3/17/2021
Lec 19

Today:

- Recap: Diffie-Hellman key Exchange
- Review: Group Theory
- Begin public key cryptography (?)

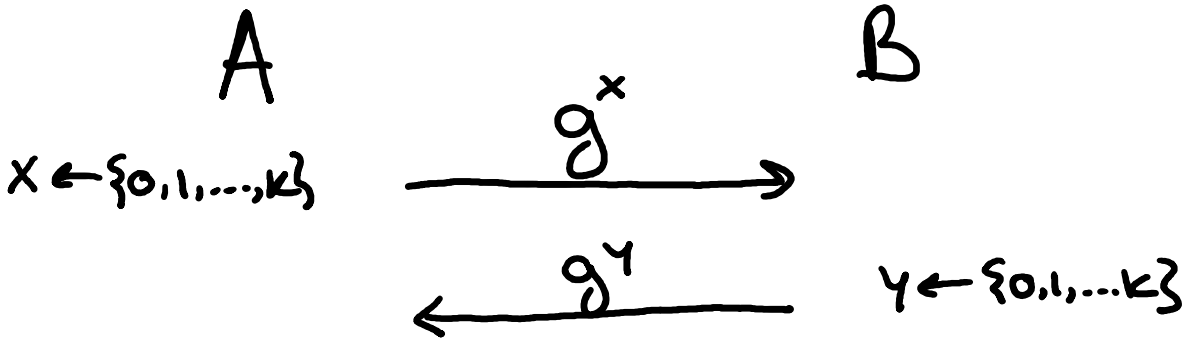
Announcements:

- Post project idea by today (if you haven't done so)
- This Friday: Add/drop date
- No class on Monday

Recall: Diffie-Helman Key Exchange:

Fix finite group $G = \{1, g, g^2, \ldots, g^k\}$

g ← generator



$$K = g^{x \cdot y}$$

Decisional Diffie Hellman

Thm: DH key exchange is secure under the DDH Assumption:

$$(g^x, g^y, g^{xy}) \approx (g^x, g^y, g^u)$$

$$x, y, u \leftarrow \{0,1,\ldots,K\}$$

What is a group, and for which groups do we beleive the DDH assumption holds?

Group Theory

Def: A group $(G, \cdot)$ consists of a set of elements G and an operation $\cdot : G \times G \longrightarrow G$ s.t.

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

A group is commutative if $\forall a,b \in G \quad a \cdot b = b \cdot a$

All the groups we will talk about are commutative.

Common groups used in cryptography:

$\mathbb{Z}_p^* = \left(\{1, \ldots, p-1\}, \cdot \right)$ where $\cdot$ is multiplication mod p.

(p: prime)

$\mathbb{Z}_n^* = \left(\{a \in \{1, \ldots, n\} : GCD(a,n) = 1\} \right.$ where $\cdot$ is multiplication mod n.

(n: often)

$n = p \cdot q$, p, q are primes (n is called RSA number)

Other common groups: Q_p, Q_n, Elliptic curves.

Def: The **order** of a group is the number of elements in the group.

$$|\mathbb{Z}_p^*| = p-1$$

$$|\mathbb{Z}_n^*| = n - p - q + 1 = (p-1)(q-1) \triangleq \varphi(n)$$

Euler's function

Note: The order of $\mathbb{Z}_n^*$ is hard to compute without the prime factorization p, q.

This is the basis of the RSA crypto system.

* For crypto applications we often need a group of **prime order**.

needed for DDH assumption to hold (as we shall see).

Note: $\mathbb{Z}_p^*$ & $\mathbb{Z}_n^*$ are **not** of prime order.

Generating prime order group:

Def: A prime p is a **safe** prime if $q = \frac{p-1}{2}$ is a prime.

$$Q_p = \{a^2 : a \in \mathbb{Z}_p^*\}$$ ← quadratic residues mod p

$$|Q_p| = \frac{p-1}{2} = q$$ ← prime!

