CS 6260
Number-theoretic primitives

Discrete-log related problems

- Let $G$ be a cyclic group and let $m = |G|$. The discrete logarithm function $\text{DLog}_{G,a}: G \to \mathbb{Z}_m$ takes $a \in G$ and returns $i \in \mathbb{Z}_m$ such that $g^i = a$.

- There are several computational problems related to this function:
  - Discrete-logarithm (DL) problem
  - Computational Diffie-Hellman (CDH) problem
  - Decisional Diffie-Hellman (DDH) problem

<table>
<thead>
<tr>
<th>Problem</th>
<th>Given</th>
<th>Figure out</th>
</tr>
</thead>
<tbody>
<tr>
<td>Discrete logarithm (DL)</td>
<td>$g^x$</td>
<td>$x$</td>
</tr>
<tr>
<td>Computational Diffie-Hellman (CDH)</td>
<td>$g^x, g^y$</td>
<td>$g^{xy}$</td>
</tr>
<tr>
<td>Decisional Diffie-Hellman (DDH)</td>
<td>$g^x, g^y, g^z$</td>
<td>$1$ if $z \equiv xy \pmod{</td>
</tr>
</tbody>
</table>

DL problem

- Def. Let $G$ be a cyclic group and let $m = |G|$. Let $g$ be a generator. Consider the following experiment associated with an adversary $A$.
  - Experiment $\text{Exp}^{\text{DL}}_{G,a}(A)$
    - $x \leftarrow \mathbb{Z}_m$; $X \leftarrow g^x$
    - $\pi \leftarrow A(X)$
    - If $g^\pi = X$ then return 1 else return 0
  - The $\text{dl}$-advantage of $A$ is defined as
    - $\text{Adv}^{\text{dl}}_{G,a}(A) = \Pr[\text{Exp}^{\text{dl}}_{G,a}(A) = 1]$
  - The discrete logarithm problem is said to be hard in $G$ if the $\text{dl}$-advantage of any adversary with reasonable resources is small.

- As no encryption scheme besides the OneTimePad is unconditionally secure, we need to find some building blocks - hard problems (assumptions) to base security of our new encryption schemes on.

- Block ciphers and their PRF security is not an option since now we don’t have shared keys in the public-key (asymmetric-key) setting.

- Let’s consider the discrete log related problems and the RSA problem.
CDH

- **Def.** Let $G$ be a cyclic group of order $m$. Let $g$ be a generator. Consider the following experiment associated with an adversary $A$.
  - Experiment $\text{Exp}^{\text{cdh}}_{G,g}(A)$
    - $x \leftarrow \mathbb{Z}_m$; $y \leftarrow \mathbb{Z}_m$
    - $X \leftarrow g^x$; $Y \leftarrow g^y$
    - $Z \leftarrow A(X,Y)$
    - If $Z = g^{xy}$ then return 1 else return 0
  - The cdh-advantage of $A$ is defined as
    $$\text{Adv}^{\text{cdh}}_{G,g}(A) = \Pr[\text{Exp}^{\text{cdh}}_{G,g}(A) = 1]$$
  - The computational Diffie-Hellman (CDH) problem is said to be hard in $G$ if the cdh-advantage of any adversary with reasonable resources is small.

DDH

- **Def.** Let $G$ be a cyclic group of order $m$. Let $g$ be a generator. Consider the following experiments associated with an adversary $A$.
  - Experiment $\text{Exp}^{\text{ddh-1}}_{G,g}(A)$
    - $x \leftarrow \mathbb{Z}_m$
    - $y \leftarrow \mathbb{Z}_m$
    - $z \leftarrow x+y \mod m$
    - $X \leftarrow g^x$; $Y \leftarrow g^y$; $Z \leftarrow g^z$
    - $d \leftarrow A(X,Y,Z)$
    - Return $d$
  - Experiment $\text{Exp}^{\text{ddh-0}}_{G,g}(A)$
    - $x \leftarrow \mathbb{Z}_m$
    - $y \leftarrow \mathbb{Z}_m$
    - $z \leftarrow \mathbb{Z}_m$
    - $X \leftarrow g^x$; $Y \leftarrow g^y$; $Z \leftarrow g^z$
    - $d \leftarrow A(X,Y,Z)$
    - Return $d$
  - The cdh-advantage of $A$ is defined as
    $$\text{Adv}^{\text{ddh}}_{G,g}(A) = \Pr[\text{Exp}^{\text{ddh-1}}_{G,g}(A) = 1] - \Pr[\text{Exp}^{\text{ddh-0}}_{G,g}(A) = 1]$$
  - The decisional Diffie-Hellman (DDH) problem is said to be hard in $G$ if the dhh-advantage of any adversary with reasonable resources is small.

Relations between problems

- Fix a group and a generator
  - Can solve $\text{DL}$ $\Rightarrow$ Can solve $\text{CDH}$ $\Rightarrow$ Can solve $\text{DDH}$
  - DDH is hard $\Rightarrow$ CDH is hard $\Rightarrow$ DL is hard

- The computational complexity of the problems depend on the choice of a group.

- For most groups there is an algorithm that solves the DL problem in $O(|G|^{1/2})$
- Let’s consider $G = \mathbb{Z}_p^*$ for a prime $p$.
  - **Claim.** [DDH is easy]. Let $p \geq 3$ be a prime, let $G = \mathbb{Z}_p^*$ and let $g$ be a generator of $G$. Then there is an adversary $A$, with running time $O(|p|^3)$ such that
    $$\text{Adv}^{\text{ddh}}_{G,g}(A) = \frac{1}{2}$$
• **Proof.** The idea is to compute and analyze the Legendre symbols of the inputs.

• Adversary $A(X, Y, Z)$
  - If $J_p(X) = 1$ or $J_p(Y) = 1$
    - Then $s \leftarrow 1$ Else $s \leftarrow -1$
  - If $J_p(Z) = s$ then return $1$ else return $0$

We claim that

\[
\Pr\left[\text{Exp}_G^{ddh^{-1}}(A) = 1\right] = 1
\]

\[
\Pr\left[\text{Exp}_G^{ddh-0}(A) = 1\right] = \frac{1}{2}
\]

Subtracting and noting that computing the Legendre symbol takes cubic time in $|p|$ (computed via exponentiation) we get the statement.

• **Proof.**

  - The best algorithm to solve the CDH problem in $\mathbb{Z}_p^*$ is (seems to be) by solving the DL problem.
  - The (seemingly) best algorithm to solve the DL problem is the GNFS (General Number Field Sieve) that runs
    \[
    O(\exp(C+o(1))\cdot \ln(p)^{1/3} \cdot (\ln \ln(p))^{2/3})
    \]
    where $C \approx 1.92$.
  - If the prime factorization of order of the group is known: $p - 1 = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$, the the DL problem can be solved in time in the order of $\sum_{i=1}^{n} \alpha_i \cdot (\sqrt{p_i} + |p|)$
  - Thus if we want the DL problem to be hard, then at least one prime factor needs to be large. E.g. $p=2q+1$, where $q$ is a large prime.

• **We often want the DDH problem to be hard.**

  - The DDH problem is believed to be hard in several groups, e.g.
    - $\text{QR}(\mathbb{Z}_p^*)$ - the subgroup of quadratic residues of $\mathbb{Z}_p^*$ where $p=2q+1$, $p,q$, are primes. It’s a cyclic group of prime order.