COMS BC3262: Introduction to Cryptography

Lecture 15: Discrete Log, CDH, and DDH

March 25, 2026

Office Hours

Office hours:

- **Eysa**: Mondays 3-5, Milstein 512
- **Mark**: Tuesdays 6:30-8:30, Milstein 503

This week there may be an extra review session on Friday to review topics from the first half of the course (tentatively 2pm, location TBD)

- Completely optional but highly recommended for anyone who feels iffy on anything we covered before spring break
- Hosted by one of last semester's intro crypto TAs

Today’s Lecture

- Cyclic Groups
- Discrete Log Assumption
- Collision-resistant hash functions from DL

Cyclic Groups

Cyclic Groups

Definition: Let $\mathbb{G}$ be a finite group of order m and let $g \in \mathbb{G}$. Then

- $\langle g \rangle = \{g^0, g^1, g^2, \ldots\}$
- The order of g (denoted $\mathrm{ord}(g)$) is the smallest $0 < i \leq m$ such that $g^i = 1$

Facts:

- $\langle g \rangle$ is a subgroup of $\mathbb{G}$ (called “the subgroup generated by g”)
- $\langle g \rangle = \{g^0, g^1, g^2, \ldots, g^{\mathrm{ord}(g)-1}\}$
- $g^x = g^y$ if and only if $x = y \bmod m$
- The order of g divides the order of $\mathbb{G}$, i.e., $\mathrm{ord}(g) \mid m$

Cyclic Groups

Example: $\mathbb{Z}_{15}^{*} = \{1,2,4,7,8,11,13,14\}, \ |\mathbb{Z}_{15}^{*}| = 8$

Cyclic Groups

Example: $\mathbb{Z}_{15}^* = \{1,2,4,7,8,11,13,14\}$, $|\mathbb{Z}_{15}^*| = 8$

- $\langle 2 \rangle =$

Cyclic Groups

Example: $\mathbb{Z}_{15}^{*} = \{1,2,4,7,8,11,13,14\}$, $|\mathbb{Z}_{15}^{*}| = 8$

- $\langle 2 \rangle = \{1,2,4,8\}$

Cyclic Groups

Example: $\mathbb{Z}_{15}^* = \{1,2,4,7,8,11,13,14\}$, $|\mathbb{Z}_{15}^*| = 8$

- $\langle 2 \rangle = \{1,2,4,8\}$
- $\langle 7 \rangle =$

Cyclic Groups

Example: $\mathbb{Z}_{15}^* = \{1,2,4,7,8,11,13,14\}$, $|\mathbb{Z}_{15}^*| = 8$

- $\langle 2 \rangle = \{1,2,4,8\}$
- $\langle 7 \rangle = \{1,7,4,13\}$

Cyclic Groups

Example: $\mathbb{Z}_{15}^* = \{1,2,4,7,8,11,13,14\}$, $|\mathbb{Z}_{15}^*| = 8$

- $\langle 2 \rangle = \{1,2,4,8\}$
- $\langle 7 \rangle = \{1,7,4,13\}$
- $\langle 4 \rangle =$

Cyclic Groups

Example: $\mathbb{Z}_{15}^* = \{1,2,4,7,8,11,13,14\}$, $|\mathbb{Z}_{15}^*| = 8$

- $\langle 2 \rangle = \{1,2,4,8\}$
- $\langle 7 \rangle = \{1,7,4,13\}$
- $\langle 4 \rangle = \{1,4\}$

Cyclic Groups

Example: $\mathbb{Z}_{15}^* = \{1,2,4,7,8,11,13,14\}$, $|\mathbb{Z}_{15}^*| = 8$

- $\langle 2 \rangle = \{1,2,4,8\}$
- $\langle 7 \rangle = \{1,7,4,13\}$
- $\langle 4 \rangle = \{1,4\}$
- $\langle 11 \rangle =$

Cyclic Groups

Example: $\mathbb{Z}_{15}^* = \{1,2,4,7,8,11,13,14\}$, $|\mathbb{Z}_{15}^*| = 8$

- $\langle 2 \rangle = \{1,2,4,8\}$
- $\langle 7 \rangle = \{1,7,4,13\}$
- $\langle 4 \rangle = \{1,4\}$
- $\langle 11 \rangle = \{1,11\}$

