Elliptic Curve Diffie-Hellmann Key Exchange

Public Set-Up: $E: y^2 \equiv x^3 + bx + c$

and point $P \in E(\mathbb{F}_p)$

$N = \text{order}(P)$ $\quad (N \cdot P = \infty)$

a, b, ab "lives" mod N

Alice

secret random

$0 < a < N$

aP

Bob

secret random

$0 < b < N$

bP

compute: $a(bP) = abP$

compute: $b(aP)$

$abP = b(aP)$

secret key

DH Problem for E.C.'s

Given aP, bP, find abP

Discrete Log Problem for E.C.'s

Given aP, find a.

Note: key = pt on curve.

Could use coordinates as secret for AES etc.

El Gamal for E.C.

Public Setup: E elliptic curve over $\mathbb{F}_p$

$P \in E(\mathbb{F}_p)$

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

Alice

message:

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

Bob

Setup Public/Private key pair:

Private (Secret): $0 < b < N$ randomly chosen

Public: $B = bP$

B ←

Encryption:

random $0 < k < N$

$S = kP$

$T = M + kB$

ciphertext (S, T) →

Decryption:

$T - bS$

$= M + kB - bkP$

$= M + kbP - bkP$

$= M$

How to put a message in text into $M \in E(\mathbb{F}_p)$?

m = number. $E: y^2 = x^3 + bx + c$

Let $x = m$

Then let $\rho = x^3 + bx + c$

If ρ is a square mod p, then let $y^2 = \rho$.

$M = (x, y)$

If not, pad/change x.

Ex.

MATH $\xrightarrow{\text{ASCII}}$ 10 09 07 11 61 04 00 (padding)

(message)

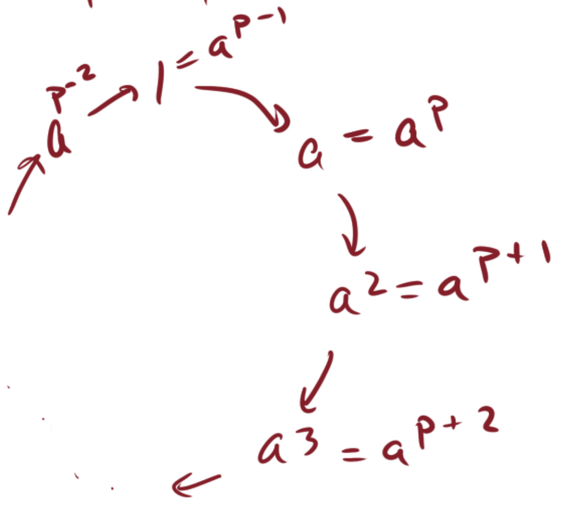
try x

$x+1$

$x+2$

Finding Square Roots mod p

$|(\mathbb{Z}/p\mathbb{Z})^*| = p-1$. Let $a \in (\mathbb{Z}/p\mathbb{Z})^*$. g = primitive root



If $p \equiv 3 \pmod 4$
then $p+1 \equiv 0 \pmod 4$.

So $a^{\frac{p+1}{4}}$ is well-defined.

and $\boxed{x = a^{\frac{p+1}{4}}}$ is a solution to $x^4 \equiv a^2 \pmod p$.

i.e. $\boxed{x^2 \equiv \pm a} \pmod p$.

Algorithm to find square root of $a \bmod p \equiv 3 \pmod 4$.

① Compute $t = a^{\frac{p+1}{4}}$.

② Case I: $t^2 = a$

We're done!

Case II: $t^2 = -a$

There's no square root!

Why can't $t^2 = -a$ and there exist $s^2 = a$?

If so, $t^2/s^2 = -1$, so $-1 = z^2$ for some z.

But $-1 = g^{\frac{p-1}{2}}$.

Then $2\,\mathrm{Lg}(z) = \frac{p-1}{2}$ is even.

But $\frac{p-1}{2}$ is odd when $p \equiv 3 \pmod 4$.

Upshot:

$p \equiv 3 (4)$ ① exactly one of $a, -a$ is a square.

EC El Gamal Digital Signature

A signature is appended to a document.

Properties:

① Signing (Alice) w/ public/private key pair

Input: Document m

Output: Signed document, ie. pair (m, sig)

(sig depends on m, public/private key pair)

② Verifying (Bob)

Input: Alice's public key
Signed message

Output: YES/VALID or NO/INVALID.

③ Key Properties: It hard to produce pairs (m, sig) that validate YES without access to Alice's private key.

"forging"