This is the case since the mapping $x \longmapsto x^2$ is a 2-to-1 mapping $a, \underbrace{-a}_{\| \; p-a} \longmapsto a^2$

(Follows from the fact that GF[p] is a field, and from the fundamental Thm of Algebra that says that a deg 2 poly has at most 2 roots)

We believe that DDH holds in Q_p assuming p is a safe prime.

Typically, we use groups of very large size 2^κ κ = security parameter.

Common Operations: Exponentiation & inverse.

How do we do these operations efficiently? ← In time poly(k).

Exponentiation: Repeated Squaring

Given a, b compute a^b as follows

$$a^b = \begin{cases} 1 & \text{if } b=0 \\ (a^{b/2})^2 & \text{if } b \text{ even} \\ a \cdot a^{b-1} & \text{if } b \text{ odd} \end{cases}$$

Requires $\leq 2 \log b$ multiplications

$\approx \Theta(k^3)$ time (a few miliseconds for 1024 bit integer)

Computing Inverses:

Fermat's Little Thm: $\forall$ prime p $\forall a \in \mathbb{Z}_p^*$ $a^{p-1} = 1$

Corollary: $a^{-1} = a^{p-2}$ ← can be computed efficiently by repeated squaring

How do we generate a large random k-bit prime?

needed for RSA group $\mathbb{Z}_n^*$

Using Fermat's Little Thm:

Choose a random k-bit number $n \in \{0,1\}^k$.

Check if it is prime by choosing a random $a \leftarrow \{1,\dots,n-1\}$ and checking if $a^{n-1} = 1$.

If so, output n as the prime number.

O.w. try again.

This works because:

① Primes are dense: There are about $\frac{2^k}{\ln 2^k}$ k-bit prime numbers ← Prime Number Thm

② The test $a^{p-1} = 1$ work w.h.p. for <u>random</u> p

This test does not work for adversarially chosen p.

* Miller & Rabin have a primality that work w.h.p. <u>for every</u> p
* Agrawal-Kayal-Saxena 2002 gave a <u>deterministic</u> primality test.

To generate a safe prime:

Choose a random $n \leftarrow \{0,1\}^k$

and test if n is prime & if $\frac{n-1}{2}$ is prime

Order of Elements & Generators

Def: $\forall$ finite group G $\forall a \in G$

$$\text{order}(a) = \text{minimum } u \in \mathbb{N} \text{ s.t. } a^u = 1 \text{ in } G$$

$$\mathbb{N} = \{1,2,3,\ldots\}$$

Lagrange's Thm: $\forall$ finite group G $\forall a \in G$

$$a^{|G|} = 1$$

Generalization of Fermat's Little Thm

Corollary: $\forall$ finite group G $\forall a \in G$

$$\text{order}(a) \mid |G|$$

Proof: If $\text{order}(a) = u$ st. $|G| = \alpha u + \beta$

for $\beta \in \{1,2,\ldots,u-1\}$ then

$$1 = a^{|G|} = a^{\alpha u + \beta} = (a^u)^\alpha \cdot a^\beta = a^\beta$$

Contradicting the fact that the order of a is u.

Notation: $\forall$ finite group G $\forall a \in G$

$$\langle a \rangle = \{ a, a^2, \ldots, a^{\text{order}(a)} \}$$

subgroup generated by a.

Def: If $\langle a \rangle = G$ then we say that a is a generator of G.

Def: A finite group G is cyclic if

$\exists a \in G$ st. $\langle a \rangle = G$

Thm: $\mathbb{Z}_n^*$ is cyclic iff n is

$2, 4, p^m$ or $2 \cdot p^m$

Claim: A prime order group G has no non-trivial subgroups ↖ beyond G & $\{1\}$

Pf: Suppose it has a non trivial subgroup $G' \subseteq G$. Let $a \in G' \setminus \{1\}$.

Then $\langle a \rangle \subseteq G'$.

By the corollary above $\text{order}(a) \mid |G|$.