Cyclic Groups

Definition: A group $\mathbb{G}$ is cyclic if there exists $g \in \mathbb{G}$ such that $\mathbb{G} = \langle g \rangle$. In this case, g is called a generator of the group

- $(\mathbb{Z}_N, +)$ is cyclic with generator 1

Cyclic Groups

Definition: A group $\mathbb{G}$ is cyclic if there exists $g \in \mathbb{G}$ such that $\mathbb{G} = \langle g \rangle$. In this case, g is called a generator of the group

- $(\mathbb{Z}_N, +)$ is cyclic with generator 1

Theorem: A group $\mathbb{G}$ with prime order is cyclic and every $g \in \mathbb{G} \backslash \{1\}$ is a generator

Theorem: If p is prime then $(\mathbb{Z}_p^*, \cdot)$ is cyclic

- Note: $\mathbb{Z}_p^*$ is *not* a prime order group (unless $p = 3$) since $p - 1$ isn't prime. Not every element in $\mathbb{Z}_p^* \backslash \{1\}$ is necessarily a generator either.

Cyclic Groups

Theorem: There is an efficient randomized algorithm that on input 1^n outputs a random n-bit prime p, together with a random generator $g \in \mathbb{Z}_p^*$

We will not go over the proof for this, but it is worth knowing that there is an efficient algorithm for sampling a cyclic group and generator

Cyclic Groups

Consider $(\mathbb{Z}_p^*, \cdot)$ for a prime p. This is a cyclic group for some g:

$$\mathbb{Z}_q^* = \{1,\ldots,p-1\}$$

Cyclic Groups

Consider $(\mathbb{Z}_p^*, \cdot)$ for a prime p. This is a cyclic group for some g:

$$\mathbb{Z}_q^* = \{1,\ldots,p-1\} = \{g^1, g^2, \ldots, g^{p-1}\}$$

Cyclic Groups

Consider $(\mathbb{Z}_p^*, \cdot)$ for a prime p. This is a cyclic group for some g:

$$\mathbb{Z}_q^* = \{1,\ldots,p-1\} = \{g^1, g^2, \ldots, g^{p-1}\} = \{g^0, g^1, \ldots, g^{p-2}\}$$

Cyclic Groups

Consider $(\mathbb{Z}_p^*, \cdot)$ for a prime p. This is a cyclic group for some g:

$$\mathbb{Z}_q^* = \{1,\ldots,p-1\} = \{g^1, g^2, \ldots, g^{p-1}\} = \{g^0, g^1, \ldots, g^{p-2}\} = \langle g \rangle$$

Cyclic Groups

Consider $(\mathbb{Z}_p^*, \cdot)$ for a prime p. This is a cyclic group for some g:

$$\mathbb{Z}_q^* = \{1, \ldots, p-1\} = \{g^1, g^2, \ldots, g^{p-1}\} = \{g^0, g^1, \ldots, g^{p-2}\} = \langle g \rangle$$

Note that this group is isomorphic to $(\mathbb{Z}_{p-1}, +)$

- Can define bijection $f : \mathbb{Z}_{p-1} \to \mathbb{Z}_p^*$ as $f(x) = g^x \mod p$ (for a generator g)
  - $f(0) = g^0 = g^{p-1} = 1 \mod p$
  - $f(1) = g^1, \ldots$

Cyclic Groups

Claim: Let $\mathbb{G}$ be a cyclic group of order m, and let g be a generator. Then the mapping $f : \mathbb{Z}_m \to \mathbb{G}$ defined by $f(x) = g^x$ is an isomorphism

Cyclic Groups

Mathematically $(\mathbb{Z}_p^*, \cdot)$ and $(\mathbb{Z}_{p-1}, +)$ are the same. But computationally they're not necessarily!

- While $f(x) = g^x \bmod p$ is efficiently computable, the inverse f^{-1} is believed not to be!

