CIS 4360: Computer Security Fundamentals

Asymmetric Crypto

Viet Tung Hoang

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

Agenda

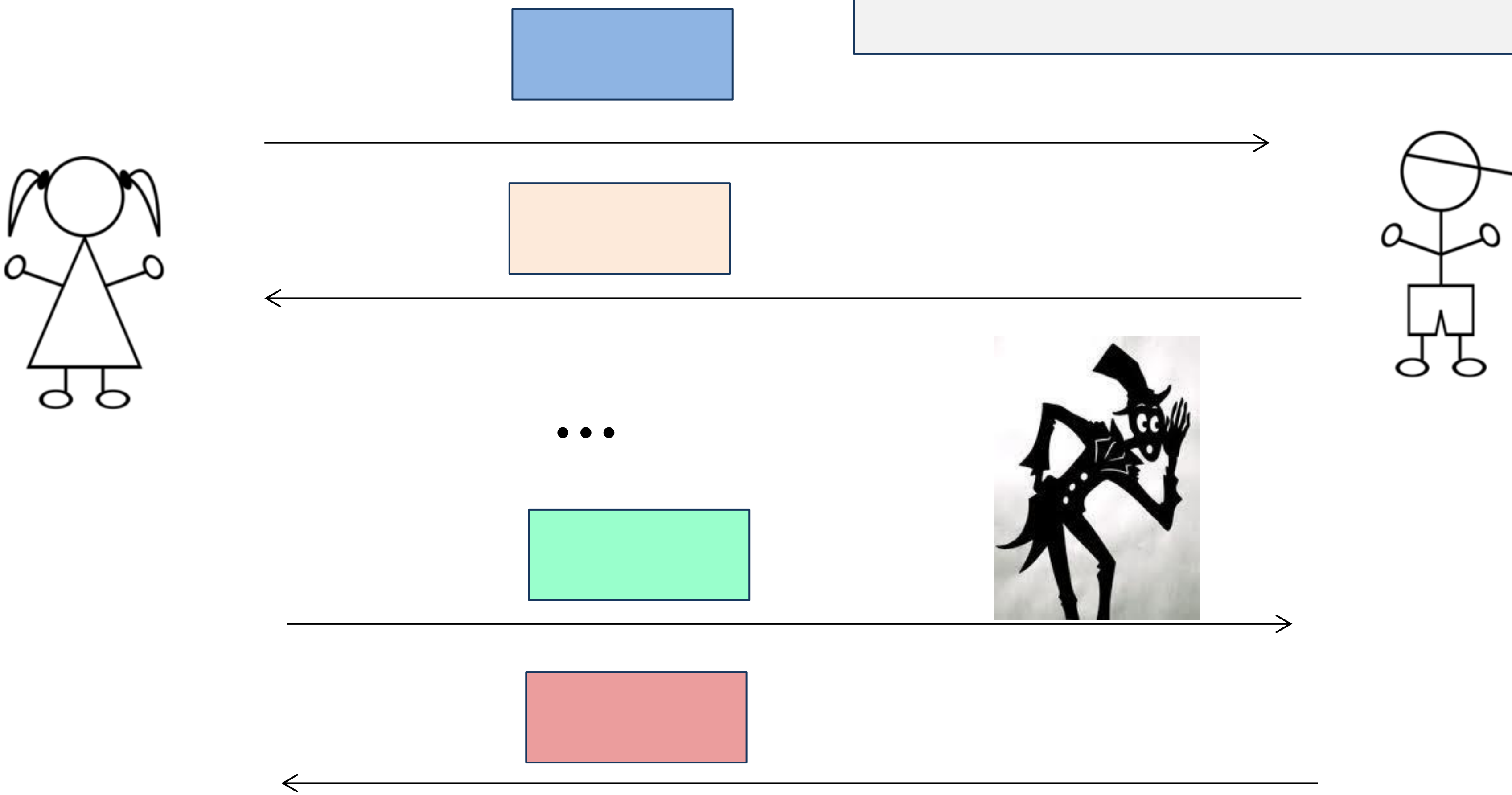
1. **Motivation: Key Exchange**
2. Number Theory Basics
3. Diffie-Hellman Assumptions

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?

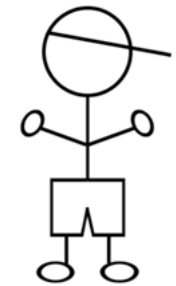

1976

Basic Diffie-Hellman Key Exchange

Public param: a $\overbrace{\text{large prime } p}^{\text{In practice, means 2048-bit}}$, a number g called a primitive root mod p.

