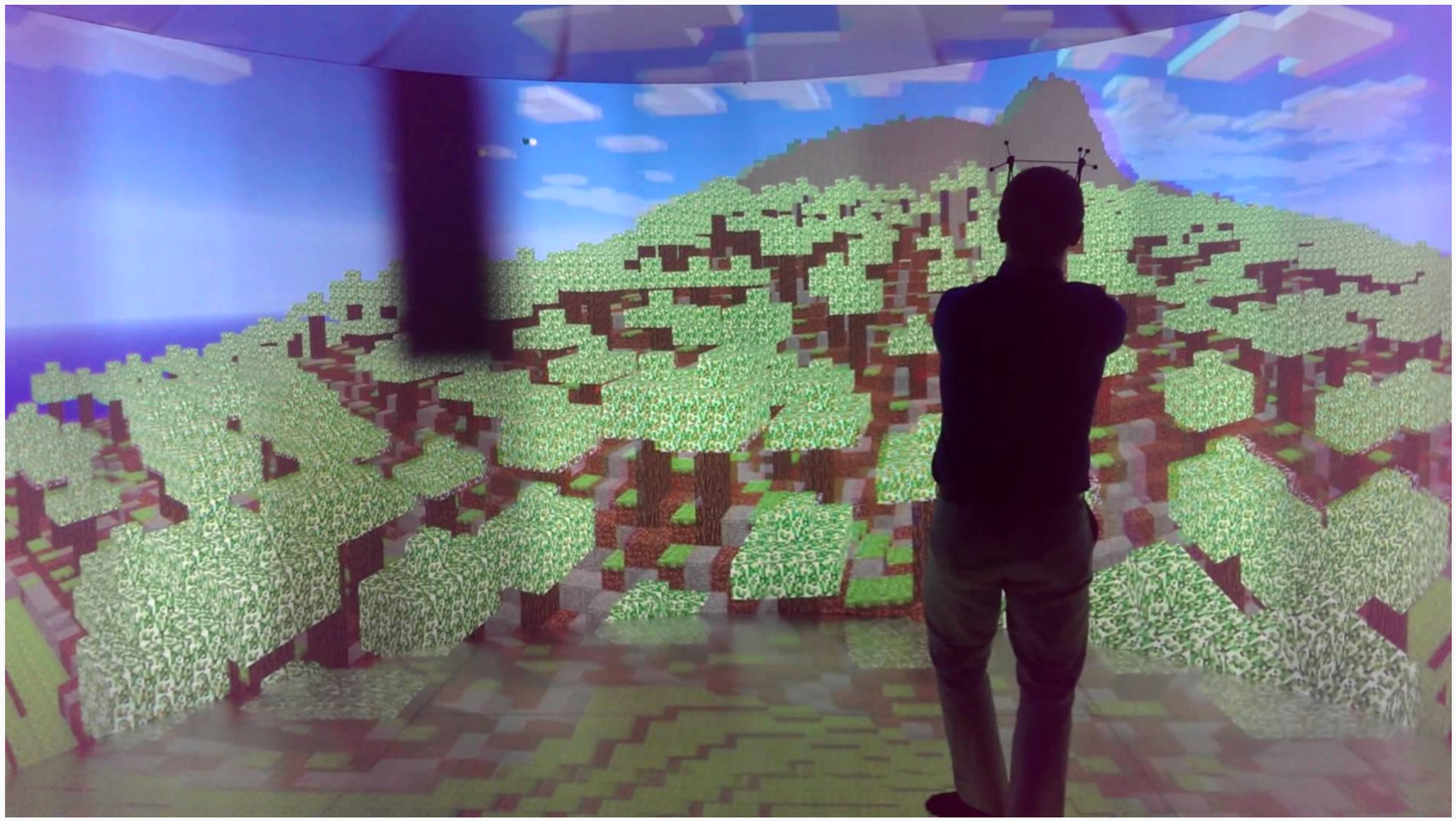
Unit 9: Cryptography

Dave Abel

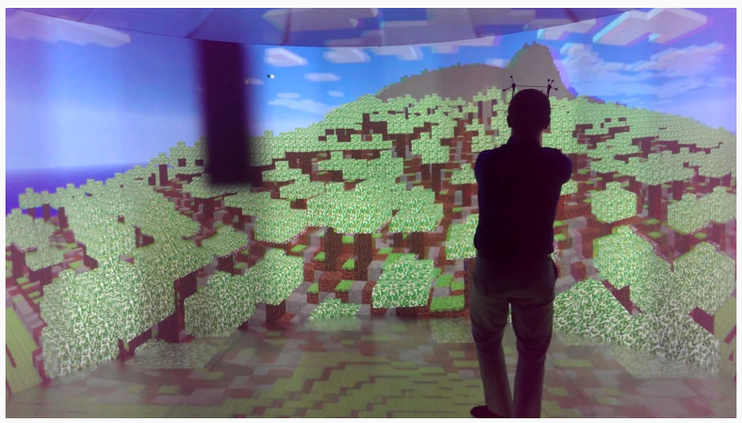
April 15th, 2016

Yurt, Round Two



Yurt, Round Two

- If you want to go, email me with subject “Yurt”
- Specify which time you’d like to go:
  - Monday, May 9th from 2pm-3pm
  - Tuesday, May 10th from 11am-noon



Outline

- Some excellent questions from you all!
- Randomness
- Cryptography vs. Security
- Security Breaches, Hacking, and Chickens and Eggs

Some Questions (From Y'all)!

