# CIS 3362 - 10/23/23

Write your primality check/factor + phi(n) code.

① Can Alice + Bob exchange a secret key by communicating on a "public line" only?

② Can Alice + Bob completely communicate back and forth w/ everyone listening, but no one understanding what they are saying?

→ TODAY - Diffie-Hellman Key Exchange
Code Book Story

→ WED - RSA encryption

In public Diffie-Hellman created before RSA.
In private RSA was discovered before Diffie-Hellman, and both of these predate the public discovery.

In order either to work we need some mathematical function that is "ONE-WAY"

easy to calculate forward (modular expo)
hard to undo calculation

Public Components: $p$ (prime #)
$g$ (generator)

Diffie-Hellman worked together

Alice
pick secret key $a$
$1 < a < p-1$

$g^a \bmod p$ →

Bob

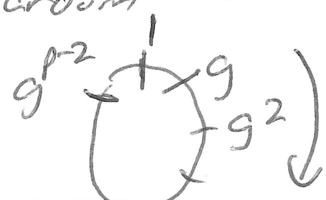
← $g^b \bmod p$

Bob
pick secret key $b$
$1 < b < p-1$

Alice receives $g^{\cancel{a}b}$ compute $(g^b)^a \bmod p$

Bob receives $g^a \to$ compute $(g^a)^b \bmod p$
↓
$g^{ab} \bmod p$

generator randomly generates each int 1 to $p-1$ in a random order




Transmitted

using $g^a \bmod p$
$g^b \bmod p$

$$g^a \times g^b = g^{a+b}$$

$$\frac{g^a}{g^b} = g^{a-b}$$
(mod inv

it's hard to calculate $g^{ab}$

At the end of this, Alice + Bob have a shared key $\rightarrow$ $g^{ab} \bmod p$, that neither "picked", but they both know they have the same common piece of information.