

## CS 6260 Number-theoretic primitives

- 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.

### Discrete-log related problems

- Let  $\mathbf{G}$  be a cyclic group and let  $m = |\mathbf{G}|$ . The discrete logarithm function  $\text{DLog}_{\mathbf{G},g}(a): \mathbf{G} \rightarrow \mathbf{Z}_m$  takes  $a \in \mathbf{G}$  and returns  $i \in \mathbf{Z}_m$  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

Problem	Given	Figure out
Discrete logarithm (DL)	$g^x$	$x$
Computational Diffie-Hellman (CDH)	$g^x, g^y$	$g^{xy}$
Decisional Diffie-Hellman (DDH)	$g^x, g^y, g^z$	Is $z \equiv xy \pmod{ \mathbf{G} }$ ?

### DL problem

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

## CDH

- Def. Let  $\mathbf{G}$  be a cyclic group of order  $m$ . Let  $g$  be a generator. Consider the following experiment associated with an adversary  $A$ .

Experiment  $\text{Exp}_{G,g}^{\text{cdh}}(A)$

- $x \xleftarrow{\$} \mathbf{Z}_m; y \xleftarrow{\$} \mathbf{Z}_m$
- $X \leftarrow g^x; Y \leftarrow g^y$
- $Z \leftarrow A(X, Y)$
- If  $Z = g^{xy}$  then return 1 else return 0
- The cdh-advantage of  $A$  is defined as

$$\text{Adv}_{G,g}^{\text{cdh}}(A) = \Pr[\text{Exp}_{G,g}^{\text{cdh}}(A) = 1]$$

- The computational Diffie-Hellman (CDH) problem is said to be hard in  $\mathbf{G}$  if the cdh-advantage of any adversary with reasonable resources is small.

## DDH

- Def. Let  $\mathbf{G}$  be a cyclic group of order  $m$ . Let  $g$  be a generator. Consider the following experiments associated with an adversary  $A$ .

Experiment  $\text{Exp}_{G,g}^{\text{ddh-1}}(A)$

- $x \xleftarrow{\$} \mathbf{Z}_m$
- $y \xleftarrow{\$} \mathbf{Z}_m$
- $z \leftarrow xy \bmod m$
- $X \leftarrow g^x; Y \leftarrow g^y; Z \leftarrow g^z$
- $d \leftarrow A(X, Y, Z)$
- Return  $d$

Experiment  $\text{Exp}_{G,g}^{\text{ddh-0}}(A)$

- $x \xleftarrow{\$} \mathbf{Z}_m$
- $y \xleftarrow{\$} \mathbf{Z}_m$
- $z \xleftarrow{\$} \mathbf{Z}_m$
- $X \leftarrow g^x; Y \leftarrow g^y; Z \leftarrow g^z$
- $d \leftarrow A(X, Y, Z)$
- Return  $d$

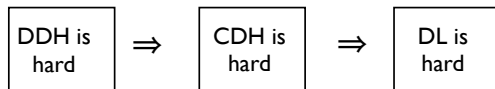
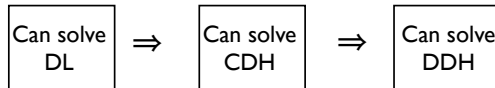
- The cdh-advantage of  $A$  is defined as

$$\text{Adv}_{G,g}^{\text{ddh}}(A) = \Pr[\text{Exp}_{G,g}^{\text{ddh-1}}(A) = 1] - \Pr[\text{Exp}_{G,g}^{\text{ddh-0}}(A) = 1]$$

- The decisional Diffie-Hellman (DDH) problem is said to be hard in  $\mathbf{G}$  if the ddh-advantage of any adversary with reasonable resources is small.

## Relations between problems

- Fix a group and a generator



- 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  $\mathbf{G} = \mathbf{Z}_p^*$  for a prime  $p$ .

- Claim. [DDH is easy]. Let  $p \geq 3$  be a prime, let  $\mathbf{G} = \mathbf{Z}_p^*$ , and let  $g$  be a generator of  $\mathbf{G}$ . Then there is an adversary  $A$ , with running time  $O(|p|^3)$  such that

$$\text{Adv}_{G,g}^{\text{ddh}}(A) = \frac{1}{2}$$

- **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

$$\Pr [\mathbf{Exp}_{G,g}^{\text{ddh-1}}(A) = 1] = 1$$

$$\Pr [\mathbf{Exp}_{G,g}^{\text{ddh-0}}(A) = 1] = \frac{1}{2}$$

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

- The best algorithm to solve the CDH problem in  $\mathbf{Z}_p^*$  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

$$O(e^{(C+o(1)) \cdot \ln(p)^{1/3} \cdot (\ln \ln(p))^{2/3}})$$

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.
  - $\text{QR}(\mathbf{Z}_p^*)$  -the subgroup of quadratic residues of  $\mathbf{Z}_p^*$  where  $p=2q+1$ ,  $p, q$ , are primes. It's a cyclic group of prime order.