- This is known as the "Discrete log assumption" (DLA) for $\mathbb{Z}_p^*$

  - Note that this is an *assumption*

    - For some groups we believe this to be true, for others we don't

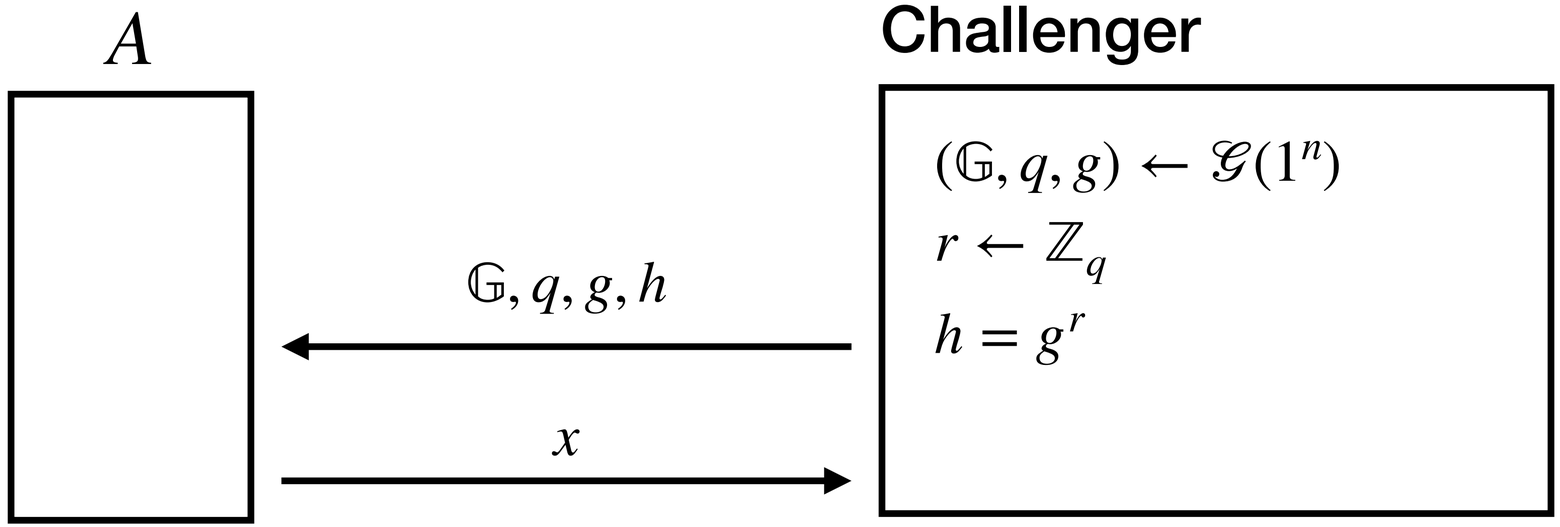
Discrete Log Assumption

The Discrete Logarithm Assumption

- Let $\mathbb{G}$ be a cyclic group of order q (i.e., $|G| = q$) and let g be a generator
  - In other words, $\mathbb{G} = \{g^0, g^1, g^2, \ldots, g^{q-1}\}$
- For every $h \in \mathbb{G}$ there exists $x \in \mathbb{Z}_q$ such that $h = g^x$
  - x is called the discrete log of h with respect to g

The Discrete Logarithm Assumption

Let $\mathcal{G}$ be a PPT algorithm that on input 1^n outputs $(\mathbb{G}, q, g)$, where $\mathbb{G}$ is a cyclic group of order q that is generated by g.



$$\mathsf{DLA}_{A,\mathcal{G}}(n) = \begin{cases} 1 & g^x = h \\ 0 & \text{otherwise} \end{cases}$$