But since $|G|$ prime & $a \neq 1$ it must be the case that $\text{order}(a) = |G|$, and thus, $\langle a \rangle = G$, contradiction.

When we use a cyclic group G often we use it with a generator $g \in G$ so that

$f_g : \{1, \ldots, |G|\} \longrightarrow G$ is a bijection.

$x \longmapsto g^x$ ← Exponentiation

$g^x \longmapsto x$ ← Discrete Log Problem which is assumed to be hard.

For $\mathbb{Z}_p^*$ fastest Discrete Log (DL) alg' runs in time $\approx 2^{\log p^{1/3}}$ ← sub-exponential

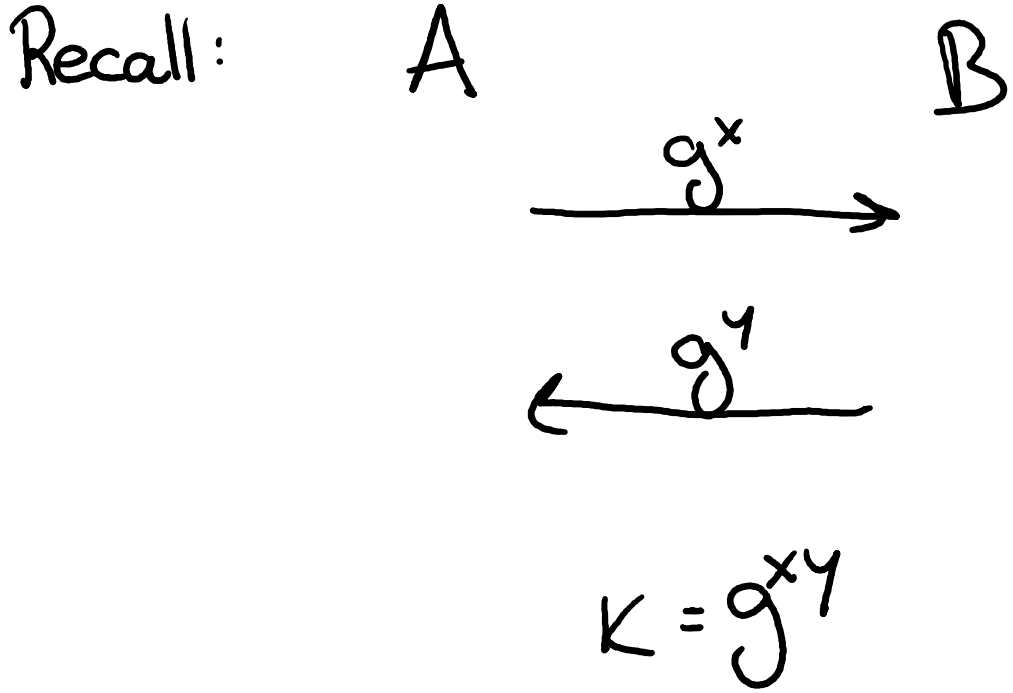
* For elliptic curves the fastest DL alg' runs in exponential time. ← This is why elliptic curves are more efficient in practice.

Going back to DH Key Exchange:

We need to choose a cyclic group G w. generator g s.t. DDH holds:

$$(g^x, g^y, g^{xy}) \cong (g^x, g^y, g^u)$$

Recall:



How do we choose G:

How do we choose g:

Does DDH holds in $\mathbb{Z}_p^*$?

Teaser for next week:

Public key encryption:

$PK = g^x$ for random $x \leftarrow \{1, \ldots, |G|\}$

$SK = x$

Mask (a la one-time pad)

$$Enc(\underbrace{g^x}_{PK}, \underbrace{m}_{msg}) : g^y, m \cdot g^{xy}$$

$y \leftarrow \{1, \ldots, |G|\}$ random.

The fact that g^{xy} is a good mask follows directly from DDH

$Dec(x, g^y, m \cdot g^{xy})$: Compute g^{xy} and unmask.

This is El-Gamal Encryption scheme