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

X



$x \leftarrow_{\$} S$
$X \leftarrow g^x \bmod p$

$y \leftarrow_{\$} S$
$Y \leftarrow g^y \bmod p$

Y

$K \leftarrow Y^x \bmod p$

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

$K \leftarrow X^y \bmod p$

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 $n \in \{1, 2, 3, \ldots\}$, define

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

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

Example: $n = 14$

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

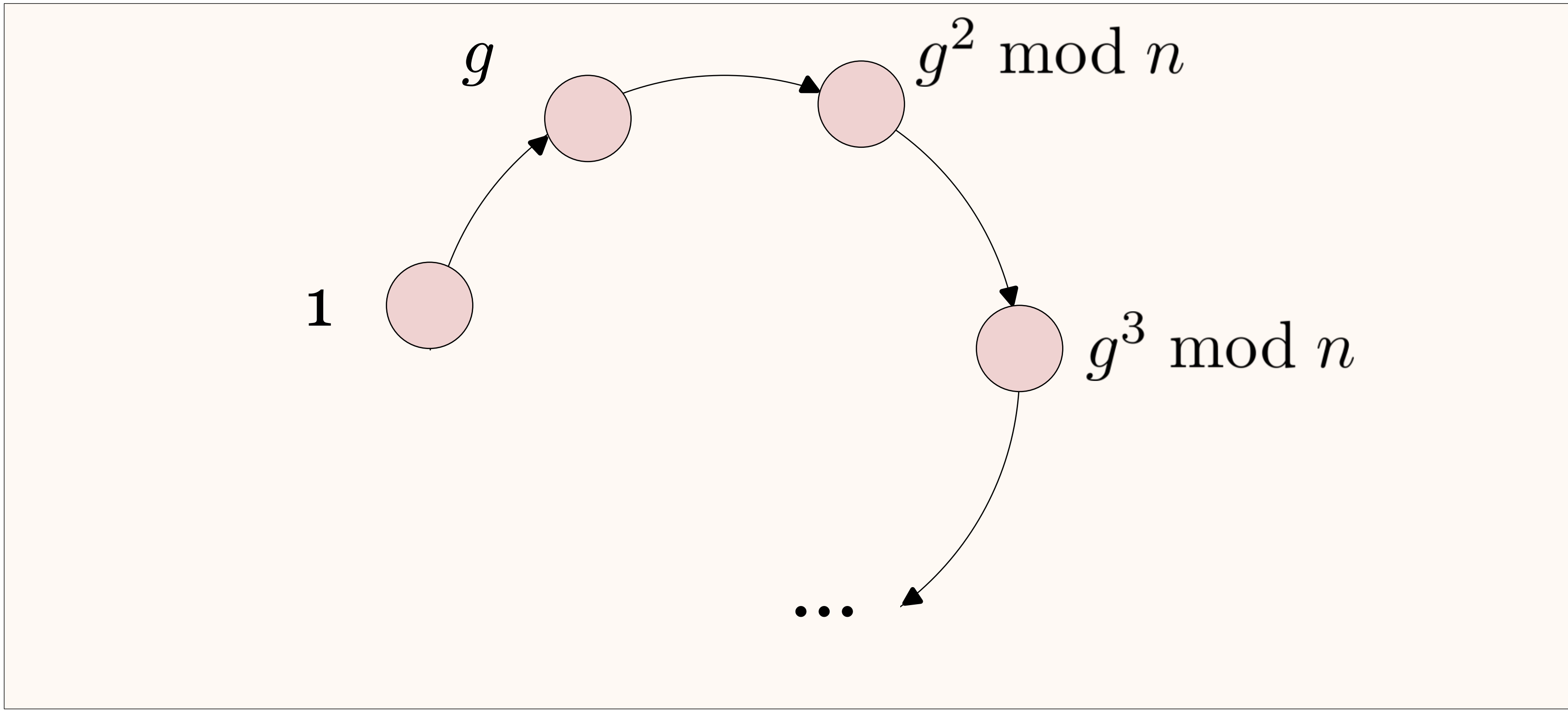
$$\mathbb{Z}_{14}^* = \{1, 3, 5, 9, 11, 13\} \qquad \varphi(14) = 6$$