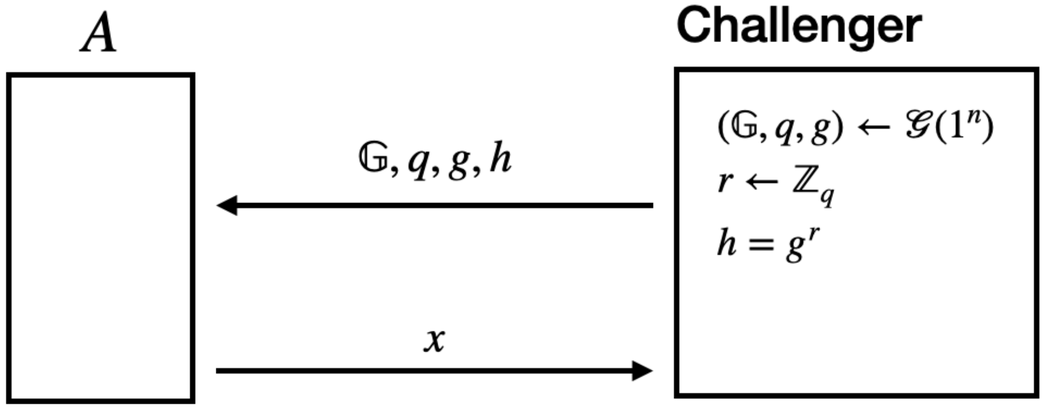
The Discrete Logarithm Assumption

Let $\mathcal{G}$ be a PPT algorithm that on input 1^n outputs $(\mathbb{G}, q, g)$, where $\mathbb{G}$ is a cyclic group of order q that is generated by g.

Definition:

The Discrete Log Assumption holds with respect to $\mathcal{G}$ if for all PPT adversaries A there exists a negligible function $\mathsf{negl}(\cdot)$ such that

$$\Pr[\mathsf{DLA}_{A,\mathcal{G}}(n) = 1] \leq \mathsf{negl}(n)$$



$$\mathsf{DLA}_{A,\mathcal{G}}(n) = \begin{cases} 1 & g^x = h \\ 0 & \text{otherwise} \end{cases}$$

The Discrete Logarithm Assumption

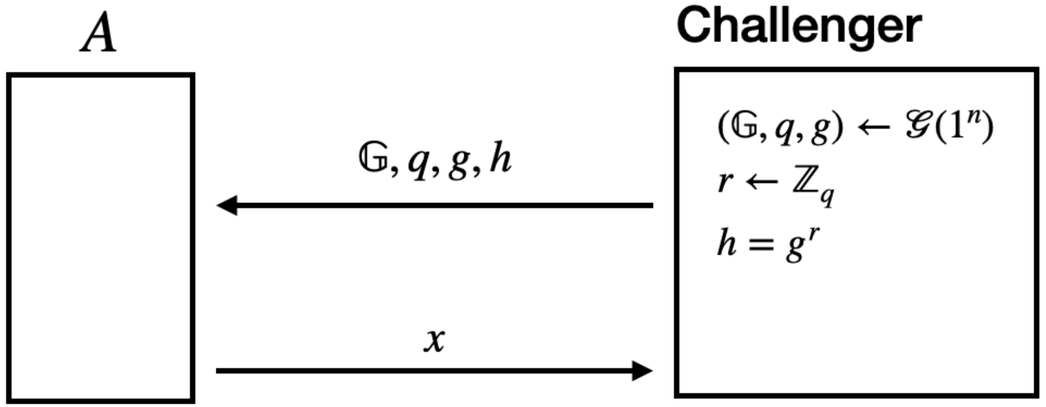
Let $\mathcal{G}$ be a PPT algorithm that on input 1^n outputs $(\mathbb{G}, q, g)$, where $\mathbb{G}$ is a cyclic group of order q that is generated by g.

Definition:

The Discrete Log Assumption holds with respect to $\mathcal{G}$ if for all PPT adversaries A there exists a negligible function $\text{negl}(\cdot)$ such that

$\Pr[\text{DL}$

Why is this defined "with respect to $\mathcal{G}$"?



$$\text{DLA}_{A,\mathcal{G}}(n) = \begin{cases} 1 & g^x = h \\ 0 & \text{otherwise} \end{cases}$$

The Discrete Logarithm Assumption

Do we think this assumption hold for all groups?

Example: Consider the (multiplicative) group $\mathbb{Z}_{13}^* = \langle 2 \rangle$

- What is the discrete log of 11 with respect to 2?
  - That is, find x such that $2^x = 11 \mod 13$?

Example: Consider the (additive) group $\mathbb{Z}_{13} = \langle 1 \rangle$

- What is the discrete log of 11 with respect to 1?

The Discrete Logarithm Assumption

Do we think this assumption hold for all groups?

Example: Consider the (multiplicative) group $\mathbb{Z}_{13}^* = \langle 2 \rangle$

- What is the discrete log of 11 with respect to 2?
  - That is, find x such that $2^x = 11 \mod 13$?

