

# CIS 4360, SPRING 2026

## ASYMMETRIC CRYPTO

VIET TUNG HOANG

Some slides are based on material from Prof. Stefano Tessaro, University of Washington

# Agenda

---

**1. Motivation: Key Exchange**

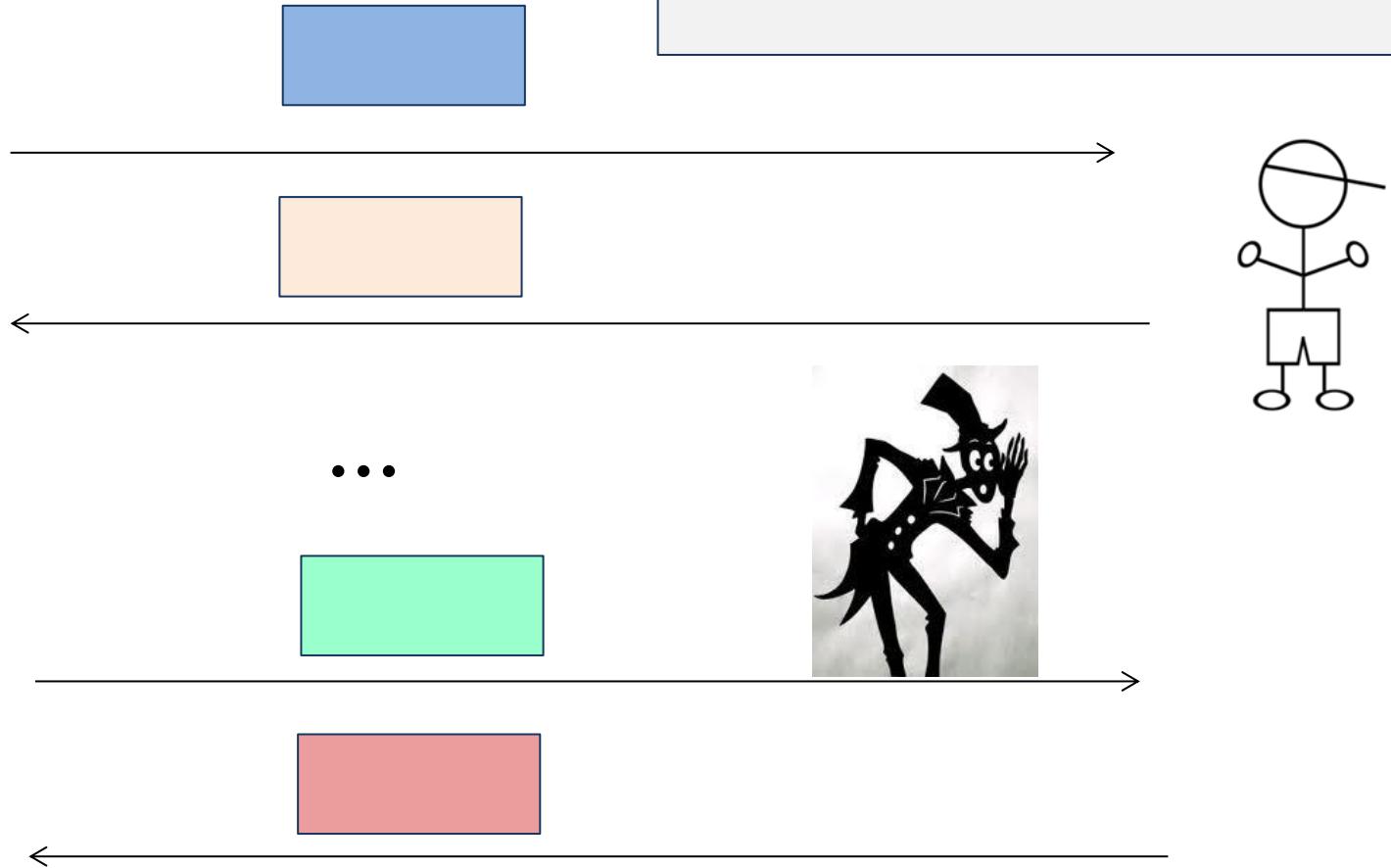
2. Number Theory Basics

3. Diffie-Hellman Assumptions

# Secret Key Exchange

Alice and Bob:

- Initially share no information
- Communicate in the presence of Eve



$K$

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

$K$

# Secret-Key Exchange

**Key exchange is a very important problem**

You use it several times every day



**Big Question:** How to build a key exchange?

A black and white photograph of a man and a woman. The man, on the left, has dark, curly hair and a full, dark beard. He is wearing a light-colored, button-down shirt. The woman, on the right, has blonde hair and is wearing a striped, short-sleeved shirt. They are both smiling and looking towards the camera. The background is slightly out of focus, showing what appears to be an interior room with a window.

1976

# 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  $S = \{0, 1, \dots, p - 2\}$



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

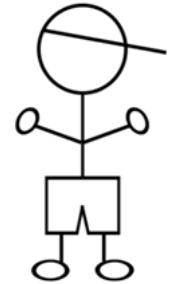
$X$



$K \leftarrow Y^x \bmod p$

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

$K \leftarrow X^y \bmod p$



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

# DH Key Exchange: Questions



What does it mean to be a primitive root mod  $p$ ?

