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 with 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)

Alice
- pick secret key \( a \)
- \( 1 < a < p-1 \)

\[ g^a \mod p \rightarrow \text{Bob} \]

Bob
- pick secret key \( b \)
- \( 1 < b < p-1 \)

\[ g^b \mod p \]

Alice receives \( g^b \)
compute \( (g^b)^a \mod p \)

Bob receives \( g^a \)
compute \( (g^a)^b \mod p \)

\[ g^{ab} \mod p \]

Generators randomly generated each int 1 to \( p-1 \) in a random order

\[ g^{a_1}, g^{a_2}, \ldots, g^{a_{p-2}} \]

Transmitted using \( g^a \mod p \)

It's hard to calculate \( g^{ab} \)
At the end of this, Alice and Bob have a shared key $g^{ab} \mod p$, that neither "picked", but they both know they have the same common piece of information.