Example: Consider the (additive) group $\mathbb{Z}_{13} = \langle 1 \rangle$

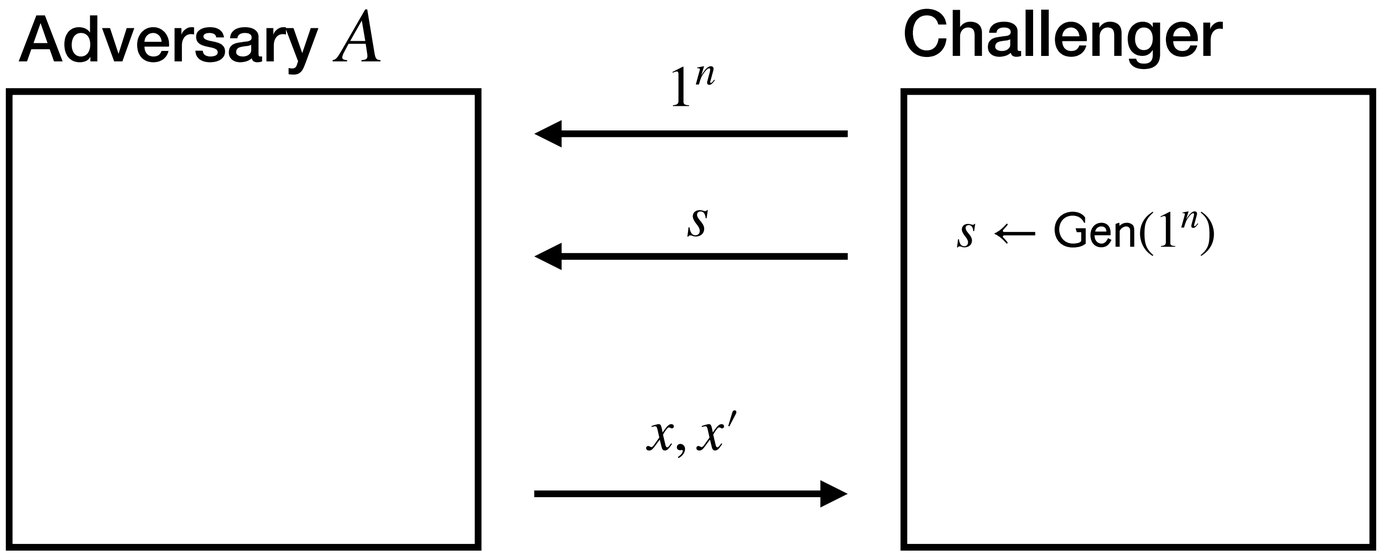
- What is the discrete log of 11 with respect to 1?

Notice that computing discrete log is easy in certain groups!

CRHF from DL

Recall: CRHF Security

Given $\Phi = (\mathsf{Gen}, H)$ and an adversary A, consider the experiment $\mathsf{HashColl}_{\Phi,A}(n)$:



$$\mathsf{HashColl}_{\Phi,A}(n) = \begin{cases} 1 & H^s(x) = H^s(x') \text{ and } x \neq x' \\ 0 & \text{otherwise} \end{cases}$$

CRHF based on DLA

Given $\mathcal{G}$, construct $\Pi = (\mathsf{Gen}, H)$ as follows:

- **Key generation**: On input 1^n, run $(\mathbb{G}, q, g) \leftarrow \mathcal{G}(1^n)$ and sample $h \leftarrow \mathbb{G}$. Output the seed as $s = (\mathbb{G}, q, g, h)$.

- **Evaluation**: On input s and $x = (x_1, x_2) \in \mathbb{Z}_q^2$, output $g^{x_1} h^{x_2} \in \mathbb{G}$

