Nov24

Monday, November 23, 2020 10:22 PM

Remainder of Semester

1. No more HW.
2. **Project 2:** Elliptic Curve Crypto.
   Due: Communicate by Dec 2
   Assignment Due Dec 5 (Sat).
3. **Final Exam:** Take home. Cumulative.
   Due: Dec 17 NOON!

Elliptic Curve Cryptography

Recall

ECDLP was the problem:

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

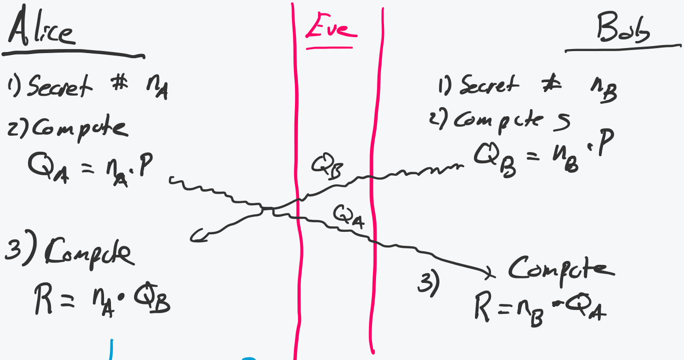
s.t. $Q = \underline{n}P = \underbrace{P + \cdots + P}_{n \text{ times}}$

Find n.

Apply this directly to cryptosystems.

Elliptic Curve Diffie Hellman Key Exchange

Alice & Bob agree on a (public) elliptic curve $E(\mathbb{F}_p)$ & a pt $P \in E(\mathbb{F}_p)$.



Alice

1) Secret # n_A
2) Compute
$Q_A = n_A \cdot P$
3) Compute
$R = n_A \cdot Q_B$

Eve

Bob

1) Secret # n_B
2) Computes
$Q_B = n_B \cdot P$
3) Compute
$R = n_B \cdot Q_A$

R a shared secret

$$n_A \cdot Q_B = n_A \cdot n_B (P) = n_B \underline{n_A} P = n_B \cdot Q_A$$

Rmk Same process as DH over $\mathbb{F}_p^*$

For Eve to solve this is for Eve to discover R, from the info Q_A & Q_B.

Def^n E an Elliptic Curve over $\mathbb{F}_p$. $P \in E(\mathbb{F}_p)$. The Elliptic Curve Diffie Hellman Problem (ECDLP) is the following

Given $n_1 \cdot P$ & $n_2 \cdot P$ find $\underline{n_1 n_2} \cdot P$

Prop

The ECDLP solves the ECDHP

Proof

Have $n_1 P$ & $n_2 P$. I ask my ECDLP Oracle to solve $Q = n_1 P$ for n_1.

Then I compute $n_1 \cdot (n_2 P) = n_1 n_2 P$

& win ∅

Remark:

Alice sends Bob $Q = (x_Q, y_Q) \in \mathbb{F}_p \times \mathbb{F}_p$.

But know

$$y_Q^2 = x_Q^3 + Ax_Q + B \quad \text{some public } A, B.$$

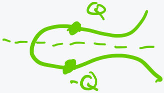
So given x_Q, only 2 values of y_Q.

↑ computed fairly easily.

① Eve learns x_Q, almost cracked it

② Alice is sending too much info.

Alternatively instead of



$$A : (x_Q, y_Q) \longmapsto B$$

Have alice send x_Q to Bob.

Bob knows $\pm Q = \pm n_A \cdot P$.

Bob computes $n_B(\pm n_A \cdot P) = \pm R = (x_R, \pm y_R)$

Example If shared secret is x_R rather than all of R, this is enough.

Message expansion halved.

Elliptic Curve Elgamal

Alice & Bob choose $E/\mathbb{F}_p$ & $P \in E(\mathbb{F}_p)$

Alice | **Eve** | **Bob**

Key Creation:

1) Secret # n_A
2) $Q_A = n_A \cdot P_A$ $\xrightarrow{Q_A}$

↑ Public key

Bob:

1) $M \in E(\mathbb{F}_p)$ message.
2) $k \in \mathbb{Z}_{>0}$ random int
3) $C_1 = kP$, $C_2 = M + kQ_A$ } cipher text

$\xleftarrow{(C_1, C_2)}$

computes

3) $C_2 - n_A \cdot C_1 = M$

Proof

$$C_2 - n_A C_1 = (M + kQ_A) - n_A k \cdot P$$

$$= M + \cancel{k n_A P} - \cancel{n_A k P} = M.$$

∅

Concerns

① Plaintexts ⟷ Points on elliptic curves?