Example: prime p

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

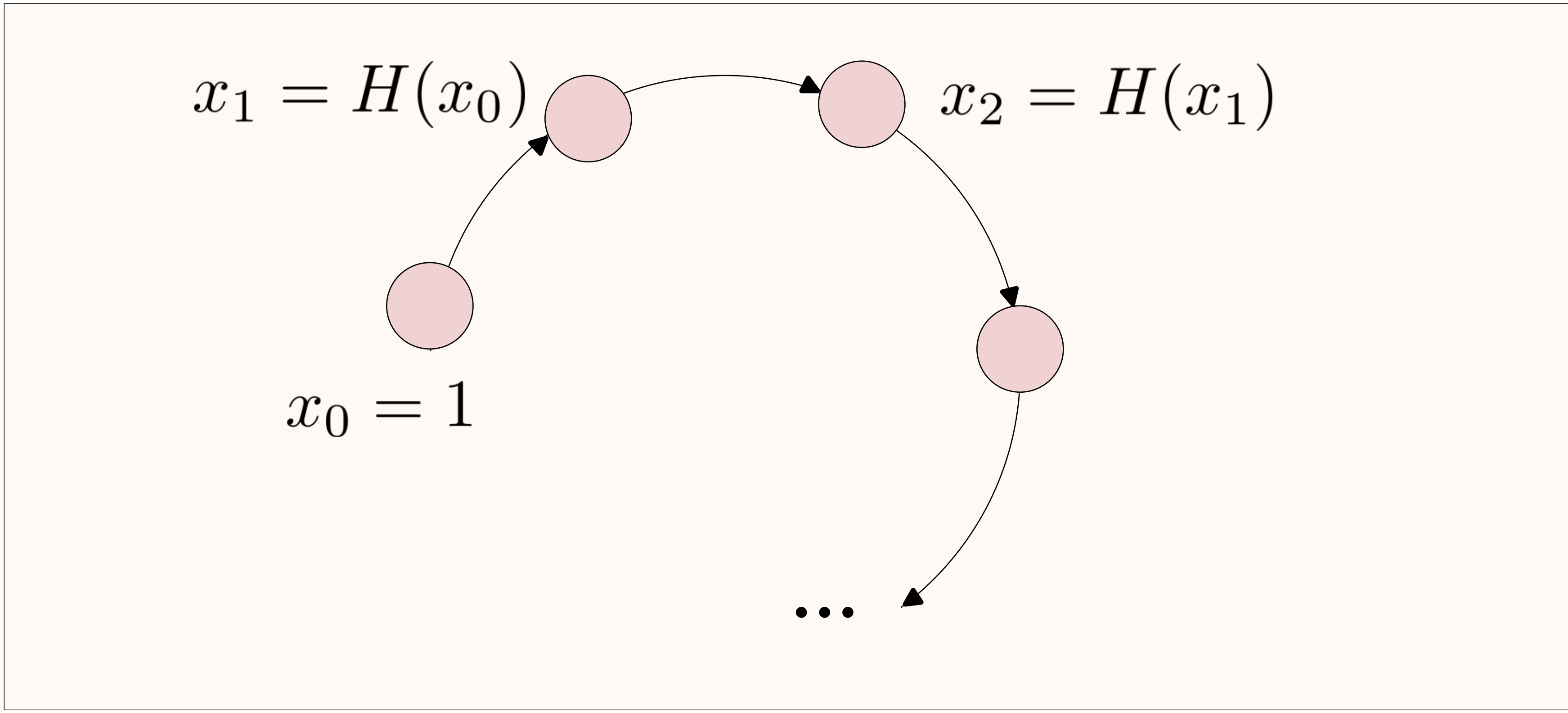
An Observation

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



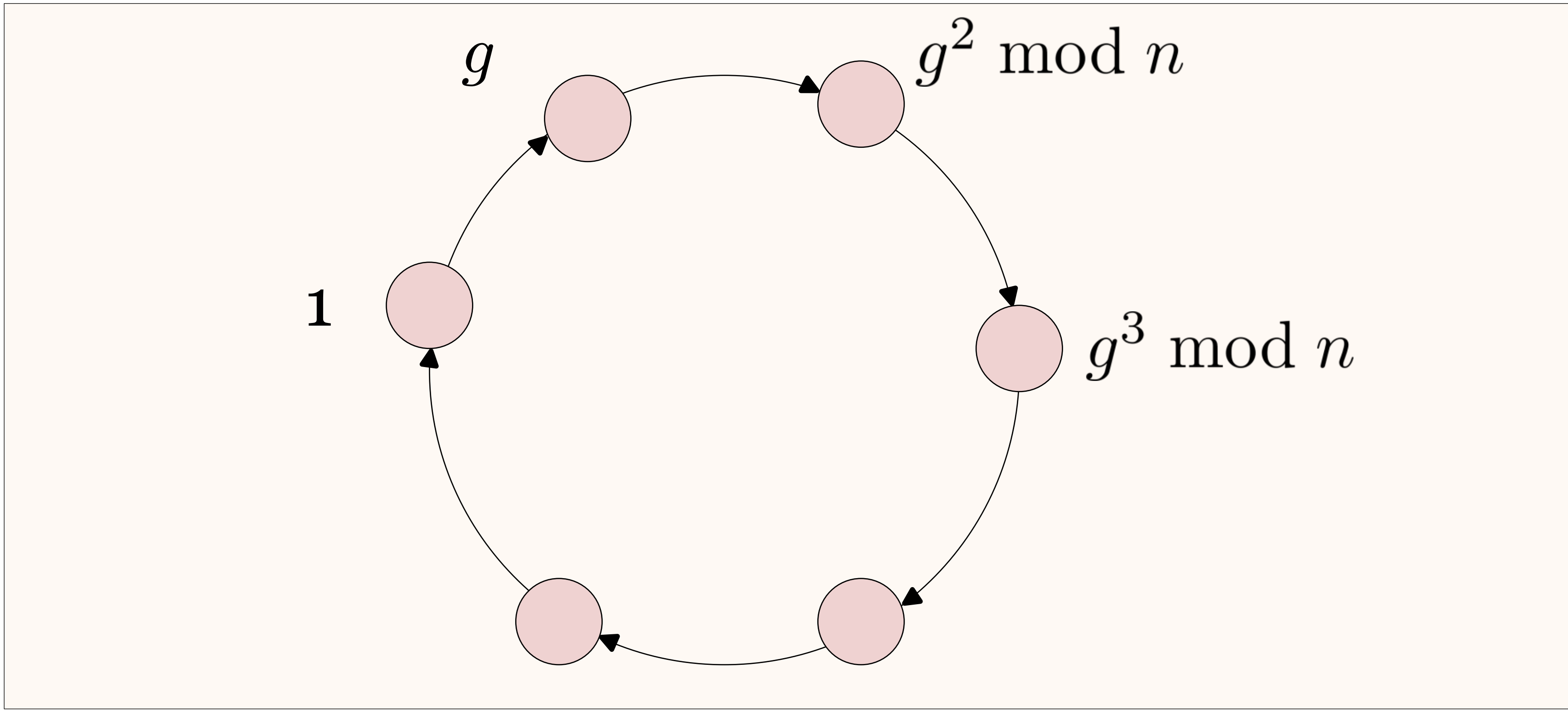
Rho Attack In Disguise

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



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

Collision Doesn't Exist ➡ Rho Shape is a Circle

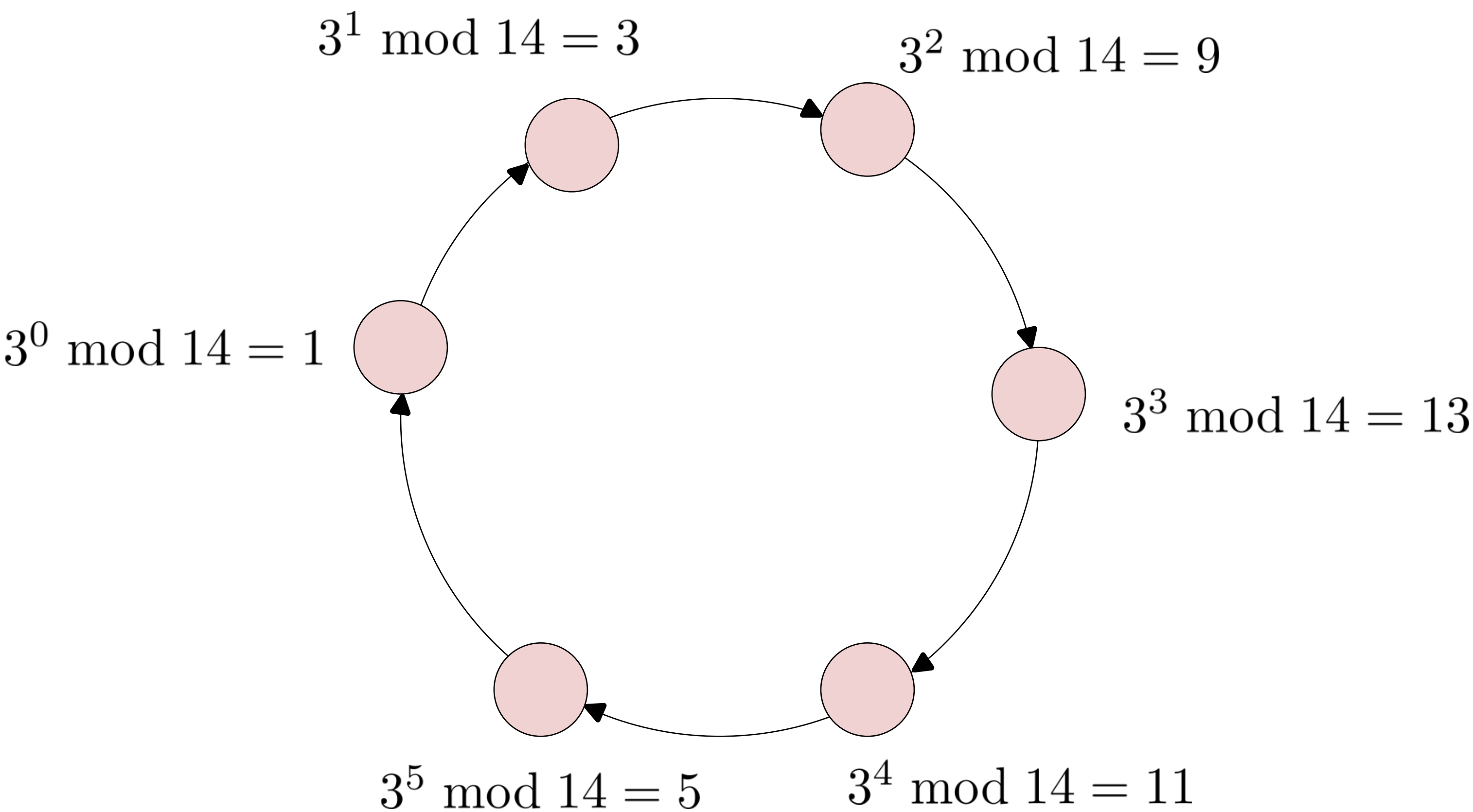


An Observation

Consider $n = 14$