Why can't Eve compute the secret key?

...

# Agenda

---

1. Motivation: Key Exchange

**2. Number Theory Basics**

3. Diffie-Hellman Assumptions

# Some Notation

For  $n \in \{1, 2, 3, \dots\}$ , define

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

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

**Example:**  $n = 14$

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

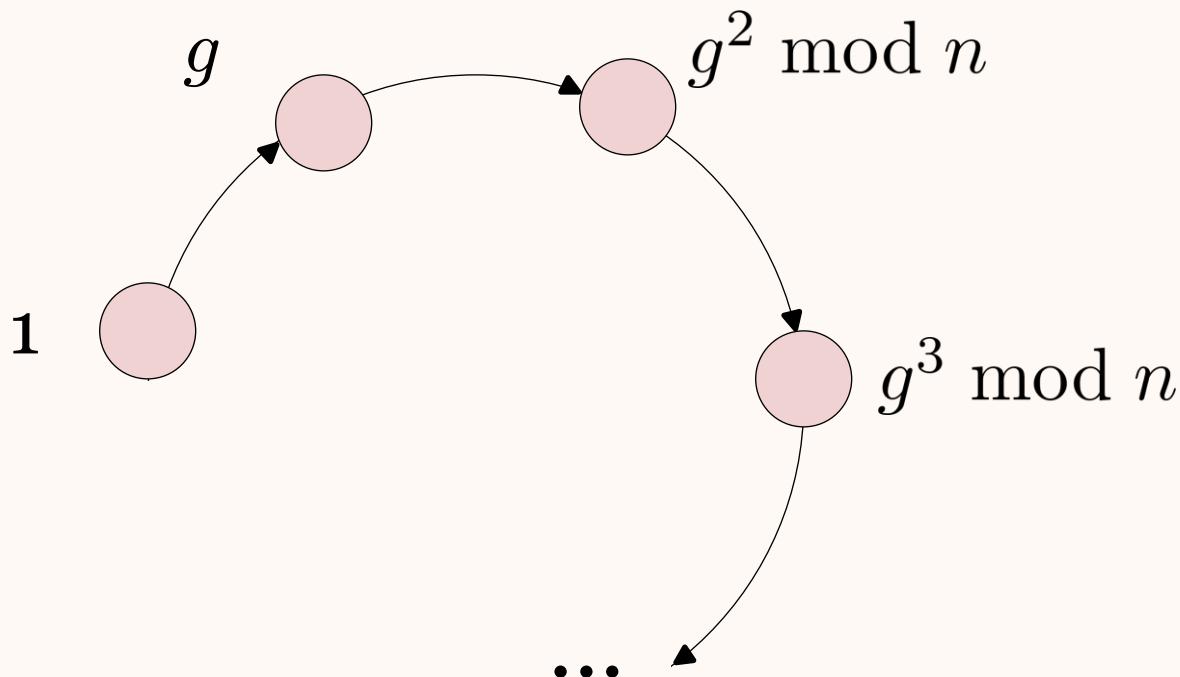
$$\mathbb{Z}_{14}^* = \{1, 3, 5, 9, 11, 13\} \quad \varphi(14) = 6$$

