Merkle's Problems

What is the problem?

- Alice and Bob want to talk.
- Alice and Bob want to talk in public.
- Alice and Bob want to talk public but no one should understand their messages.
    - People can eavesdrop but they shouldn't be able to understand the messages.

What's the key problem?

- How keys work is a whole todo, so let's imagine A and B use a padlock.
- How do they exchange keys?
    - Can Alice just send the key to Bob? (Why? Why not?)
    - Can Alice just tell Bob the padlock ID? (Why? Why not?)

The fundamental problem is

- How do two parties agree on a key when people can watch them talking about the key?

Use all the padlocks!

- Well, use a lot of them. Bob can send Alice say 10 envelopes of [padlock + key + random id].
- Alice picks an envelope, say envelope #7.
    - She puts her secret message in a box, locks it with lock #7 and writes the random id on the outside.
    - Bob reads the id outside the box and uses the corresponding key. Reads the secret message.
- What can an eavesdropper do?
    - An eavesdropper can open all 10 envelopes to find the random id.
    - That is 10x the work compared the Alice...

More generally...

- Bob prepares m envelopes with [padlock + key + random id] and opens the one Alice picks
    - m seconds to make the envelopes
    - n seconds to open just one
    - takes m + n seconds
- Alice picks one envelope and opens it
    - Looks at all m envelopes and picks one
    - Maybe n seconds to open
    - takes m + n seconds
- Eavesdropper has to open all m envelopes, taking n seconds each.
    - takes m * n seconds

More, more generally...

- If m and n are close, Bob and Alice do (m+n) ~ 2n work
- Eve does n*m ~ n^2 work

More actually...

- Bob is sending puzzles whose solutions
  - reveal his randomly-assigned id
  - reveal a secret key
- Alice picks a puzzle and solves. Then she
  - sends her secret message encrypted with the random id
  - sends the random id just out in the open (not encrypted)
- Bob reads the random id then
  - looks up and solves the puzzle
- Eve has to solve (up to) all the puzzles
  - When she solves a puzzle that matches Alice's random id, she can stop

Again...

- Alice/Bob have to do ~2n work.
- Eve has to do around n^2 work
- (Has anyone told you that n^2 is a lot?)
- Try some numbers...if Alice Bob are doing 20 seconds, Eve is doing 100 seconds.
  - That means your message won't be secret after 100 seconds.
- Alice, Bob do 5 minutes of work, Eve does 15 days of work.
  - I mean, 5 minutes is a lot of work.
  - 15 days isn't exactly eternity.

The good, the bad, the future

- Sadly, there's no way for Eve to be forced to do 2^n or n^100 or even n^3 work
- Happily, there's another way. Go look up Diffie-Hellman key exchange.
  - Similar in that Bob sends value to Alice
    - Then Alice chooses a random number, does some work on value and sends result to Bob
  - Different in that Bob only sends a small amount of information
  - Different in that the difficulty for eavesdropper relies on an non-proven assumption
    - Eavesdropper can't "efficiently" figure out the key, as far as they know