$\varphi(14) = 6$

Cycle length = 6

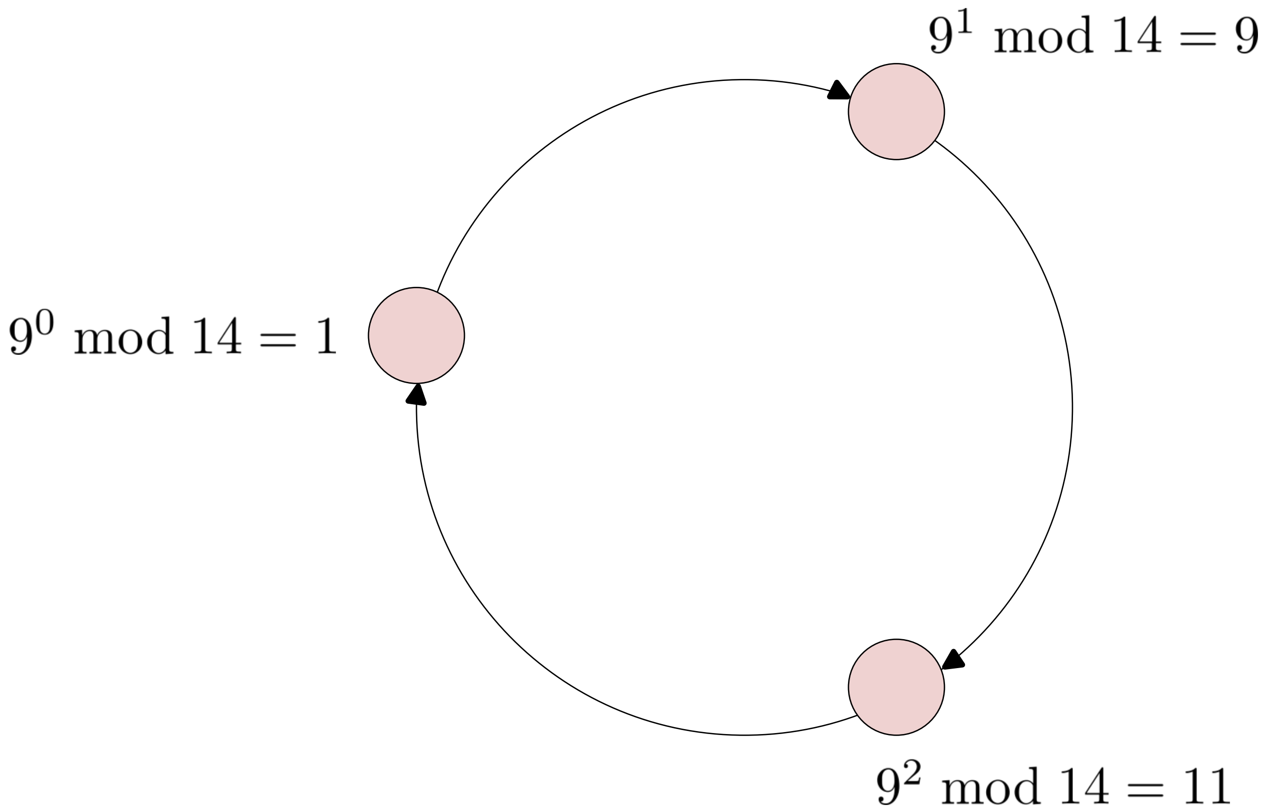


An Observation

Consider $n = 14$

$\varphi(14) = 6$

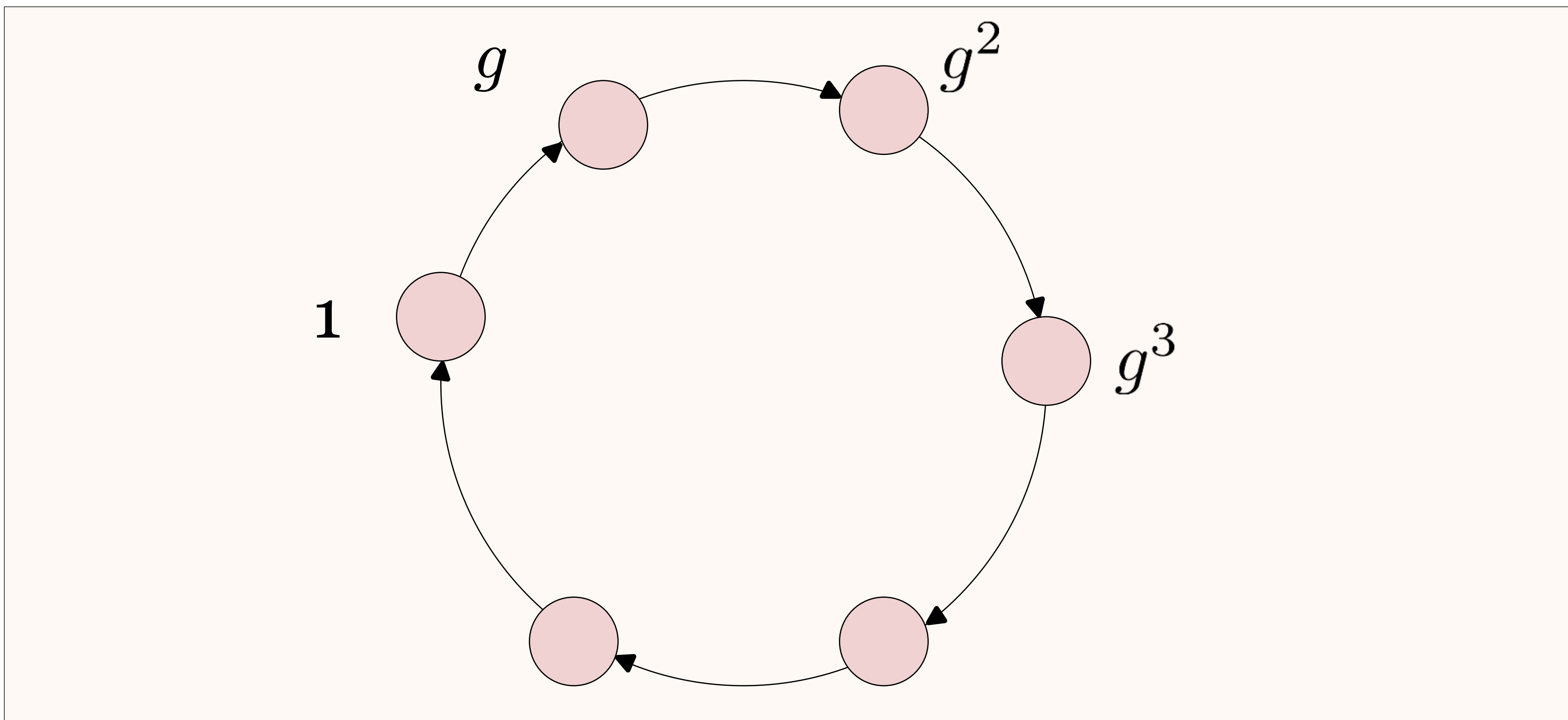
Cycle length = 3



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 $g \in Z_n^*$,

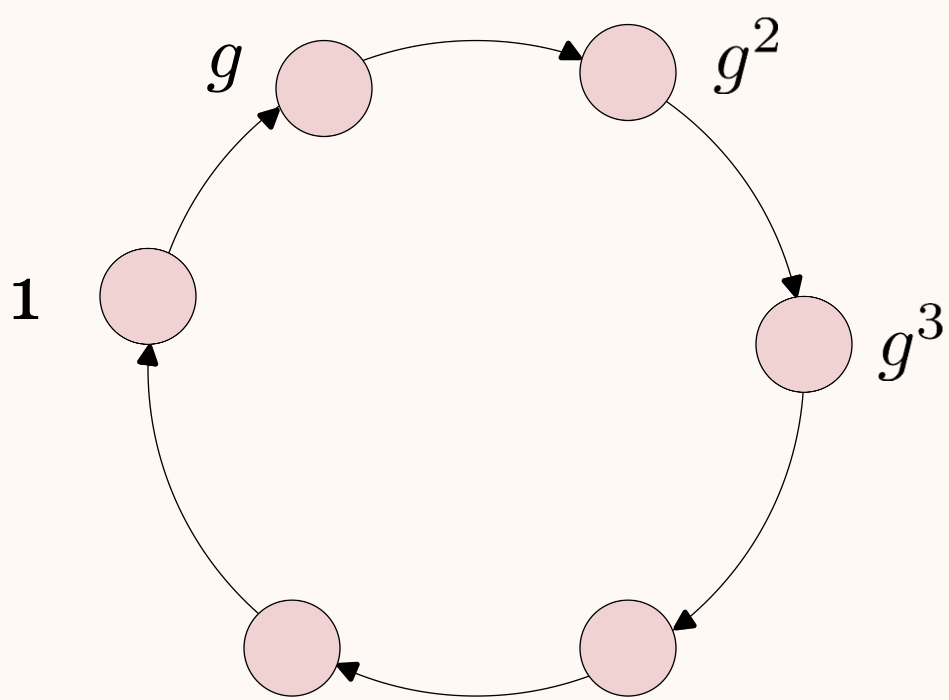
$$g^{\varphi(n)} \equiv 1 \pmod{n}$$

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

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

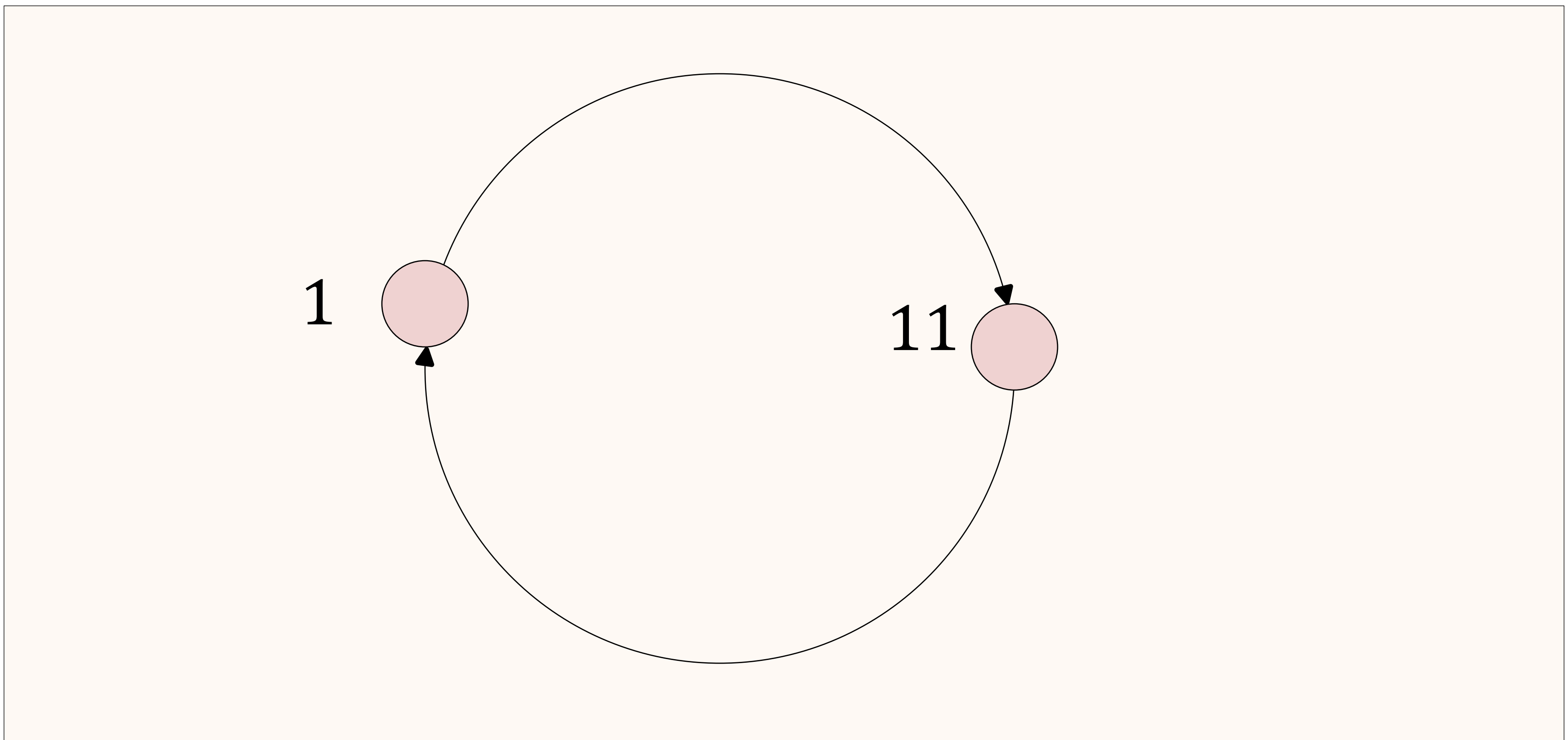