**Example:** prime  $p$

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

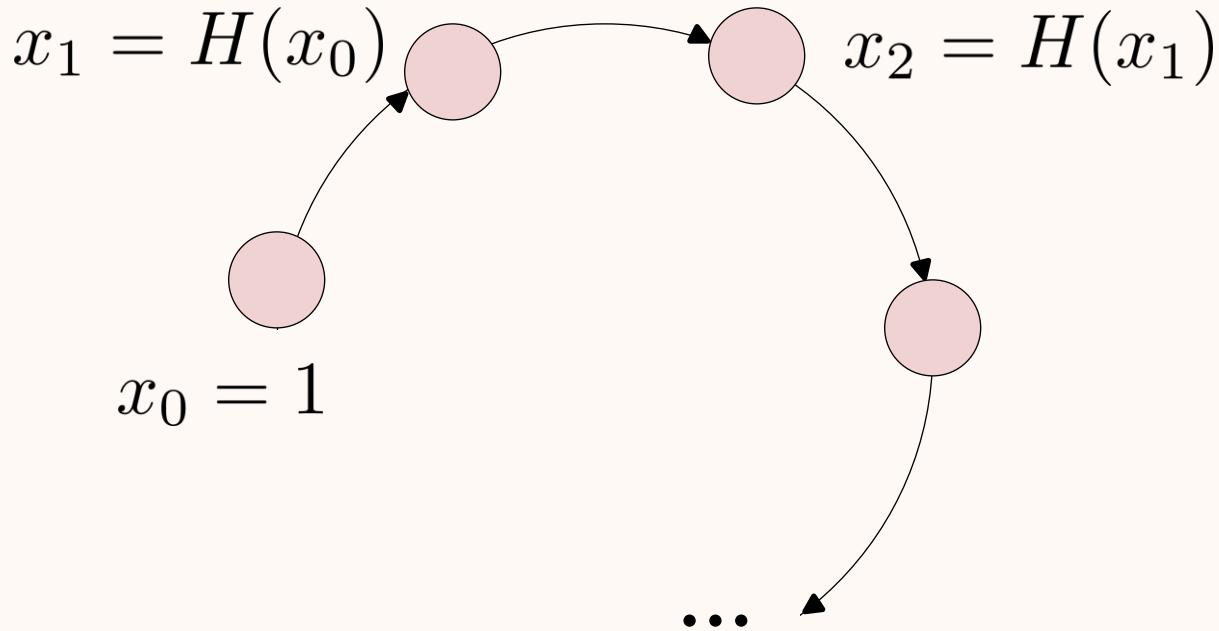
# An Observation

Consider a number  $g \in \mathbb{Z}_n^*$



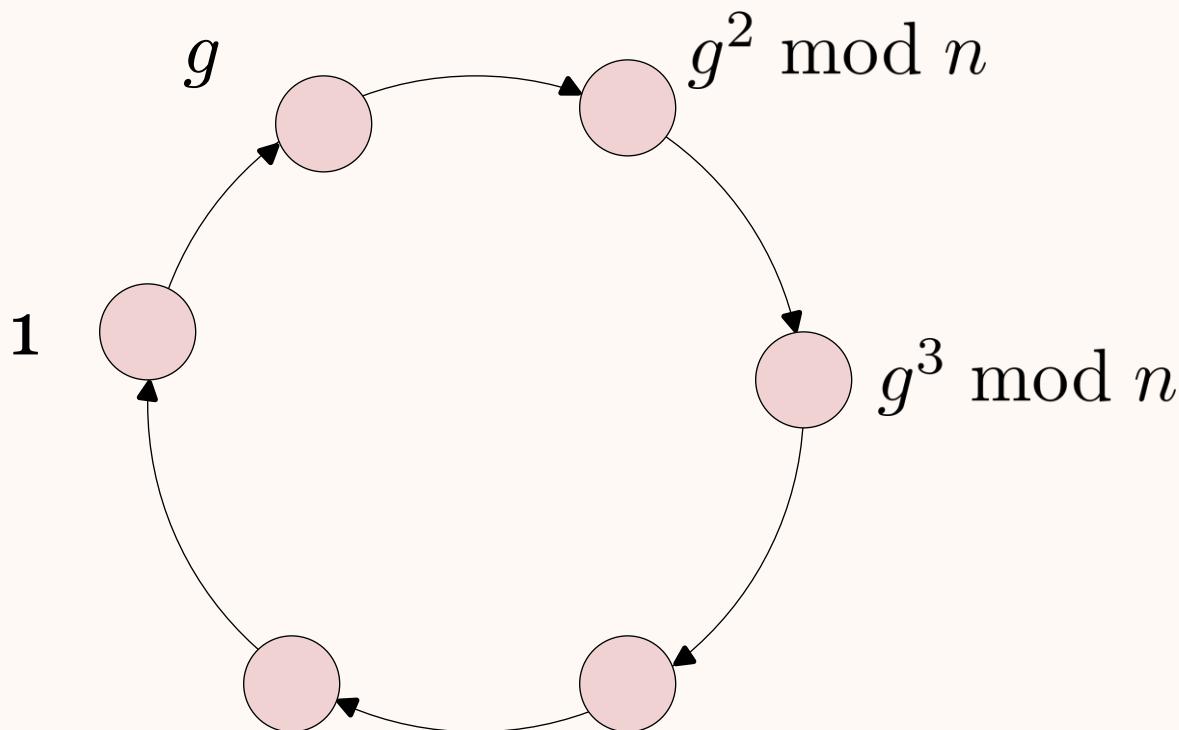
# Rho Attack In Disguise

$$H(x) = x \cdot g \bmod n$$



**Question:** Find a collision of this hash on domain  $\mathbb{Z}_n^*$

# Collision Doesn't Exist $\Rightarrow$ Rho Shape is a Circle

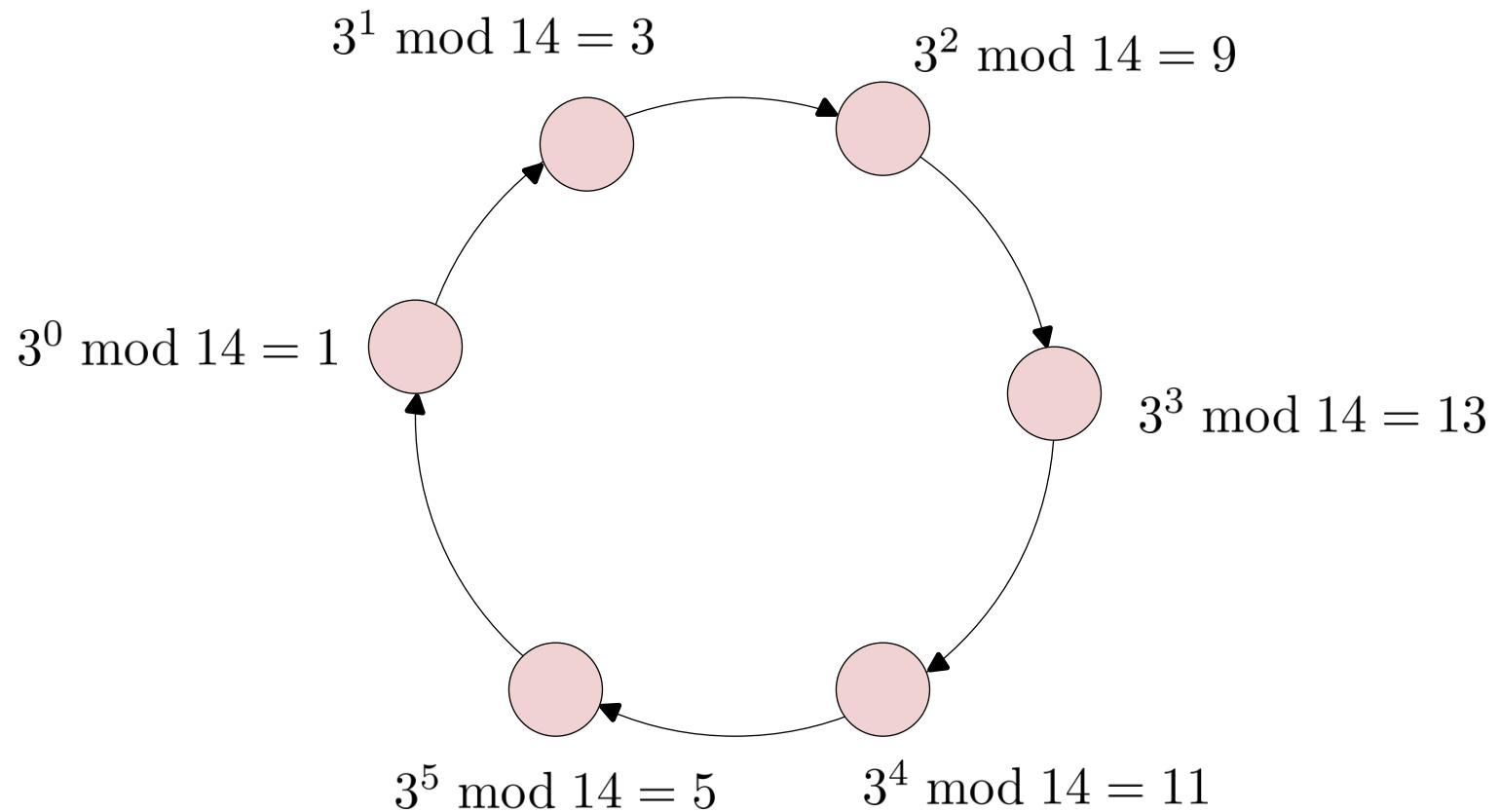


# An Observation

Consider  $n = 14$

$$\varphi(14) = 6$$

Cycle length = 6

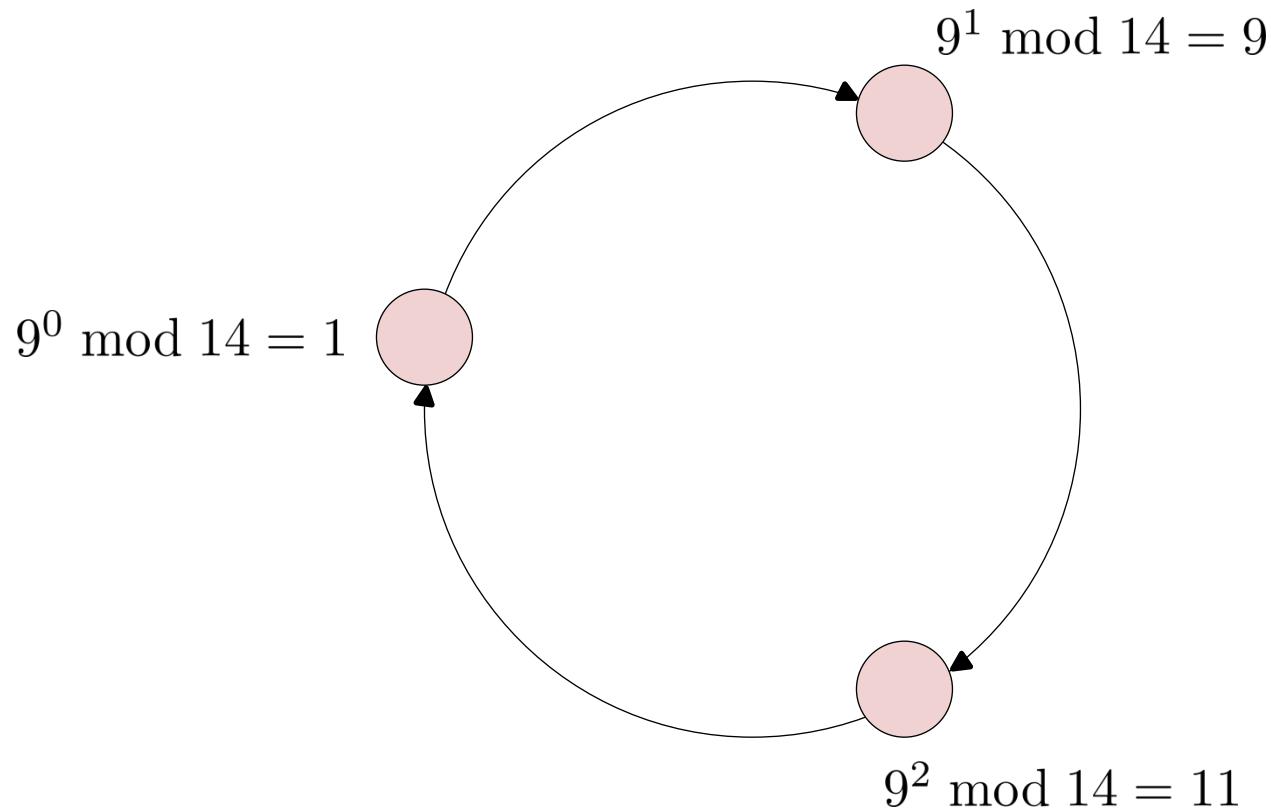


# An Observation

Consider  $n = 14$

$$\varphi(14) = 6$$

Cycle length = 3

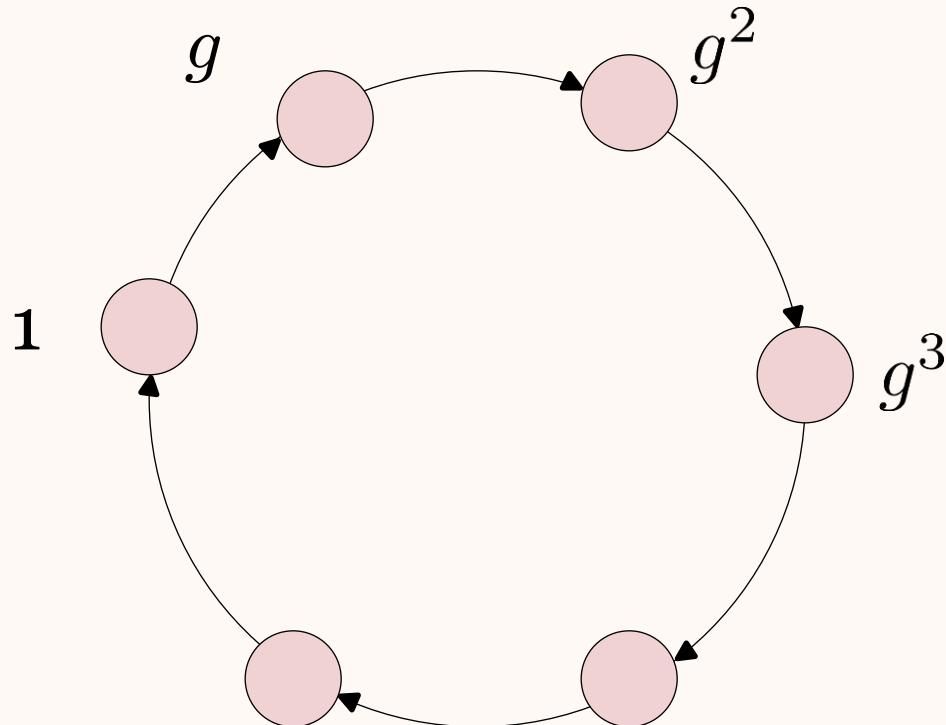


