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

In practice, means 2048-bit

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

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

- $x \leftarrow S$
- $X \leftarrow g^x \mod p$
- $y \leftarrow S$
- $Y \leftarrow g^y \mod p$

$K \leftarrow Y^x \mod p$

**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

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

\[ x_1 = H(x_0) \]
\[ x_2 = H(x_1) \]
\[ x_0 = 1 \]

\[ \ldots \]

**Question:** 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

\[
3^0 \mod 14 = 1 \quad 3^1 \mod 14 = 3 \quad 3^2 \mod 14 = 9 \quad 3^3 \mod 14 = 13
\]

\[
3^4 \mod 14 = 11 \quad 3^5 \mod 14 = 5
\]
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
Euler’s Theorem: For any $g \in \mathbb{Z}_n^*$,

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

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 $\langle g \rangle_n = \{g^i \text{ mod } n \mid i = 0, 1, 2, \ldots\}$ 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
Agenda

1. Motivation: Key Exchange
2. Number Theory Basics
3. Diffie-Hellman Assumptions
Review of DH Key Exchange

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

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

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

\[
x \leftarrow^s S \\
X \leftarrow g^x
\]

\[
y \leftarrow^s S \\
Y \leftarrow g^y
\]

\[
K \leftarrow Y^x
\]

\[
K \leftarrow X^y
\]
### Decisional DH Assumption

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

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

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

Random key \( (X, Y, K) \)

\[ A \]

Real key in DH key exchange

\[ b' \]

The DH key exchange is secure if DDH holds.
Caveat

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

Can break it with advantage $1/2$
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 $g$

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

$$X \leftarrow g^x$$

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

$$Y \leftarrow g^y$$

$$Z \leftarrow Y^x$$

$$\overleftarrow{\text{Z}} \leftarrow X^y$$

$$K \leftarrow H(Z)$$

$$\overleftarrow{\text{K}} \leftarrow H(Z)$$
The strengthened DH key exchange is secure if CDH holds, and $H$ is modeled as a random oracle.