Maybe

textToInt(message) = $\underset{\sim}{x_1}$

$P = (x_1, y_1)$ $\quad y_1^2 = \underbrace{x_1^3 + a x_1 + b}$

↑ maybe, not a square

yikes

② 4-1 message expansion.

Potential Solutions

Solve ① (Project 2).

Idea:

Use ECC (a la DH) to get a shared secret in $\mathbb{F}_p^*$. Wrap that together w/ a symmetric encryption over $\mathbb{F}_p^*$. Package it as one thing like Elgamal & voila!

⤳ solves message expansion ② as well.

Main cryptosystem of Project 2.

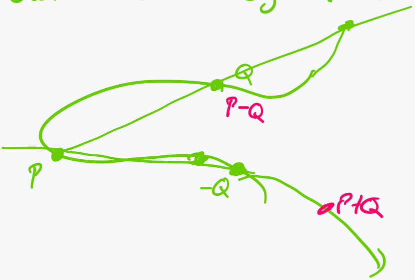
Solve ② Only send x-coord & send one extra bit.

e.g./

$$\begin{cases} 0 & \text{if } 0 \le y < \frac{1}{2}p \leftarrow \\ 1 & \text{if } \frac{1}{2}p \le y < p \leftarrow \end{cases}$$

(Does this bit help Eve a bit?)

Rmk Just x-coord elgamal is not enough.



Elliptic Curve Digital Signatures (ECDSA)

Demonstrates philosophy of using ECs to mask data in $\mathbb{F}_p$.

Notation $P \in E(\mathbb{F}_p)$. $x(P) =$ x-coord of P

$y(P) =$ y-coord P.

($P = \mathcal{O}$, both are ∞).

Setup

- Samantha signs a document d. $d^{sig.}$
- Victor verifies the signature matches.

They decide on (public) $E/\mathbb{F}_p$ and a point $Q \in E(\mathbb{F}_p)$ has large prime order q.

Key Creation

- Sam chooses a secret signing key s w/ $1 < s < q-1$
- Sam computes $V = sQ \in E(\mathbb{F}_p)$. This public verification key.

Signing a Document

never repeat.

- Document $d \in \mathbb{F}_q^*$
- Sam chooses random $e \in \mathbb{F}_q^*$.
- Computes

$$\left.\begin{aligned} \rightarrow \quad s_1 &= x(eQ) \bmod q. \\ * \quad s_2 &= (d + s s_1)e^{-1} \bmod q \end{aligned}\right\} \text{Signature}$$

Verification

$$\left.\begin{array}{l} * \ v_1 = d \cdot s_2^{-1} \mod q \\ * \ v_2 = s_1 s_2^{-1} \mod q \end{array}\right\}$$

$$R = \underline{v_1 \cdot Q + v_2 \cdot V} \in E(\mathbb{F}_p)$$

Verifies $\underline{x(R)} = s_1 \mod q$.

Proof

Observe $|Q| = q$. Then $a \equiv b \mod q$

$aQ = bQ \in E(\mathbb{F}_p)$

$$\begin{aligned} R &= v_1 Q + v_2 V \\ &= d s_2^{-1} Q + s_1 s_2^{-1} V \\ &= d s_2^{-1} Q + s_1 s_2^{-1} s Q \\ &= (d + s_1 s) s_2^{-1} Q \\ &= (e s_2) s_2^{-1} Q \\ &= eQ \end{aligned}$$

Taking x-coords says $x(R) = x(eQ)$

$= s_1$

Upshot

ECDLP more secure than DLP so use smaller #s & have better efficiency.

Lenstra's Elliptic Curve Factorization Alg

Recall Pollard's $p-1$ Algorithm

Factor $N=pq$ by finding a power a^L satisfying

$$\left.a^L \equiv 1 \bmod p \qquad a^L \not\equiv 1 \bmod q\right\} \gcd(a^L-1, N) = p$$

Fermat's Little Theorem suggests $p-1 \mid L$ but $q-1$ doesn't.

Take $L = n!$ & hope this $n!$ swallows up prime factors of $p-1$ but not those of $q-1$.

Best when $p-1$ was product of small primes.

Question

What was important about $p-1$?

⇝ Lot's of elts in $\mathbb{F}_p$ have order $p-1$

$\alpha^{p-1} \equiv 1 \bmod p$.

Doing math mod N hoping to stumble up elts of small order mod p.

Translate to Elliptic curves!