# The Common Trait

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



# Restating in Algebraic Form

**Euler's Theorem:** For any  $g \in Z_n^*$ ,

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



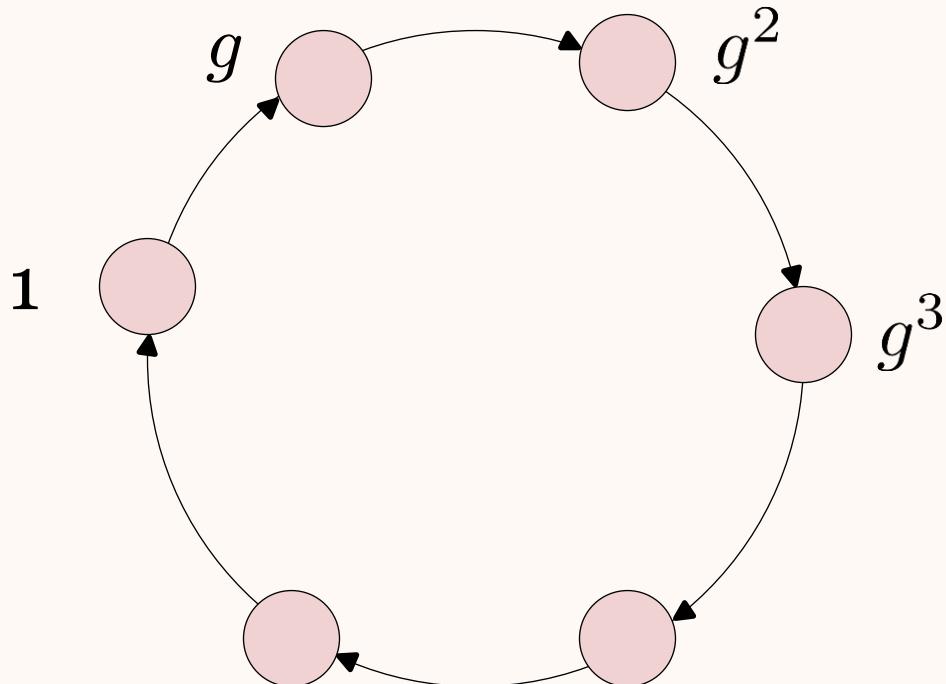
**Fermat's Little Theorem:** For any prime  $p$  and any  $g \in Z_p^*$ ,