Q: Why do we use OWFs for cryptography if we're still not sure about SOLVE = VERIFY? Seems Risky!

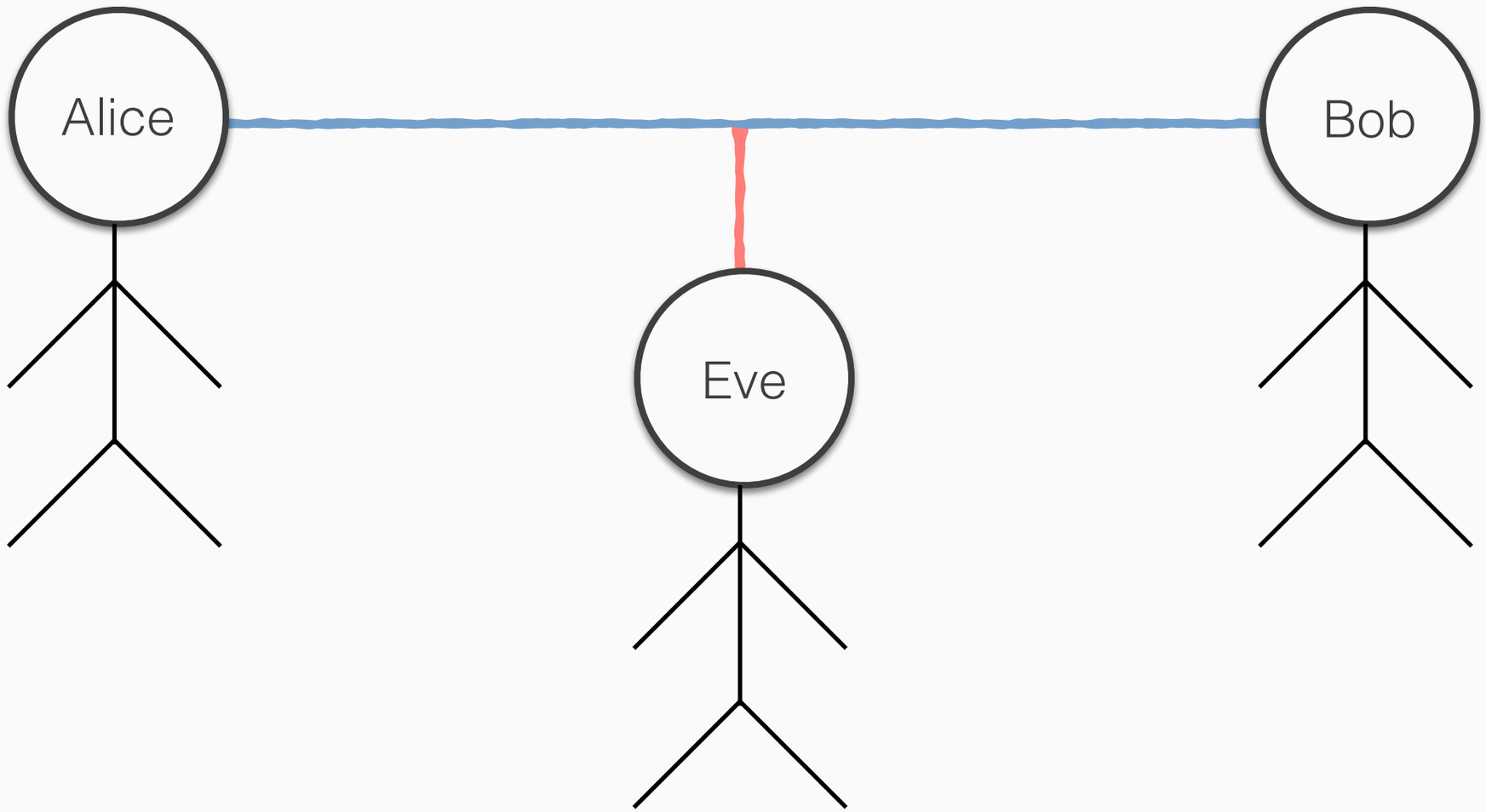
A1: If SOLVE = VERIFY, then there *is* an efficient way to break our crypto systems, but we don't know of it yet. It may be incredibly difficult to come up with the algorithm!

