Lecture 8: Intro to Asymmetric Crypto

Viet Tung Hoang
Agenda

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

$x \leftarrow S$
$X \leftarrow g^x \mod p$

$y \leftarrow S$
$Y \leftarrow g^y \mod p$

$K \leftarrow Y^x \mod p$

**Question:** Why do Alice and Bob have the same key?

$K \leftarrow X^y \mod p$
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

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

$$\mathbb{Z}_n^* = \{t \in \mathbb{Z}_n \mid \gcd(t, n) = 1\} \quad \varphi(n) = |\mathbb{Z}_n^*|$$

**Example:** $n = 14$

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

$$\mathbb{Z}_{14}^* = \{1, 3, 5, 9, 11, 13\} \quad \varphi(14) = 6$$

**Example:** prime $p$

$$\mathbb{Z}_p^* = \{1, 2, \ldots, p - 1\} \quad \varphi(p) = p - 1$$
An Observation

Consider a number \( g \in \mathbb{Z}_n^* \)
Rho Attack In Disguise

\[ H(x) = x \cdot g \mod n \]

\[ x_1 = H(x_0) \]

\[ x_2 = H(x_1) \]

\[ x_0 = 1 \]

Find a collision of this hash on domain \( \mathbb{Z}^*_n \)
Collision Doesn’t Exist $\rightarrow$ Rho Shape is a Circle
An Observation

Consider $n = 14$

$\varphi(14) = 6$

Cycle length = 6

$3^0 \mod 14 = 1$

$3^1 \mod 14 = 3$

$3^2 \mod 14 = 9$

$3^3 \mod 14 = 13$

$3^4 \mod 14 = 11$

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

Consider \( n = 14 \)

\[ \varphi(14) = 6 \]

Cycle length = 3

\[ 9^0 \mod 14 = 1 \]

\[ 9^1 \mod 14 = 9 \]

\[ 9^2 \mod 14 = 11 \]
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
Restating in Algebraic Form

**Euler’s Theorem:** For any $g \in \mathbb{Z}_n^*$,

$$g^{\varphi(n)} \equiv 1 \pmod{n}$$

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

$$g^{p-1} \equiv 1 \pmod{p}$$
Generators and Cyclic Groups

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

\[ n = 12, g = 11, \langle g \rangle_n = \{1, 11\} \]
Examples

\[ n = 5, g = 2, \langle g \rangle_n = \{1, 2, 3, 4\} \]
Primitive Roots

If the cycle length is \( \varphi(n) \) then we say that \( g \) is a **primitive root** mod \( n \)

**Theorem:** For any prime \( p \), there **exist** primitive roots mod \( p \)

**Exercise:** Find all primitive roots of 7
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 \( QR_p = \left\{ a : \left( \frac{a}{p} \right) = 1 \right\} \)

Example: \( QR_7 = \{1, 2, 4\} \)
In Cyclic View, Sign Alternates

**Theorem:** If $g$ is a primitive root mod $p$ then

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

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

Legendre’s Theorem: \[
\left( \frac{a}{p} \right) = a^{(p-1)/2} \mod p
\]

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

Consider a primitive root $g$

What’s the relative position of $X = g^{(p-1)/2} \mod p$?
It’s at the Antithesis of the Origin

Why? We need to walk half the cycle length to go from the origin to $X$
Generalize It Further

Consider a primitive root $g$

What’s the relative position of $Y = g^{(p-1)t/2} \mod p$?
The Common Trait

If $t$ is odd

Why? We need to walk $t/2$ cycles to go from the origin to $Y$

If $t$ is even
Restating in Algebraic Way

If $t$ is odd

$$Y = g^{t(p-1)/2} \mod p = \text{parity}(t)$$

If $t$ is even
Restating in Algebraic Way

\[ g^{t(p-1)/2} \mod p = \text{parity}(t) \]

Let \( a = g^t \mod p \)

\[ a^{(p-1)/2} \mod p = \text{parity}(t) \]

\[ \left( \frac{a}{p} \right) = \text{parity}(t) \]

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

1. Motivation: Key Exchange

2. Number Theory Basics

3. Diffie-Hellman Assumptions
Review of DH Key Exchange

\[ G = \{ g^i \mid i \in S \} \]

**Public param:** a large cyclic group \( G \) generated by \( g \)

Let \( S = \{ 0, 1, \ldots, |G| - 1 \} \)
The DH key exchange is secure if the DDH assumption holds.
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:** \( QR_p \) where \( p \) is a large "safe" prime

\( |QR_p| = (p - 1)/2 \) 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 $g$

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

$X \leftarrow g^x$

$Y \leftarrow g^y$

$Z \leftarrow Y^x$

$Z \leftarrow X^y$

$K \leftarrow H(Z)$

$K \leftarrow H(Z)$
Computational DH Assumption

is believed to hold for $\mathbb{Z}_p^*$

Real

$x, y \leftarrow \{0, 1, \ldots, |G| - 1\}; \quad X \leftarrow g^x, Y \leftarrow g^y, Z \leftarrow g^{xy}$

$A$ tries to guess $Z$

The strengthened DH key exchange is secure if the CDH assumption holds, and the hash $H$ is modeled as a random oracle.