$$g^{p-1} \equiv 1 \pmod{p}$$



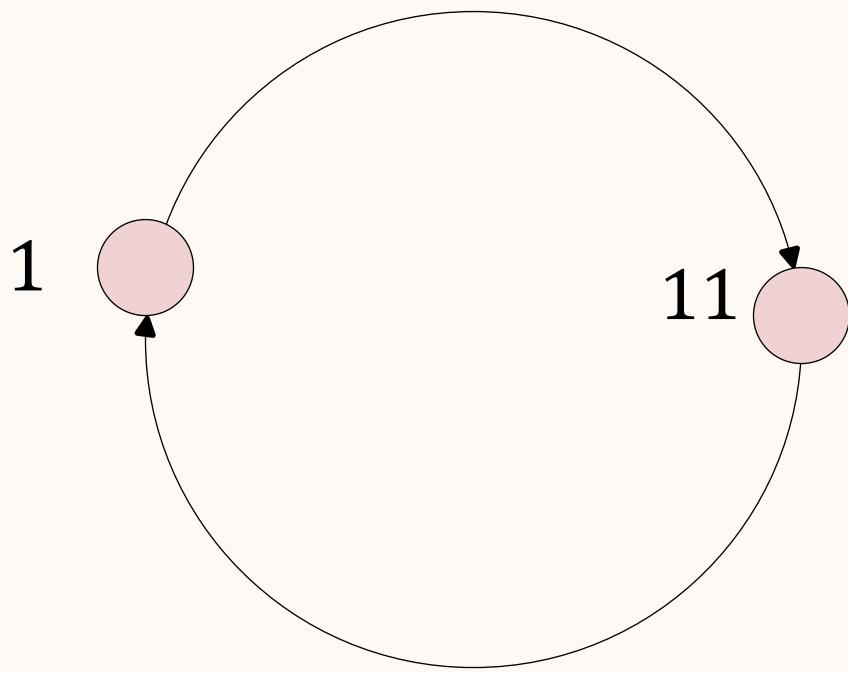
# Generators and Cyclic Groups

Define  $\langle g \rangle_n = \{g^i \bmod n \mid i = 0, 1, 2, \dots\}$  as the **cyclic group** mod  $n$  generated by  $g$



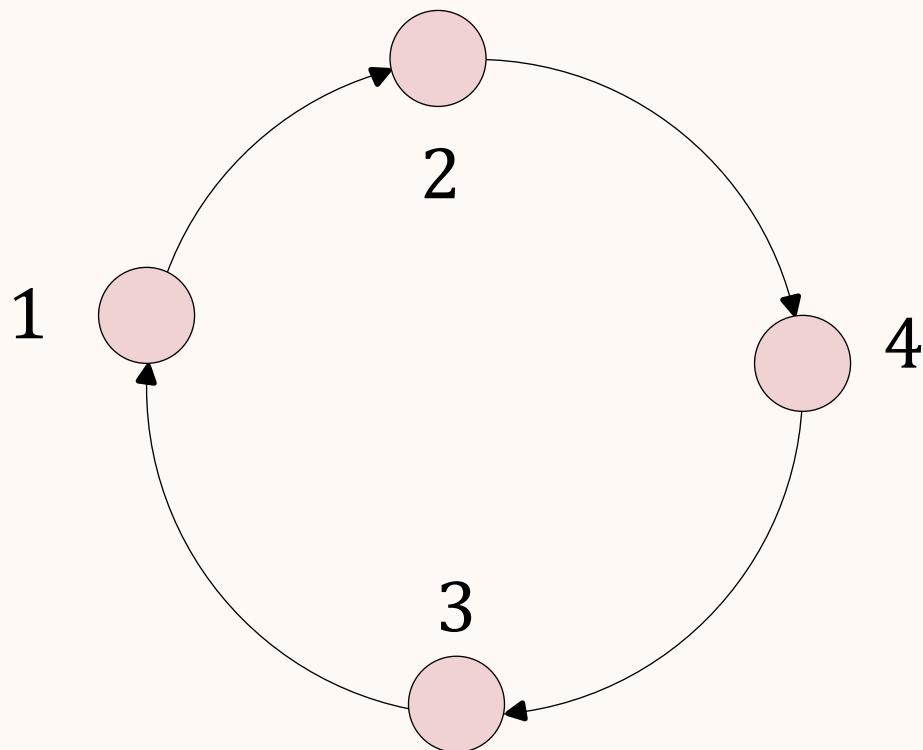
# Examples

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



# 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

---

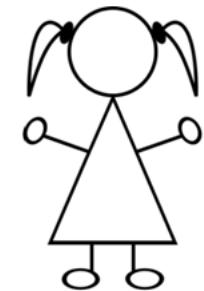
1. Motivation: Key Exchange
2. Number Theory Basics
3. **Diffie-Hellman Assumptions**