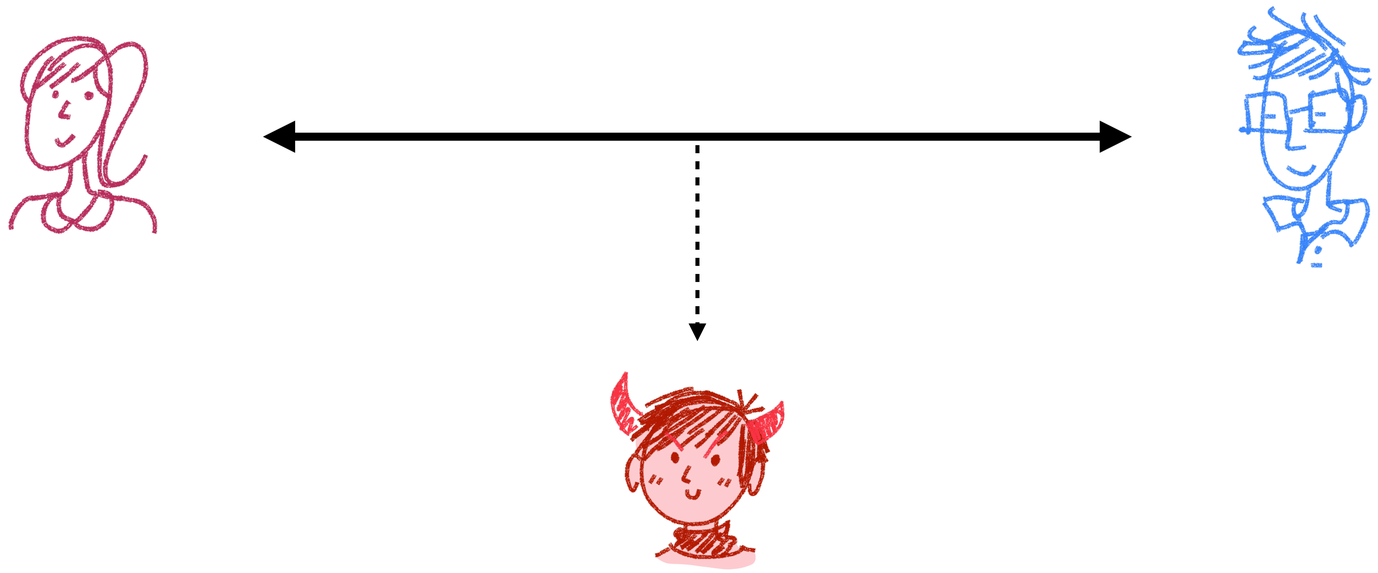
Theorem: If the discrete log assumption holds relative to $\mathcal{G}$, then Π is collision-resistant.

Diffie-Hellman Key Agreement/ Key Exchange

Key Agreement (KA)/Key Exchange (KE)

Alice and Bob don’t have an existing shared secret key.

Can they communicate over a public channel to agree on a secret key?



Diffie-Hellman Key Exchange

$(\mathbb{G}, q, g) \leftarrow \mathcal{G}(1^n)$

$x \leftarrow \mathbb{Z}_q$

$h_a = g^x$

Diffie-Hellman Key Exchange

$(\mathbb{G}, q, g) \leftarrow \mathcal{G}(1^n)$

$x \leftarrow \mathbb{Z}_q$

$h_a = g^x$

$(\mathbb{G}, q, g),\ h_a$ →

Diffie-Hellman Key Exchange

$(\mathbb{G}, q, g) \leftarrow \mathcal{G}(1^n)$

$x \leftarrow \mathbb{Z}_q$

$h_a = g^x$

$(\mathbb{G}, q, g),\ h_a$ →

$y \leftarrow \mathbb{Z}_q$

$h_b = g^y$

Diffie-Hellman Key Exchange

$(\mathbb{G}, q, g) \leftarrow \mathcal{G}(1^n)$

$x \leftarrow \mathbb{Z}_q$

$h_a = g^x$

$(\mathbb{G}, q, g),\ h_a$ →

$y \leftarrow \mathbb{Z}_q$

$h_b = g^y$

← h_b

Diffie-Hellman Key Exchange

$(\mathbb{G}, q, g) \leftarrow \mathcal{G}(1^n)$

$x \leftarrow \mathbb{Z}_q$

$h_a = g^x$

$(\mathbb{G}, q, g),\ h_a$ →

$y \leftarrow \mathbb{Z}_q$

$h_b = g^y$

← h_b

$k = (h_b)^x$

$k = (h_a)^y$

Diffie-Hellman Key Exchange

$(\mathbb{G}, q, g) \leftarrow \mathcal{G}(1^n)$

$x \leftarrow \mathbb{Z}_q$

$h_a = g^x$

$(\mathbb{G}, q, g),\ h_a$ →

← h_b

$y \leftarrow \mathbb{Z}_q$

$h_b = g^y$

$k = (h_b)^x$

$k = (h_a)^y$

Correctness: Both output the same k:

