you recall the formula for circles?



polynomial: $x^2 + y^2 = r^2$

IF we add coefficients

$ax^2 + by^2 = c$ we get an ellipse.



There is a set of real values that are in the set of values that satisfy that equation.

the Elliptic Curve over $\mathbb{Z}_p$, $p > 3$, is the set of all pairs $(x, y) \in \mathbb{Z}_p$ that fulfill

$$y^2 \equiv x^3 + ax + b \mod p$$

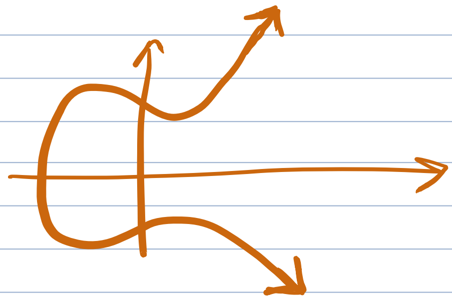
together with an imaginary point of infinity $\mathcal{O}$
where $a, b \in \mathbb{Z}_p$

and the condition that $4a^3 + 27b^2 \neq 0 \mod p$

That's a lot. Let's take it slower.

We can ignore that mod p part and just graph it!

not really the same thing
but no one is looking!



$y^2 = x^3 - 3x + 3$

The curve does not self intersect.

Elements of this Elliptic Curve group are tuples (x, y) just like points on a circle are tuples.

How do we make a group of this??

1. $a \circ b = c \in G$ the operator is closed
2. $a \circ (b \circ c) = (a \circ b) \circ c$ associativity
3. there exists an identity element $1 \in G$
   $a \circ 1 = 1 \circ a = a$ for all $a \in G$
4. for all $a \in G$, there exists an inverse a^{-1} such that
   $a \circ a^{-1} = a^{-1} \circ a = 1$
5. "Abelian" groups also have an operator such that
   $a \circ b = b \circ a$ for all $a, b \in G$ commutative

First we need an operator.
We'll call it addition, but it's not really addition.

$$P + Q = R$$

by which I mean

$$(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$$

Since we require closure, "addition" better result with R being a point on the curve as well.

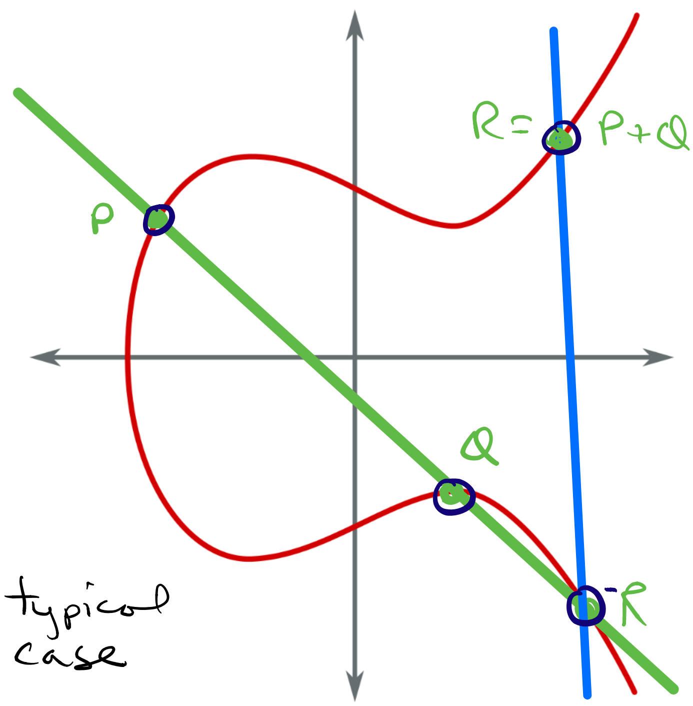
So let's define addition.

