Today: Group theory review

Diffie Hellman Key Exchange

Five crypto groups: \( \mathbb{Z}_p, \mathbb{Q}_p, \mathbb{Z}_n, \mathbb{Q}_n \),

Elliptic curves

Reading: Katz-Lindell 7.8

Def: A (finite) abelian group \((G, \cdot)\) satisfies the following:

- Identity: \(1 \in G \) s.t. \( \forall a \in G \) \( a \cdot 1 = 1 \cdot a = a \)
- Inverse: \( \forall a \in G \) \( \exists b \in G \) s.t. \( a \cdot b = 1 \) \((b = a^{-1})\)
- Associativity: \( \forall a, b, c \in G \) \( a \cdot (b \cdot c) = (a \cdot b) \cdot c \)
- Commutativity: \( \forall a, b \in G \) \( a \cdot b = b \cdot a \)

Recall:

Def: Order \( (a) \) = least \( u > 0 \) s.t. \( a^u = 1 \) (in G)

Lagrange's Thm: In a finite group \( G \) of size \( t \)

\[ \forall a \in G \quad \text{order}(a) | t \]

Corollary: In a finite group \( G \) of size \( t \)

\[ \forall a \in G \quad a^t = 1 \]
Example \( \forall a \in \mathbb{Z}_p \quad a^{p-1} \equiv 1 \mod p \) (Fermat's Thm)

\( \forall a \in \mathbb{Z}_n \quad a^{\phi(n)} \equiv 1 \mod n \) (Euler's Thm)

(since \( |\mathbb{Z}_p^*| = p-1 \) & \( |\mathbb{Z}_n^*| = \phi(n) \))

Recall:
- Def: \( \langle a \rangle = \{ a^i : i \geq 0 \} \) = subgroup generated by \( a \)

Def: If \( \langle a \rangle = G \) then \( a \) is a generator of \( G \), and \( G \) is cyclic.

Claim: \( |\langle a \rangle| = \text{order}(a) \).

Exercise: In a finite abelian group \( G \) of prime order \( \forall a \in G \) if \( a \neq 1 \) then \( G \) is a generator of \( G \).

Thm: \( \mathbb{Z}_n^* \) is cyclic iff \( n \) is \( 2, 4, 2^m \) or \( 2p^m \).
Fact: If $G$ is a cyclic group of order $t$, and $g$ is a generator, then the relation \( x \mapsto g^x \) is 1-to-1 between $\{0, 1, \ldots, t-1\}$ and $G$.

\[ x \mapsto g^x \quad \text{exponentiation} \]

\[ g^x \mapsto x \quad \text{discrete logarithm (DL)} \]

- Computing discrete logarithms (the DL problem) is assumed to be hard for "well-chosen" groups. Eg. for $\mathbb{Z}_p^*$, where $p$ is a large random prime, or large random safe prime.

  Not in all groups! ($\mathbb{Z}_p^*$)

  - Fastest alg: takes time $> 2^{\log p / 3}$ sub-exp alg

- Common public-key setup:

  Public system parameters:

  \[ P = \text{large prime} \quad \text{(eg. 1024 bits)} \]

  \[ g = \text{generator of } \mathbb{Z}_p^* \]

  User: \[ sk = x \text{ random in } \{0, 1, \ldots, P-2\} \]

  \[ pk = y = g^x \mod P \]
Secrecy of $x$ follows from the DL assumption that asserts that it is hard to find discrete logarithms

\[
\text{(Appears to be roughly as hard as factoring )}
\]

\[
\text{(an integer of the same size as } p
\]

\[
\text{for both, best known alg } \approx \mathcal{O}(k^{1/3}) \text{ time)
\]

\[\text{Not a thm!}\]

- We often need to be able to represent msgs as group elements:

If $M$ is a msg space and $G$ is a group, we need an injective (1-to-1) map $f: M \rightarrow G$

such that $f(m)$ can "represent" msg $m$.

Eg., if $p > 2^k$ then we can identify $k$-bit msgs with the integers $1, 2, \ldots, 2^k \mod p$

(in $\mathbb{Z}_p^*$)

- In some groups this can be tricky.
**Diffie-Hellman Key Exchange**

**Q:** How to establish shared secret in presence of eavesdropper? (Eve is passive - only listens)

(Precurser to true public key cryptography).