Generators and Cyclic Groups

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



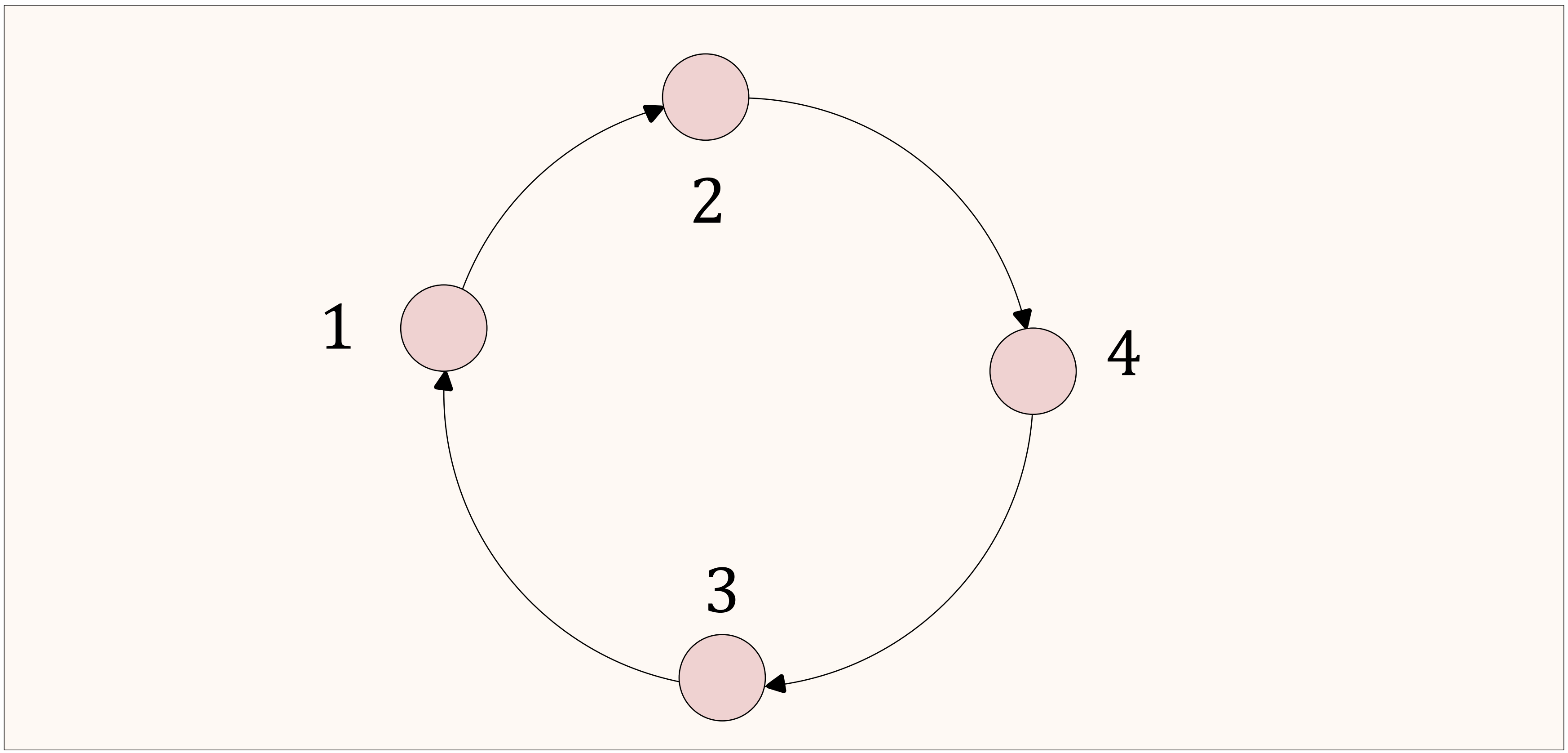
Examples

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



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

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

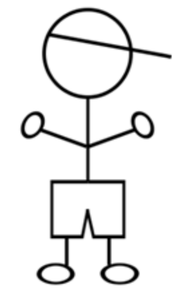
Public param: a large cyclic group $\mathbb{G}$ generated by g

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