$$(h_b)^x = (g^y)^x = g^{xy} = (g^x)^y = (h_a)^y$$

Diffie-Hellman Key Exchange

$(\mathbb{G}, q, g) \leftarrow \mathcal{G}(1^n)$

$x \leftarrow \mathbb{Z}_q$

$h_a = g^x$

$(\mathbb{G}, q, g),\ h_a$ →

← h_b

$y \leftarrow \mathbb{Z}_q$

$h_b = g^y$

$k = (h_b)^x$

$k = (h_a)^y$

Security: Just looking at the messages, Eve should not be able to figure out k

Diffie-Hellman Key Exchange

Are we able to prove security just from the discrete log assumption?

$(\mathbb{G}, q, g) \leftarrow \mathcal{G}(1^n)$

$x \leftarrow \mathbb{Z}_q$

$h_a = g^x$

$(\mathbb{G}, q, g),\ h_a$

h_b

$y \leftarrow \mathbb{Z}_q$

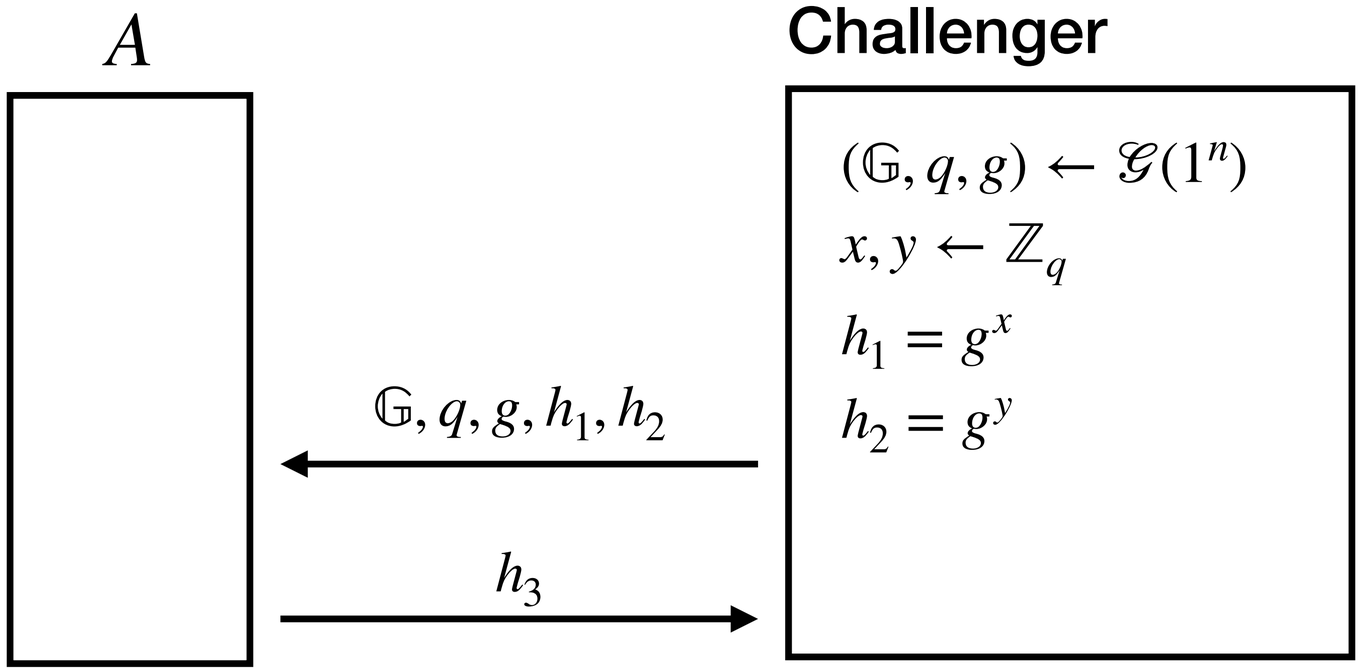
$h_b = g^y$

$k = (h_b)^x$

$k = (h_a)^y$

Security: Just looking at the messages, Eve should not be able to figure out k

Computational Diffie-Hellman Assumption (CDH)