- Let $G$ be a cyclic group w. generator $g$
- $G$ & $g$ fixed and public.

\[ A \quad B \]

- Alice chooses a random secret $x$ from 50,1,7,161-13
- Alice computes $g^x$
- Bob similarly chooses secret $y$ from 50,1,7,161-13
- Bob computes $g^y$

\[ g^x \quad g^y \]

Alice computes $K = (g^y)^x$

Bob computes $K = (g^x)^y$

\[ K = g^{xy} \]

- If DL hard, Eve can't compute $x$ or $y$.
  That doesn't mean she can't compute $K$!
Computational Diffie-Hellman Assumption (CDH):

Given \( g^x, g^y \) it is hard to compute \( g^{xy} \) (i.e. negligible chance to succeed).

CDH \( \Rightarrow \) Eve doesn’t learn \( K \) except w. negligible probability.

Q: Can Alice & Bob use \( K \) as a shared secret key to encrypt and/or MAC later traffic?

Eve may learn a lot of information about \( K \) (such as 200 msb’s?).

Decisional Diffie-Hellman Assumption (DDH):

Given \( g^x, g^y \) it is hard to distinguish between \( g^{xy} \) & \( g^u \) where \( u \) is random in \( \{0,1,\ldots,10^{l-1}\} \)

w.p. > \( \frac{1}{2} + \text{negl} \).

Thm: DDH \( \Rightarrow \) DH key exchange is secure.

(Eve cannot distinguish between \( K \) and a fresh random key.)
**Pf:** Follows immediately from the assumption!

Assuming DDH, we can use $k$ to encrypt and/or
MAC later.

- Don't use same $k$ for both!

  A MAC can leak enough information to break
  the enc but not enough to allow forgery,
  and vice versa.

- Use $k$ to derive 2 fresh keys: one for MAC
  & one for enc (using PRG).

**Next week:** commitment scheme & public key
encryption scheme under DL (DDH/CDH).
5 Common Groups:

1. \( \mathbb{Z}_p^* = \{0, 1, \ldots, p-2\} \) \( p \) prime

   \( \mathbb{Z}_p^* \) is always cyclic

   Often, we use \( p=2q+1 \) (\( q \) is prime) \( \Rightarrow \) \( p \) safe prime

   • Half of \( \mathbb{Z}_p^* \) are generators, the others are squares (\( \mathbb{Q}_p \)). \( \Rightarrow \) Easy to test!

   • \( \mathbb{Z}_p^* \) has a large subgroup of prime order
     (i.e. order \( q \)) \( \Rightarrow \) very useful (we will see next week)

2. \( \mathbb{Q}_p = \text{Quadratic residues (squares)} \mod \text{prime } p \)

   \( = \{\alpha^2 : \alpha \in \mathbb{Z}_p^*\} \subseteq \mathbb{Z}_p^* \)

   \( |\mathbb{Q}_p| = \frac{1}{2} |\mathbb{Z}_p^*| = \frac{p-1}{2} \) ("half of \( \mathbb{Z}_p^* \) are squares")

   \( \mathbb{Q}_p \) is cyclic: If \( \langle g \rangle = \mathbb{Z}_p^* \) then \( \langle g^2 \rangle = \mathbb{Q}_p \)

   If \( p=2q+1 \) (\( p \) is safe prime) then

   \( |\mathbb{Q}_p| = q \) \( \Rightarrow \) prime order subgroup.

   \( \Rightarrow \) Any element (other than 1) generates \( \mathbb{Q}_p \).

L.11.8
\[ \mathbb{Z}_n^* = \{ a \in \mathbb{Z}_{p-1} : \gcd(a, n) = 1 \} \quad \text{(RSA)} \]

**Def:** \( \psi(n) = |\mathbb{Z}_n^*| \)

If \( n = pq \), where \( p, q \) distinct odd primes then \( \mathbb{Z}_n^* \) is not cyclic.

\[ \mathbb{Z}_n^* \cong \mathbb{Z}_{p-1}^* \times \mathbb{Z}_{q-1}^* \]

the order of each element \( a \in \mathbb{Z}_n^* \) is \( \text{lcm}(p-1, q-1) < \frac{p-1}{2} \times \frac{q-1}{2} \)

\( Q_n = \{ a^2 : a \in \mathbb{Z}_n^* \} = \text{"squares mod } n\text{"} = \text{"quadratic residues mod } n\text{"} \)

If \( n = pq \) where \( p = 2r+1 \) safe prime \((r \text{ prime})\)
\( q = 2s+1 \) safe prime \((s \text{ prime})\)

then \( |Q_n| = r \cdot s \) & \( Q_n \) is cyclic.
Elliptic Curves

Recall: In \( \mathbb{Z}_p^* \) we have sub-exp alg for finding DL.

We would like a group \( G \) for which solving DLP takes time \( \exp(\log |G|) \) (exp. time).