We are worried about two cases

$P+Q$ point addition (where $P \neq Q$)

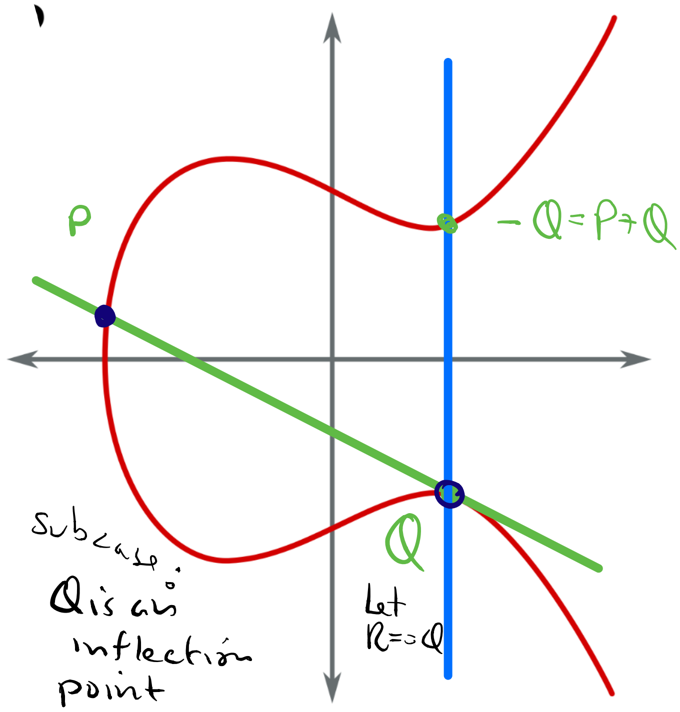
$P+P$ point doubling

Find the line from P to Q, and then $-R$ is the point that intersects that line; Find R as the reflection across x-axis.



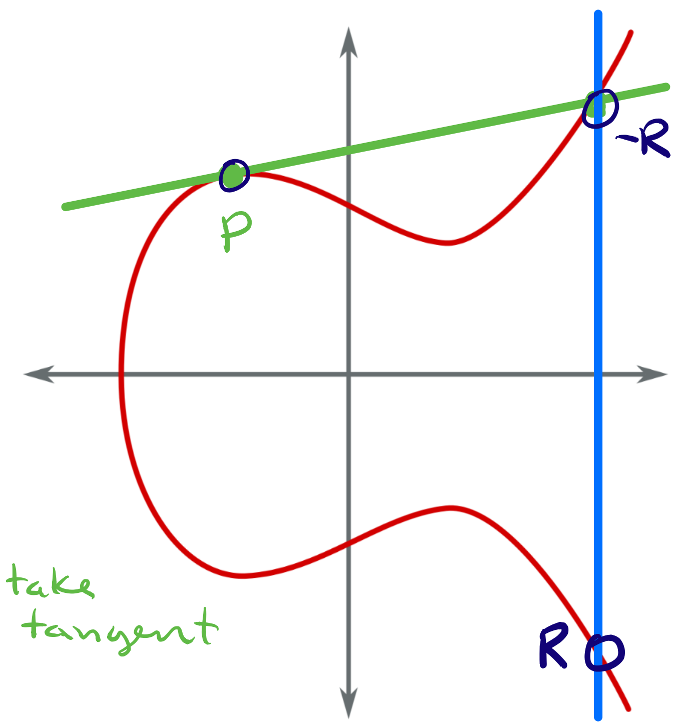
Here's the typical case.

Here's a wierd case where Since Q is at this inflection point, there is no R that is on the curve and the line. So we set R=Q.



Point Doubling P+P= ?

Here, we can't draw a line, so we just take the tangent at P, find the intersection, and mirror.



We can do these operations in mod p.

We lose the nice geometric illustration

We solve for the slope S of the line that connects P and Q.

$$P + Q = R$$

$$(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$$

$$x_3 = S^2 - x_1 - x_2 \mod p$$

$$y_3 = S(x_1 - x_3) - y_1 \mod p$$

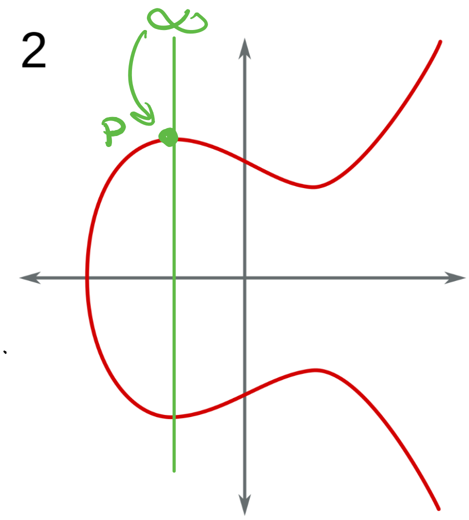
where

$$S = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} \mod p, & \text{if } P \neq Q \\[2ex] \dfrac{3x_1^2 + a}{2y_1} \mod p, & \text{if } P = Q \end{cases}$$

That's closure.

