$y^2 \equiv x^3 + 2x + 1 \mod 7$ $\quad P=(0,6)$ $\quad Q=(0,1)$ $\quad Q=-P$

Line through P, Q. $\quad$ slope $= \frac{6-1}{0-0} = \frac{5}{0}$ div. by 0

Line is $x = 0$

$y^2 = x^3 + 2x + 1 \mod 35$ $\quad P=(28,13)$ $\quad Q=(0,1)$

Line through P, Q $\quad$ slope $= \frac{13-1}{28-0} = \frac{12}{28} = \frac{3}{7}$ div. by 7 mod 35

not coprime

$7 = \gcd(7, 35)$ $\Leftarrow$ $\Rightarrow 7^{-1}$ doesn't exist!

$7 \leftarrow N$

non-invertible run

An abelian group is a set w/ an operation which is

- associative
- have an identity
- inverses
- commutative

	$(\mathbb{Z}/p\mathbb{Z})^*$, $\times$	E, $+$
	$(f \cdot g)h = f(g \cdot h)$	$(P+Q)+R = P+(Q+R)$
	1	∞
	g^{-1}	$-P = (x, -y)$ for $P = (x, y)$
	$f \cdot g = g \cdot f$	$P+Q = Q+P$
Hard problem:	DLP Given g, g^x, find x	ECDLP (Elliptic Curve Discrete Log Problem) Given P, nP, find n.
Algorithms to attack hard problem:	Baby Step Giant Step $O(\sqrt{p})$ Birthday $O(\sqrt{p})$ Index Calculus subexp.	BSGS, Birthday $\} O(\sqrt{\#E(\mathbb{F}_p)}) \approx O(\sqrt{p})$ NO INDEX CALCULUS
Cryptographic protocols:	Diffie-Hellman El Gamal	EC Diffie-Hellman EC El Gamal

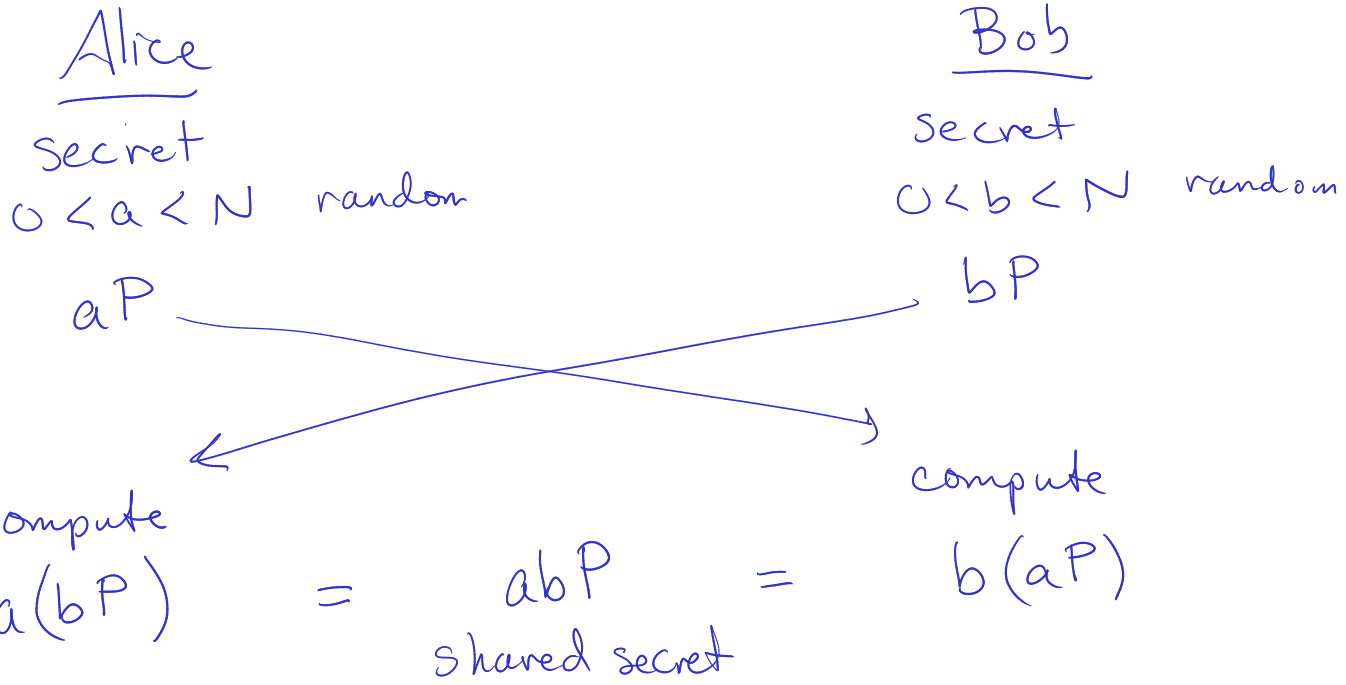
Elliptic Curve Diffie-Hellman Key Exchange

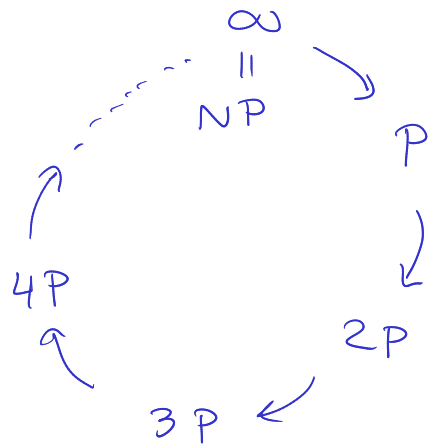
$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$

order(P) = smallest N s.t. $NP = \infty$

Public setup: $E: y^2 \equiv x^3 + bx + c$ and $P \in E(\mathbb{F}_p)$

$N = \text{order}(P)$





To use this:

① Scalar multiplication must be fast.

Successive doubling! $P \to 2P \to 4P \to 8P \to 16P$

eg. $13P = 8P + 4P + P$

(2) Discrete Log on Elliptic Curves should be hard!
It is! ☺

(3) Finding E, P for setup.
- want N large
- often want N prime

} involves math, poly time

(4) To make shared secret less structured, hash it.

El Gamal

Public setup: E over $\mathbb{F}_p$ (mod p)
$P \in E(\mathbb{F}_p)$
$N = \text{order}(P)$.

Alice

message: $M \in E(\mathbb{F}_p)$

B ⟵

Bob

Private: $0 < b < N$ random
Public: $B = bP$

Encryption:
ephemeral key pair:
$0 < k < N$ random
$K = kP$ mask = shared secret
$C = M + kB$

(K, C) ⟶

Decryption:

$$
\begin{aligned}
& C - bK \\
&= C - b(kP) \\
&= C - k(bP) \\
&= C - kB \\
&= M
\end{aligned}
$$

How to put a message on curve:

m = number

Let $x = m$

Let $\rho = x^3 + bx + c$

Hope $\rho = y^2$ in $\mathbb{F}_p$ ← find square root mod p.

So— So
- If so, then $M = (x, y)$ or $(x, -y)$
- If not, pad x, try again