$x \leftarrow\!\!\$\ S$

$X \leftarrow g^x$

X



$y \leftarrow\!\!\$\ S$

$Y \leftarrow g^y$

Y

$\boxed{K \leftarrow Y^x}$

$\boxed{K \leftarrow X^y}$

Intuition for Security

The Discrete Log Problem

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

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

Alice's secret

What adversary sees

$$x \in S \qquad\qquad g^x$$

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

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

Rand	**Real**
$X \leftarrow g^x, Y \leftarrow g^y, K \leftarrow_{\$} \mathbb{G}$	$X \leftarrow g^x, Y \leftarrow g^y, K \leftarrow g^{xy}$

Random key

Real key in
DH key exchange

$$(X, Y, K)$$

$$\mathcal{A} \longrightarrow b'$$

The DH key exchange is secure if DDH holds

Caveat

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

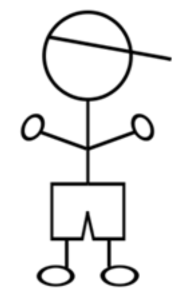
Can break it with advantage 1/2

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



$x \leftarrow_{\$} \{0, 1, \ldots, |\mathbb{G}| - 1\}$
$X \leftarrow g^x$

$y \leftarrow_{\$} \{0, 1, \ldots, |\mathbb{G}| - 1\}$
$Y \leftarrow g^y$

Y

$Z \leftarrow Y^x$

$Z \leftarrow X^y$

$\boxed{K \leftarrow H(Z)}$

$\boxed{K \leftarrow H(Z)}$

Computational DH Assumption

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

Real

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

$$(X, Y)$$

$$\mathcal{A}$$

tries to guess Z

Z'

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