# CSE 107 Discussion 2/21

## Activity 1: Additive Diffie-Hellman

In lecture we saw the Diffie-Hellman key exchange protocol: There is a public group $\mathbf{Z}_p^*$ for a prime $p$, and a public generator $g$ of $\mathbf{Z}_p^*$. Alice and Bob proceed according to:

1. Alice chooses secret $x \xleftarrow{\$} \mathbf{Z}_{p-1}$ and Bob chooses secret $y \xleftarrow{\$} \mathbf{Z}_{p-1}$.
2. Alice computes public $X \leftarrow g^x \bmod p$ and Bob computes public $Y \leftarrow g^y \bmod p$.
3. $X$ and $Y$ are sent over a public channel, so that Alice and Bob know both.
4. Now Alice and Bob can both compute the shared secret $g^{xy} \bmod p$. Alice computes $Y^x \bmod p$ and Bob computes $X^y \bmod p$.

The *Computational Diffie-Hellman* (CDH) problem says that an eavesdropper only knowing $X, Y$ cannot efficiently compute $g^{xy}$.

Let's consider a variant of the above protocol, which we call *Additive Diffie-Hellman*. Only Step (4) is changed: the shared secret will now be $g^{x+y}$ instead of $g^{xy}$.

**(a)** Can Alice and Bob still agree on a shared secret in Step (4)? What does Alice compute, and what does Bob?

**(b)** Is additive DH secure against an eavesdropper who only knows $X, Y$? Why or why not?

## Activity 2: Easy vs hard operations

Stepping back to a more general question, which of the following operations can be done efficiently, and which are hard? Let $p$ be a prime and $g$ a generator of $\mathbf{Z}_p^*$.

**(i)** Given $a, b \in \mathbf{Z}_{p-1}$ compute $a + b \bmod (p-1)$

**(ii)** Given $A, B, C \in \mathbf{Z}_p^*$ compute $A \cdot B \cdot C \bmod p$

**(iii)** Given $D \in \mathbf{Z}_p^*$ compute $D^{-1} \bmod p$

**(iv)** Given $g^a, g^b$ for $a, b \in \mathbf{Z}_{p-1}$, compute $g^{ab} \bmod p$

**(v)** Given $b, g^a, g^b$ for $a, b \in \mathbf{Z}_{p-1}$, compute $g^{ab} \bmod p$

**(vi)** Given $b, g^a, g^b$ for $a, b \in \mathbf{Z}_{p-1}$, compute $a \bmod (p-1)$

**(vii)** Given $g^a, g^b$ for $a, b \in \mathbf{Z}_{p-1}$, compute $(a + b) \bmod (p-1)$

**(viii)** Given $g^a, g^b$ for $a, b \in \mathbf{Z}_{p-1}$, compute $g^{a+b} \bmod p$

**Activity 3: Exponentiation mod 10**

Without using a calculator, what is the ones place of $3^{4445}$? (In other words, what is $3^{4445}$ mod 10?) Hint: write out $3^1$ mod 10, $3^2$ mod 10, $3^3$ mod 10, and so on until you find a pattern.

Can you come up with a fast way to solve this problem for any exponent $3^n$?

**Activity 4: Fun with groups!**

The integers $\mathbf{Z}$ under addition form a group. The operation, called *addition* is written as $a + b$. The identity element is 0, because $0 + x = x$ for all $x$. The inverse of $x$ is $-x$: $x + -x = 0$ for all $x \in \mathbf{Z}$. Repeatedly applying the operation to an element with itself $n$ times has a special name, multiplication, and is written $x + x + \ldots + x = n \cdot x$.

The nonzero real numbers $\mathbf{R}^*$ under multiplication form a group. The operation, called *multiplication* is written as $a \cdot b$. The identity element is 1, because $1 \cdot x = x$ for all $x$. The inverse of $x$ is $\frac{1}{x}$: $x \cdot \frac{1}{x} = 1$ for all $x \in \mathbf{R}^*$. Repeatedly applying the operation to an element with itself $n$ times has a special name, exponentiation, and is written $x \cdot x \cdot \ldots \cdot x = x^n$.

For each of the following groups, answer the following questions:

- What is the identity element?
- What is the *order* of the group, i.e., how many elements does the group have?
- Is there a special name for repeatedly applying the operation $n$ times?
- What happens if you repeatedly apply the operation to an element $n$ times, when $n$ is the order of the group?

1. $(\{0,1\}, \oplus)$
2. $(\{0,1\}^k, \oplus)$
3. $(\mathbf{Z}_5, +)$
4. $\mathbf{Z}_5^*$
5. $\mathbf{Z}_{10}^*$