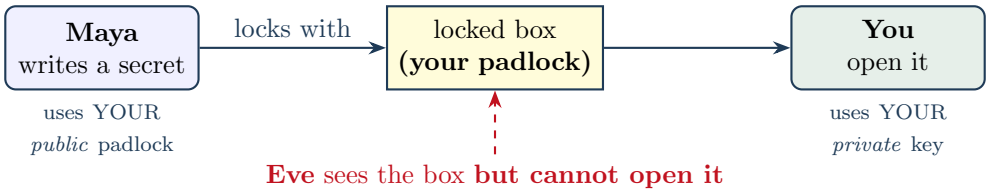
Public-Key Encryption

Name: _____

The big idea. Every code so far needed both people to share a *secret key* first. But how do you agree on a secret with someone while an eavesdropper is listening? **Public-key encryption** gives everyone *two* keys:

- a **PUBLIC key** — like an *open padlock* you hand out to the whole world, and
- a **PRIVATE key** — the *only key that opens* your padlock, which you never share.

Anyone can lock a box with your public padlock, but **only your private key can open it** — not even the person who locked it!



Part 1 Public key or private key?

1. Maya wants to send *you* a secret. Whose padlock (public key) does she use to lock the box?

   _____

2. After Maya snaps your padlock shut, can *she* reopen the box? Why or why not?

   _____

3. Eve grabs the locked box on its way to you. Can she read the message? What would she need?

   _____

4. Now *you* want to reply secretly to Maya. Whose padlock do you use?

   _____

5. Why is it safe to hand out your public padlock to everyone — even to Eve?

   _____

Part 2 The secret math: easy one way, hard the other

The two keys are linked by math that is **easy to do but very hard to undo**. Multiplying two prime numbers is easy. Un-multiplying (factoring) is hard — and that is what keeps your private key safe.

A. Easy direction — multiply these two primes:

$3 \times 11 =$ _____ $7 \times 17 =$ _____

$13 \times 19 =$ _____ $23 \times 29 =$ _____

How did that feel? _____

B. Hard direction — find the TWO prime factors:

$35 =$ _____ $\times$ _____ $91 =$ _____ $\times$ _____

$143 =$ _____ $\times$ _____ $187 =$ _____ $\times$ _____

$221 =$ _____ $\times$ _____ $323 =$ _____ $\times$ _____

Boss level: $3233 =$ _____ $\times$ _____

Part 3 Think about it

1. Which was easier — multiplying, or finding the factors?

   _____

2. Real keys use primes that are *hundreds of digits* long. Why does that keep a private key safe, even from powerful computers?

   _____

Fun fact: this is what the little padlock in your web browser means — public-key encryption locking your messages every time you shop or chat online.

Answer Key (for the teacher)

Part 1

1. **Your** public padlock (public key). Locks are done with the *recipient's* public key.
2. **No.** Once it's locked with your padlock, only your private key opens it — not even Maya.
3. **No.** She'd need your *private* key, which you never share.
4. **Maya's** public padlock — you always lock with the *recipient's* public key.
5. Because the padlock only *locks*; it can't *unlock*. Knowing it doesn't help Eve open anything.

Part 2

A. Multiply: $3 \times 11 = 33$, $7 \times 17 = 119$, $13 \times 19 = 247$, $23 \times 29 = 667$.

B. Factor: $35 = 5 \times 7$, $91 = 7 \times 13$, $143 = 11 \times 13$, $187 = 11 \times 17$, $221 = 13 \times 17$, $323 = 17 \times 19$.

Boss: $3233 = 53 \times 61$.

Part 3

Multiplying is far easier than factoring. With hundreds-of-digits primes, multiplying still takes a computer an instant, but factoring the product would take even the fastest computers longer than the age of the universe — so the private key stays secret.