To make a group, we need an **IDENTITY** element $\mathcal{O}$ such that

$$P + \mathcal{O} = P$$



It turns out, we don't have one!!

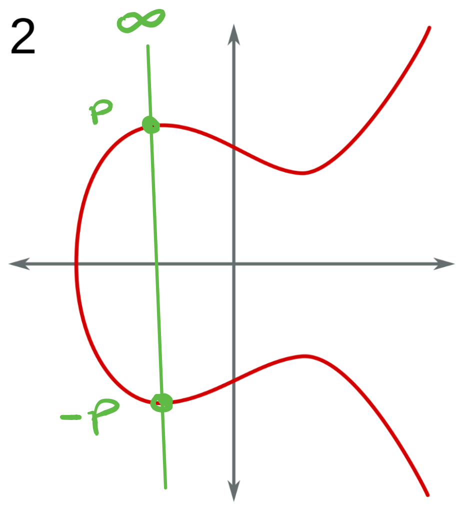
So we just define one as if it's at $+\infty$ or $-\infty$

We also need an inverse element

So that $P + (-P) = \mathcal{O}$

that's not subtraction!!

Since $\mathcal{O}$ is at ∞ then P is the reflection of $-P$.



Things are getting a little weird.

not subtraction

integer subtraction

If $P = (x_p, y_p)$ then $-P = (x_p, -y_p)$

But that's a lie. We are in mod space.

$$-P = (x_p, p - y_p \bmod p)$$

not subtraction

subtraction

For example, the inverse of $(5,16) \bmod 17$ is -1

$$= (5, -1)$$

$16(-1) \bmod 17 = 1$

Anyway, let's try an example.

Example

$E: \; y^2 \equiv x^3 + 2x + 2 \mod 17$ $\quad a=2, b=2$

Double this Point: $P = (5,1)$

$2P = (5,1) + (5,1)$

1. $s = \dfrac{3x_1^2 + a}{2y_1} = (3(5)^2 + 2)\cdot(2\cdot 1)^{-1}$

$= (75+2)(2)^{-1}$

$(77 - 17\cdot 4)\cdot 2^{-1}$

$9 \cdot 2^{-1}$

$9 \cdot 9$

$81 \quad - 17\cdot 4$

$= 13 \mod 17$

what is $2^{-1} \mod 17$?

$x \cdot 2 \mod 17 = 1$?

$9 \cdot 2 \mod 17 \overset{?}{=} 1$

$18 \mod 17 \overset{?}{=} 1$

$1 \mod 17 = 1$

yes

2. $x_3 = s^2 - x_1 - x_2$

$= 13^2 - 5 - 5$

$= 169 - 10$

$= 159 \mod 17$

$= 6 \mod 17$

3. $y_3 = s(x_1 - x_3) - y_1$

$= 13(5-6) - 1$

$= 13(-1) - 1$

$= -13 - 1$

$= -14 \mod 17$

$= 3 \mod 17$

$P + P = (6,3)$

is $(6,3)$ Really in E?

$3^2 \equiv 6^3 + 2\cdot 6 + 2 \mod 17$

$9 \equiv 216 + 12 + 2 \mod 17$

$9 \equiv 230 \mod 17$

$9 \equiv 9 \mod 17$ ✓

So let's build a crypto system

The points on an elliptic curve along with $\mathcal{O}$, and our addition operator, form a cyclic group. [unproven... but it's true]

Let's do an example to show it's cyclic

Example $E: y^2 \equiv x^3 + 2x + 2 \mod 17$

$P = (5, 1)$ Before we start.. what's $-P$? $(5, -1)$

$2P = P + P$
$3P = 2P + P$

$P = (5,1)$	$11P = (13,10)$
$2P = (6,3)$	$12P = (0,11)$
$3P = (10,6)$	$13P = (16,4)$
$4P = (3,1)$	$14P = (9,1)$
$5P = (9,16)$	$15P = (3,16)$
$6P = (16,13)$	$16P = (10,11)$
$7P = (0,6)$	$17P = (6,14)$
$8P = (13,7)$	$18P = (5,16)$
$9P = (7,6)$	$19P = \mathcal{O}$
$10P = (7,11)$	

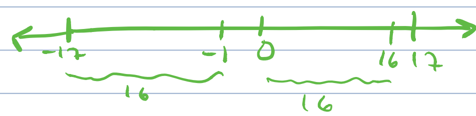
All of these follow the same math at $P+P=2P$ above.
Except $18P$ and $19P$.