# Review of DH Key Exchange

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

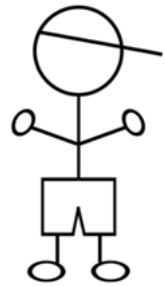
**Public param:** a large cyclic group  $\mathbb{G}$  generated by  $g$

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



$$X$$

$$\begin{aligned} x &\leftarrow_{\$} S \\ X &\leftarrow g^x \end{aligned}$$



$$Y$$



$$\begin{aligned} y &\leftarrow_{\$} S \\ Y &\leftarrow g^y \end{aligned}$$

$$K \leftarrow Y^x$$

$$K \leftarrow X^y$$

# Intuition for Security

## The Discrete Log Problem

Let  $\mathbb{G} = \{g^i \mid i \in S\}$  be a cyclic group of size  $N$

**Easy:**  $O(\log(N))$  time

Alice's secret

$$x \in S$$

What adversary sees

$$g^x$$

How hard?

Optimal for **generic** algo

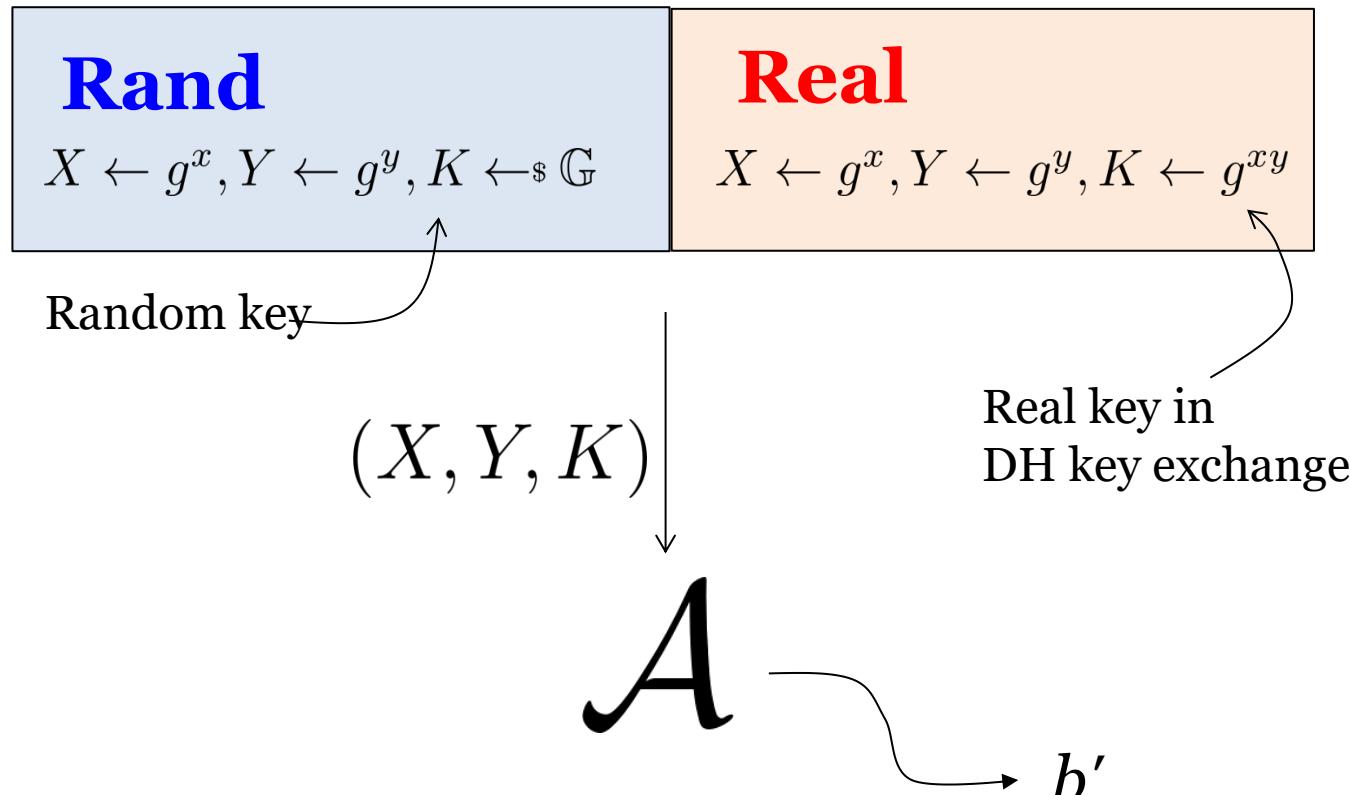
Naïve:  $O(N)$  time

Rho attack:  $O(\sqrt{N})$  time

# Decisional DH Assumption

Discrete Log hardness is **not** enough to justify security of DH key exchange, so we need a stronger assumption

