Lecture 8: Intro to Asymmetric Crypto

Viet Tung Hoang
1. Motivation: Key Exchange

2. Number Theory Basics

3. Diffie-Hellman Assumptions
Secret Key Exchange

Alice and Bob:
- Initially share no information
- Communicate in the presence of Eve

Goal: Derive a **common** secret key $K$ that Eve knows nothing about
Secret Key Exchange

Key exchange is a very important problem
You use it several times every day

How to build a secret-key exchange protocol?
Symmetric crypto existed for thousands of years, but nobody figured out how to build one.

In 1976, Diffie and Hellman proposed one
Basic Diffie-Hellman Key Exchange

Public param: a large prime $p$, a number $g$ called a primitive root mod $p$.

Let $S = \{0, 1, \ldots, p - 2\}$

In practice, means 2048-bit

$x \leftarrow S$

$x \leftarrow g^x \mod p$

$y \leftarrow S$

$Y \leftarrow g^y \mod p$

$K \leftarrow Y^x \mod p$

$K \leftarrow X^y \mod p$

Question: Why do Alice and Bob have the same key?
DH Key Exchange: Questions

What does it mean to be a primitive root mod $p$?
Why can’t Eve compute the secret key?

…
1. Motivation: Key Exchange

2. Number Theory Basics

3. Diffie-Hellman Assumptions
Some Notation

For \( n \in \{1, 2, 3, \ldots \} \), define

\[
\mathbb{Z}_n = \{0, 1, \ldots, n - 1\}
\]

\[
\mathbb{Z}_n^* = \{ t \in \mathbb{Z}_n \mid \gcd(t, n) = 1 \}\]

\[
\varphi(n) = |\mathbb{Z}_n^*|\]

**Example:** \( n = 14 \)

\[
\mathbb{Z}_{14} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13\}
\]

\[
\mathbb{Z}_{14}^* = \{1, 3, 5, 9, 11, 13\}\]

\[
\varphi(14) = 6
\]

**Example:** prime \( p \)

\[
\mathbb{Z}_p^* = \{1, 2, \ldots, p - 1\}\]

\[
\varphi(p) = p - 1
\]
An Observation

Consider $n = 14$

$3^0 \mod 14 = 1$

$3^1 \mod 14 = 3$

$3^2 \mod 14 = 9$

$3^3 \mod 14 = 13$

$3^4 \mod 14 = 11$

$3^5 \mod 14 = 5$
An Observation

Consider $n = 14$

$9^0 \mod 14 = 1$
$9^1 \mod 14 = 9$
$9^2 \mod 14 = 11$

Cycle length = 3
The Common Trait

Cycle length varies, but is always a divisor of \( \varphi(n) \)

Walking \( \varphi(n) \) steps in the cycle will always lead to the starting point
Euler’s Theorem

**Theorem:** For any \( a \in \mathbb{Z}_n^* \),

\[
a^{\varphi(n)} \equiv 1 \pmod{n}
\]

**Fermat’s Little Theorem:** For any prime \( p \) and any \( a \in \mathbb{Z}_p^* \),

\[
a^{p-1} \equiv 1 \pmod{p}
\]

**Corollary:** If \( a \in \mathbb{Z}_p^* \), then \( a^x \equiv a^{x \mod (p-1)} \pmod{p} \)
Generators and Cyclic Groups

Let \( g \in \mathbb{Z}_n^* \)

Define \( \langle g \rangle_n = \{g^i \mod n \mid i = 0, 1, 2, \ldots\} \) as the cyclic group mod \( n \) generated by \( g \)

Examples:

\( n = 12, g = 11, \langle g \rangle_n = \{1, 11\} \)

\( n = 5, g = 2, \langle g \rangle_n = \{1, 2, 3, 4\} \)

Write \( \langle g \rangle = \{g^i \mid i = 0, 1, 2, \ldots\} \) for an unspecified cyclic group generated by \( g \)
Primitive Roots

If \( \langle g \rangle_n = \mathbb{Z}_n^* \) then we say that \( g \) is a primitive root mod \( n \)