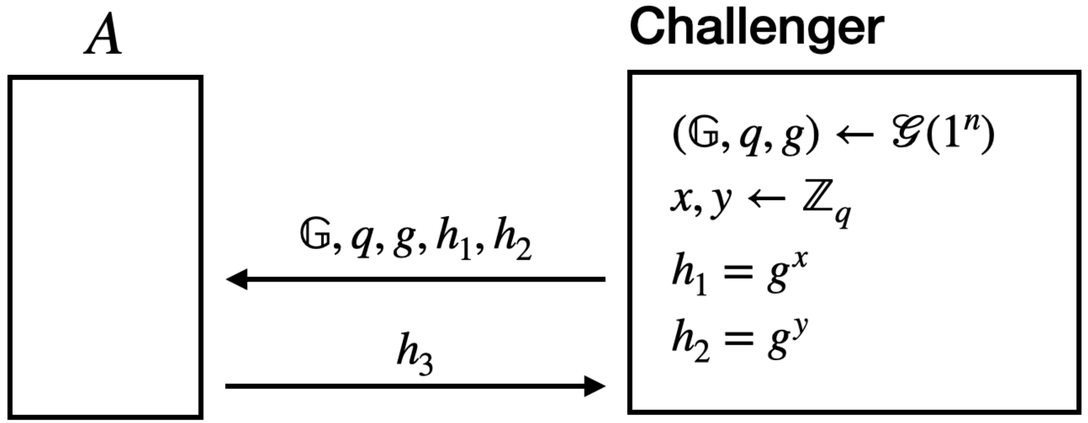
$$\mathsf{CDH}_{A,\mathcal{G}}(n) = \begin{cases} 1 & g^{xy} = h_3 \\ 0 & \text{otherwise} \end{cases}$$

Computational Diffie-Hellman Assumption (CDH)

Definition:

The Computational Diffie-Hellman Assumption (CDH) holds with respect to $\mathcal{G}$ if for all PPT A there exists a negligible function such that

$$\Pr[\mathsf{CDH}_{A,\mathcal{G}}(n) = 1] \leq \mathsf{negl}(n)$$



$$\mathsf{CDH}_{A,\mathcal{G}}(n) = \begin{cases} 1 & g^{xy} = h_3 \\ 0 & \text{otherwise} \end{cases}$$

Decisional Diffie-Hellman Assumption (DDH)

CDH is a search problem: It is hard to find g^{xy} (for uniformly distributed x, y)

DDH is a decision problem: It is hard to distinguish g^{xy} from a random group element

Definition: Decisional DH (DDH) holds with respect to $\mathcal{G}$ if for every PPT A there exists a negligible function s.t.

$$\left| \Pr_{(\mathbb{G},q,g)\leftarrow\mathcal{G}(1^n),\ x,y\leftarrow\mathbb{Z}_q}[A(\mathbb{G},q,g,g^x,g^y,g^{xy})=1] - \Pr_{(\mathbb{G},q,g)\leftarrow\mathcal{G}(1^n),\ x,y,z\leftarrow\mathbb{Z}_q}[A(\mathbb{G},q,g,g^x,g^y,g^z)=1] \right| \leq \mathsf{negl}(n)$$

PRG from DDH?

Informally, DDH says given $\mathbb{G}, q, g, g^x, g^y$, no PPT adversary can distinguish between g^{xy} and a random group element g^z

Can we use this to construct a PRG?

$$G(a, b) = (g^a, g^b, g^{ab})$$

I leave this as an exercise to the reader to reason about :)

DL vs CDH vs DDH

- **Discrete log assumption**: Given g^x, it is hard to find x
- **Computational DH**: Given g^x, g^y, it is hard to find g^{xy}
- **Decisional DH**: Given g^x, g^y, h, it is hard to tell if $h = g^{xy}$ or if h is random

What are the relationships between each of these assumptions?

Do certain assumptions imply others?

DL vs CDH vs DDH

- **Discrete log assumption**: Given g^x, it is hard to find x
- **Computational DH**: Given g^x, g^y, it is hard to find g^{xy}
- **Decisional DH**: Given g^x, g^y, h, it is hard to tell if $h = g^{xy}$ or if h is random

$$\text{DDH} \implies \text{CDH} \implies \text{DL}$$