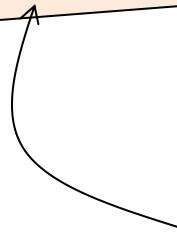
$$x, y \leftarrow_{\$} \{0, 1, \dots, |\mathbb{G}| - 1\}$$



The DH key exchange is secure if DDH holds

## Caveat

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

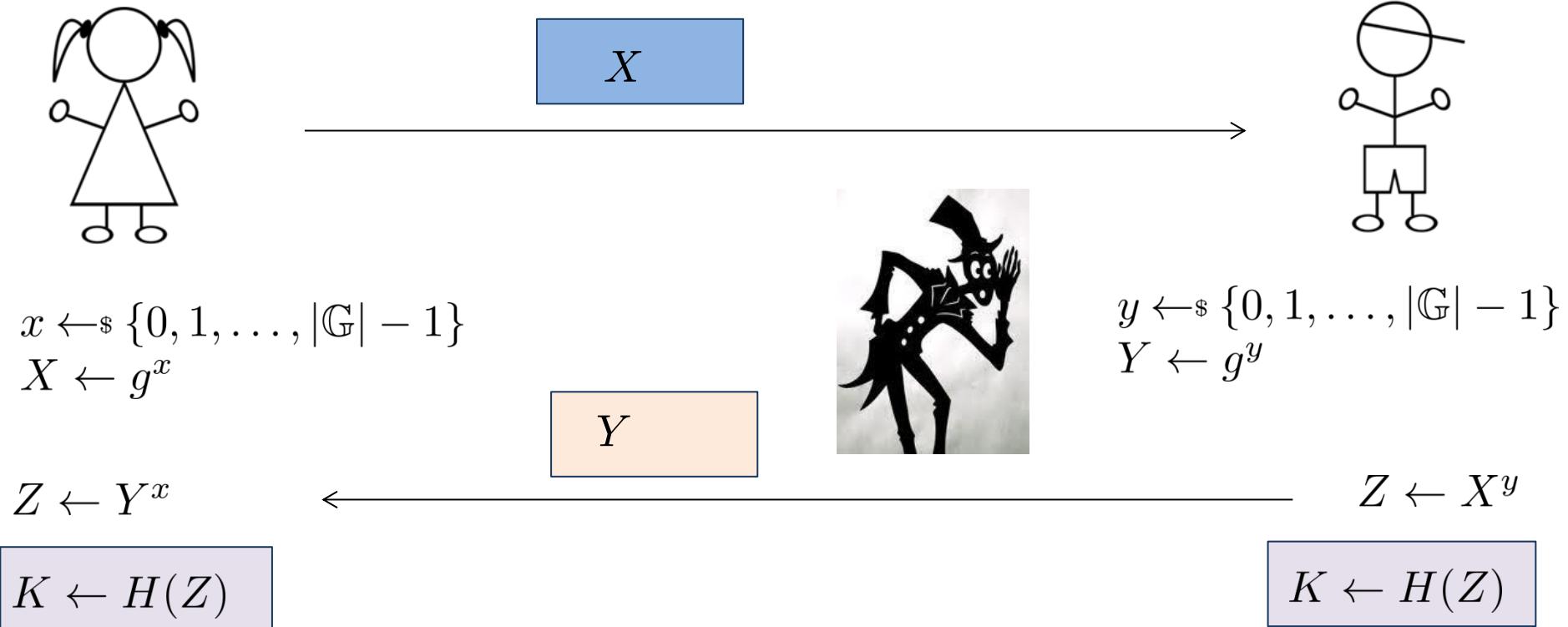


Can break it with advantage  $1/2$

# 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  $g$

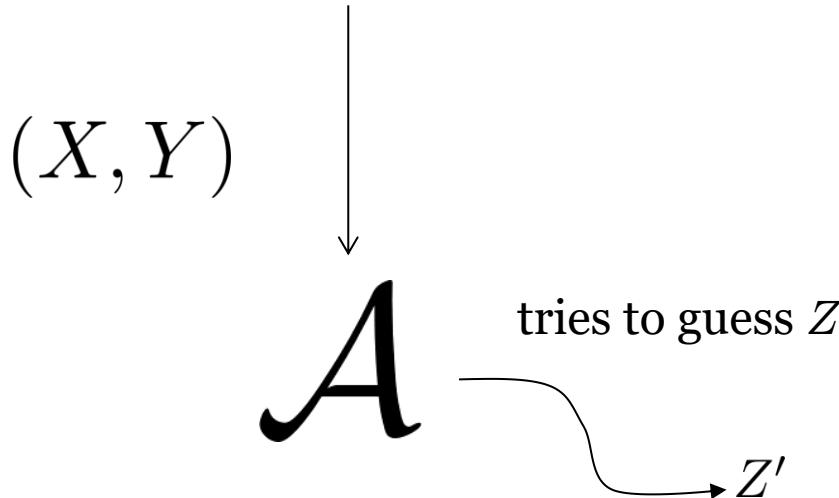


# Computational DH Assumption

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

## Real

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



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