**Theorem:** For any prime \( p \), there exist primitive roots mod \( p \)
Legendre symbol: For a prime $p$ and $a \in \mathbb{Z}_p^*$, define

$$\left( \frac{a}{p} \right) = \begin{cases} 
1 & \text{if there is some integer } t \text{ such that } a \equiv t^2 \pmod{p} \\
-1 & \text{otherwise}
\end{cases}$$

Example: $\left( \frac{2}{7} \right) = 1$ because $2 = 3^2 \pmod{7}$

Quadratic Residue group: For a prime $p$, define $\text{QR}_p = \left\{ a : \left( \frac{a}{p} \right) = 1 \right\}$

Example: $\text{QR}_7 = \{1, 2, 4\}$
Theorem: If $g$ is a primitive root mod $p$ then

$$\left( \frac{g^t \mod p}{p} \right) = \text{parity}(t) = \begin{cases} 1 & \text{if } t \text{ even} \\ -1 & \text{if } t \text{ odd} \end{cases}$$

$QR_p$ is a cyclic group generated by $g^2$
Fast Computation of Legendre Symbol

\[ x = a^{(p-1)/2} \] satisfies \[ x^2 \equiv 1 \pmod{p} \Rightarrow x \equiv \pm 1 \pmod{p} \]

Legendre’s Theorem:

\[
\left( \frac{a}{p} \right) = a^{(p-1)/2} \pmod{p}
\]

Take \(O(\log(p))\) multiplications if we use iterated squaring
Proof Sketch for Legendre’s Theorem

Let $g$ be a primitive root mod $p$ and let $a = g^t \mod p$

$$a^{(p-1)/2} \mod p = g^{t(p-1)/2} \mod p,$$ which is 1 only if $t$ is even.

Walking $t/2$ cycle length will end up at the original position only if $t$ is even.
Agenda

1. Motivation: Key Exchange

2. Number Theory Basics

3. Diffie-Hellman Assumptions
Review of DH Key Exchange

Public param: a large cyclic group $\mathbb{G}$ whose generator is $g$

Let $S = \{0, 1, \ldots, |\mathbb{G}| - 1\}$

$$\mathbb{G} = \{g^i \mid i \in S\}$$
Decisional DH Assumption

\[ x, y \leftarrow \{0, 1, \ldots, |G| - 1\} \]

**Rand**

\[ X \leftarrow g^x, Y \leftarrow g^y, K \leftarrow \$ G \]

**Real**

\[ X \leftarrow g^x, Y \leftarrow g^y, K \leftarrow g^{xy} \]

Random key

Real key in DH key exchange

\[ (X, Y, K) \]

\[ A \]

\[ b' \]

The DH key exchange is secure if the DDH assumption holds
Caveat

The DDH assumption does not hold for $\mathbb{Z}_p^*$

Reason: Given $X = g^x \mod p$, $Y = g^y \mod p$, can efficiently compute the Legendre symbol $\left( \frac{K}{p} \right)$ of the real key $K = g^{xy} \mod p$

How: $\left( \frac{K}{p} \right) = \text{parity}(xy)$, $\left( \frac{X}{p} \right) = \text{parity}(x)$, $\left( \frac{Y}{p} \right) = \text{parity}(y)$

Which group should we use for DH key exchange?

Answer: $\text{QR}_p$ where $p$ is a large “safe” prime

$|\text{QR}_p| = (p - 1)/2$ is also a prime
Strengthening DH Key Exchange

Same as before, but use a hash $H$ at the end

Public param: a large cyclic group $\mathbb{G}$ whose generator is $g$

$x \leftarrow \{0, 1, \ldots, |\mathbb{G}| - 1\} \quad y \leftarrow \{0, 1, \ldots, |\mathbb{G}| - 1\}$

$X \leftarrow g^x \quad Y \leftarrow g^y$

$Z \leftarrow Y^x \quad Z \leftarrow X^y$

$K \leftarrow H(Z) \quad K \leftarrow H(Z)$
The strengthened DH key exchange is secure if the CDH assumption holds, and the hash $H$ is modeled as a random oracle.