P = point on curve ⟷ $a \in \cancel{\mathbb{F}_p}\ \underline{\mathbb{Z}/n\mathbb{Z}}$

$$\begin{tikzcd} & \mathbb{Z}/n\mathbb{Z} \arrow[dl] \arrow[d, "CRT"] \\ \mathbb{F}_p & \mathbb{F}_q \end{tikzcd}$$

@ same time.

$\underline{n \cdot P}$ ⟷ a^L

We want to work with an elliptic

Curve E over $\mathbb{Z}/N\mathbb{Z}$

$\uparrow$ not prime.
what we want to factor.

$E: \quad y^2 = x^3 + Ax + B.$

$P = (a,b) \in E(\mathbb{Z}/N\mathbb{Z}) \longleftrightarrow b^2 \equiv a^3 + Aa + B \mod N$

Can we compute

$P, 2P, 3P, 4P, \ldots$?

Use algebraic rules in our E.C counting algorithm.... (try at least).

Example: $N = 187.$ $\quad E: \; y^2 = x^3 + 3x + 7$

$P = (38, 112).$

① $2 \cdot P$

$$\lambda = \frac{3x(P)^2 + A}{2y(P)} = 34 \cdot 91 \equiv 102 \mod 187$$

$$\frac{1}{2y(P)} = \frac{1}{224} \underset{\substack{\uparrow \\ \text{Ext Euc. Alg}}}{\equiv} 91 \mod 187$$

$$224x \equiv 1 \mod 187$$

$$x(2P) = \lambda^2 - 2x(P) = 10328 \equiv 43 \mod 187$$

$$y(2P) = \underline{\lambda(x(P) - x(2P)) - y(P)}$$

$$= 102(38 - 43) - 112 \equiv 126 \mod 187$$

$2P = (43, 126).$ check satisfies eqn.

② $3P = P \cdot 2P$

$$\lambda = \frac{\Delta y}{\Delta x} = \frac{y(2P) - y(P)}{x(2P) - x(P)} = \frac{14}{5} = 14 \cdot 75 \equiv 115.$$

$$\frac{1}{x(2P) - x(P)} = \frac{1}{43 - 38} = \frac{1}{5} \underset{\text{EEA}}{\equiv} 75 \bmod 187$$

$$x(3P) = \lambda^2 - x(2P) - x(P) \equiv 54$$

$$y(3P) \equiv 105 \bmod 187$$

$3P = (54, 105).$

---

③ Exercise $4P = 3P + P$

$$= 2P + 2P = 2(2P)$$

$$= (93, 64).$$

---

④ $5P = 3P + 2P$

$$\lambda = \frac{\Delta y}{\Delta x} \qquad \frac{1}{\Delta x} = \frac{1}{x(3P) - x(2P)}$$

$$= \frac{1}{54 - 43} = \frac{1}{11}$$

Do EEA to find $\frac{1}{11}$ mod 187

Find gcd$(11, 187) = 11$

Can't divide by 11...... stuck or.....

WE JUST FACTORED 187

Found $11 \mid 187$ .... $187 = 11 \cdot 17$ ✓

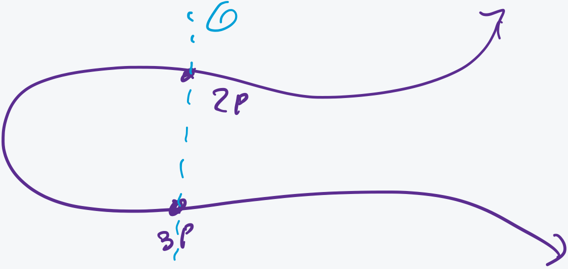
$\rightsquigarrow$ This is the idea.

What happened?

Look @ $E(\mathbb{F}_{11})$

$3P + 2P$ note $11 \mid \Delta x = x(3P) - x(2P)$

$\rightsquigarrow$ $x(3P) \equiv x(2P) \mod 11.$



$3P + 2P = \mathcal{O}$ in $E(\mathbb{F}_{11})$.

$5P = \mathcal{O}$

So $|P| = 5$ as a pt in $E(\mathbb{F}_{11})$.

$P = (38, 112) = (5, 2) \mod 11$

$5P = \mathcal{O}$

What happened is P had small order mod a prime dividing N.

↑This is directly analogous to Pollard.

Summarize

Idea

- Point on $E(\mathbb{Z}/N\mathbb{Z})$ w/ small order on $E(\mathbb{F}_p)$ for $p|N$
- Witness small order by failure of EEA
- Gives you a factor of N.