Elliptic Curves!
- Very different from \( \mathbb{Z}_p^* \), \( \mathbb{Z}_n^* \), \( \mathbb{Q}_p \), \( \mathbb{Q}_m \)

- Appear in many diverse areas of mathematics:
  number theory, complex analysis, crypto, mathematical physics

[Koblitz, Miller 85]
Used in

\[ \text{Def: An elliptic curve is a curve given by an equation of the form} \]
\[ y^2 = x^3 + Ax + B \]

s.t. the discriminant
\[ \Delta = 4A^3 + 27B^2 \text{ is non-zero} \]

= the polynomial \( x^3 + Ax + B \) has distinct roots
For reasons to be explained later we also toss in an extra point $\infty$.

$$E = \{ (x, y) : y^2 = x^3 + Ax + B \} \cup \{ \infty \}.$$ 

The coordinates can be in any field: $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \text{GF}[p]$ used in crypto!

$$E(q) = \{ (x, y) \in \text{GF}[q]^2 : y^2 = x^3 + Ax + B \pmod{q} \} \cup \{ \infty \}$$

$A, B \in \text{GF}[q]$.

Claim: $E(q)$ is a finite group.

**How is the operation defined?** (coming up...)

- Best known alg that solves DLP takes time $\sim \sqrt{q}$ (exponential).

- Clearly $|E(q)| < 2q + 1$

**Thm** [Hasse, 1922] $|E(q)| = q + 1 + t$

$$- 2\sqrt{q} \leq t \leq 2\sqrt{q}$$
Note: We would expect $|E(q)| \approx q + 1$

if $x^3 + Ax + B$ acted "randomly":

$\sim \frac{1}{2}$ the values are squares, each of which
has two square roots.

Fact: $|E(q)|$ can be computed "efficiently" (time $< (\log q)^6$)

This is important since for crypto we want $E(q)$ to
contain a subgroup of large prime order.

Group operation: Geometrically

\[
\begin{align*}
\text{identity} &= \infty \\
\forall Q \in E(q) &\quad Q + \infty = Q \\
Q + (-Q) &= \infty
\end{align*}
\]

Addition of 2 points $P, Q$ is performed by

drawing the line connecting $P, Q$, finding its 3rd
intersection with $E(g)$, denoted by $R$, and letting

$$p + q = -r$$

- $p + p = ?$ Draw the tangent line through $p$, and continue as before. This can be done over any finite field!

Let $P = (x_1, y_1)$, $Q = (x_2, y_2)$, $-R = p + q = (x_3, y_3)$

The line through $P, Q$ can be written as

$$y = \frac{y_2 - y_1}{x_2 - x_1} (x - x_1) + y_1 = \lambda x + \nu$$

To find $R$ we need to find the intersection of

$$E(g) : \quad y^2 = x^3 + ax + b$$

$$L : \quad y = \lambda x + \nu$$

$$= x^3 + ax + b - (\lambda x + \nu)^2 =$$

$$= (x - x_1) \cdot (x - x_2) \cdot (x - x_3)$$

$$= x^3 - (x_1 + x_2 + x_3) x^2 + (x_1 x_2 + x_1 x_3 + x_2 x_3) x - x_1 x_2 x_3$$

$$\Rightarrow \quad \lambda^2 = x_1 + x_2 + x_3$$

$$\Rightarrow \quad x_3 = \lambda^2 - x_1 - x_2$$

$$y_3 = \lambda x_3 + \nu$$
Note: If \( x_1 = x_2 \), \( y_1 \neq y_2 \), \( P + Q = \infty \) (vertical line)

If \( P = Q \) & \( y = 0 \), \( P + Q = \infty \) (vertical tangent)

* If \( P = Q \) \& \( y \neq 0 \), \( \lambda = \frac{-3x_1^2 + A}{2y_1} \) (tangent)

\[
\begin{align*}
x_3 &= \lambda^2 - 2x_1 \\
y_3 &= \lambda(x_3 - x_1) + y_1
\end{align*}
\]

Thm:

identity → 1. \( P + \infty = \infty + P = P \) \( \forall P \in E(q) \)

inverse → 2. \( P + (-P) = \infty \) \( \forall P \in E(q) \)

associativity → 3. \( P + (Q + R) = (P + Q) + R \) \( \forall P, Q, R \in E(q) \)

commutativity → 4. \( P + Q = Q + P \) \( \forall P, Q \in E(q) \)

\[\Rightarrow (E, +) \text{ is a finite commutative group.}\]

DLP seems to be very hard (requiring \( \sim |E|^{1/2} \) steps) for "well-chosen" \( E(q) \) (see NIST standard curves)

* Some elliptic curves admit "bilinear maps" enabling wonderful crypto (stay tuned!)