At $18P = (5,16)$
$= (5,-1)$
$= -P$

why? It because of how 16 and -1 are related in mod 17.

what's $16 \mod 17$? 16

what's $-1 \mod 17$?
$(17-1) \mod 17 = 16$



and so
$19P = 18P + P$
$= -P + P$
$= \mathcal{O}$

$20P = \mathcal{O} + P = P$

$21P = P + P = 2P$

We have a cyclic group. We have generator.

We can plug this into DHKE!

One more thing to discuss:

We need to know the number of elements in the group.

Because that tells us the difficulty of breaking it.

Here's an important theorem

Given an E.C. defined as above

IT is a group with $\#E$ elements;

We can bound $\#E$ by:

$$p + 1 - 2\sqrt{p} \leq \#E \leq p + 1 + 2\sqrt{p}$$

↑ what term dominates here?

$2^{160} + 1 - \sqrt{2^{160}}$

$\approx 10^{48}$

So if we need an elliptic curve with 2^{160} elements, we need a prime of about size 2^{160}; i.e., a 160 bit number.

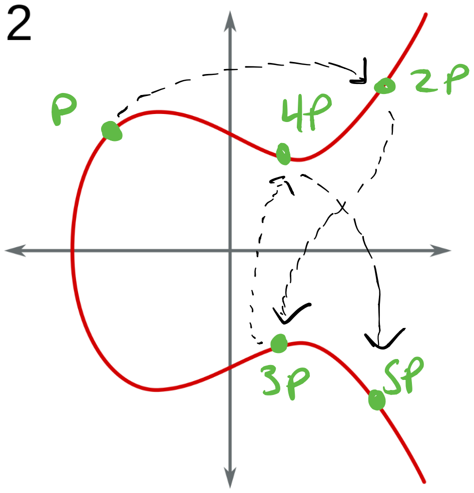
Definition of the Elliptic Curve Discrete Log Problem

Given Elliptic Curve E. Consider primitive element P
and another element T.

The DLP is finding the integer d, where $1 \leq d \leq \#E$
such that $\underbrace{P + P + \cdots + P}_{d \text{ Times}} = dP = T$

point multiplication
not integer multiplication

2



P is our generator

P, 2P, 3P, 4P, 5P, etc. $\Rightarrow$ T

Everyone knows E and P.

The private key is d. (number of hops)

The public key is $dP = T$

E.C.D.L.P.: Given T and P, find d

DHKE with Elliptic Curves

A SETUP

- choose prime p and curve E.

$$E: y^2 \equiv x^3 + ax + b \mod p$$

- choose generator $P = (x_P, y_P)$

Finding a suitable curve is difficult! people have done this for us.

B. Key Exchange

1. Alice : choose $K_{A-} = a \in \{2, 3, \ldots, \#E - 1\}$

   compute $K_{A+} = aP = A = (x_A, y_A)$

2. Bob : choose $K_{B-} = b \in \{2, 3, \ldots, \#E - 1\}$

   compute $K_{B+} = bP = B = (x_B, y_B)$

3. Alice $\to$ Bob : A
4. Bob $\to$ Alice : B
5. Alice : computes $aB = a(bP)$
6. Bob: computes $bA = b(aP)$

Since addition in E.C. groups is associative, we know that $aB = bA$

$$a(bP) = b(aP)$$

The observer must

solve for $a = \log_P A \mod p$

doing so is $O(\#E) \approx O(p)$

Example E: $y^2 \equiv x^3 + 2x + 2 \mod 17$

$\#E = 19$ and primitive $P = (5,1)$

1. Alice $K_{A-} = 3$

   $K_{A+} = 3P = (10,6)$

2. Bob $K_{B-} = 10$

   $K_{B+} = 10P = (7,11)$

3. $K_{AB} = 10(10,6)$ or $3(7,11)$

   $= (13,10)$ $= (13,10)$

   (math not shown)

tuple for a shared key??
typically, the hash of the x coordinate is used as the shared key (or 128 bits of it, etc.)

e.g. hash(13) $\Rightarrow$ key for AES.

4. Send a message to Bob
   $C = \{P\}_{K_{AB}}$

Signatures with E.C. are a bit more involved still!!

You can read about them — not that bad but this is enough for us to cover.