A2: Many folks are 99% confident SOLVE is not the same as VERIFY

A3: Good point! This does seem a little nutty. Folks are researching other methods, now.

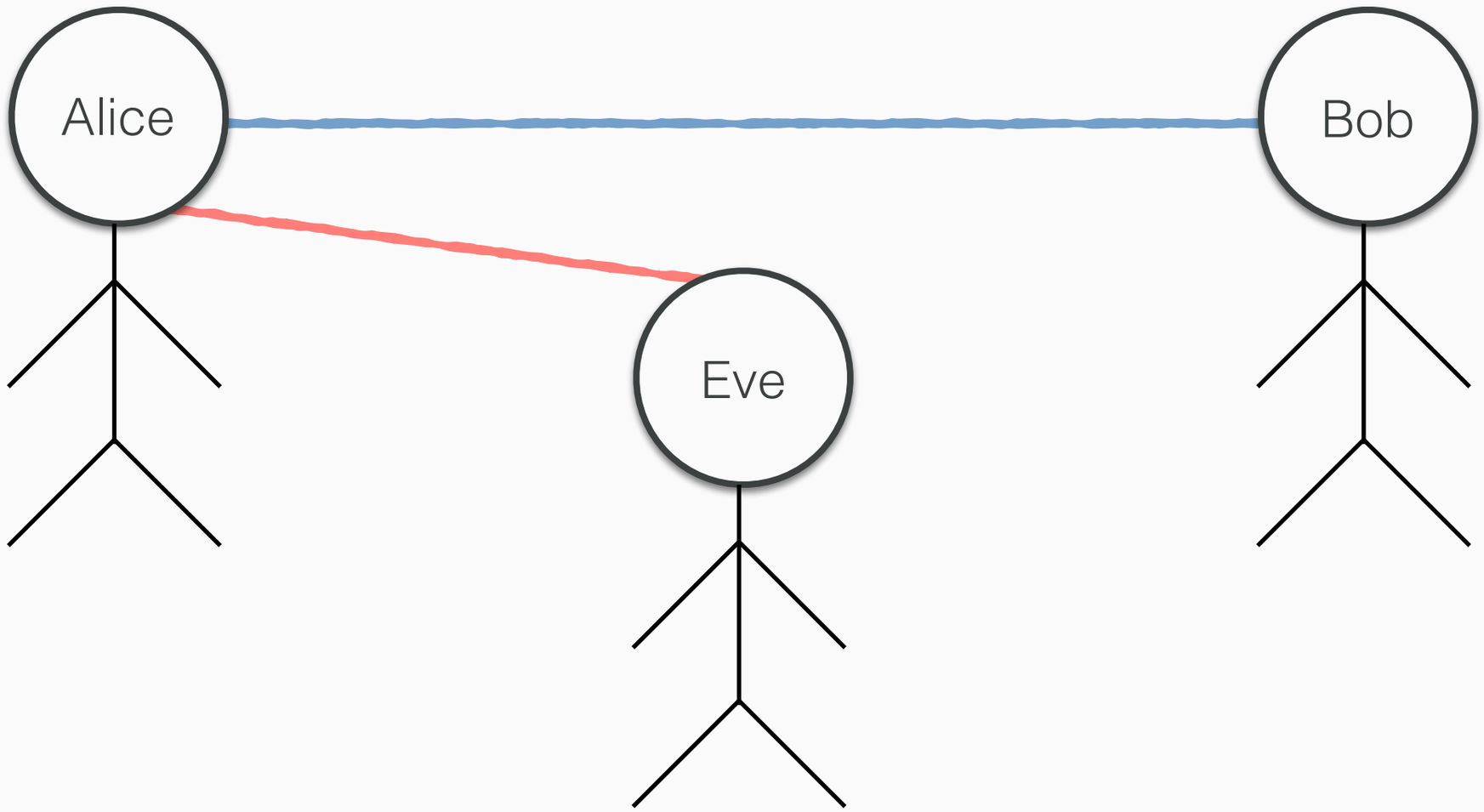
Some Questions (From Y'all)!

Q: What if Eve isn't just able to look at the encrypted message? What if we change her powers up?



Some Questions (From Y'all)!

Q: What if Eve isn't just able to look at the encrypted message? What if we change her powers up?



Some Questions (From Y'all)!

Q: What if Eve isn't just able to look at the encrypted message? What if we change her powers up?

A: This introduces the more general field of *Security*, which is concerned with protecting the information on our machines from intruders. We'll talk about this more today!

Some Questions (From Y'all)!

Q: How are there ever security breaches, then? If all this is secure?

A: Many modern crypto systems are actually a bit *slow*. Not crazy slow, but will take a few minutes. We don't really want to wait that long, practically, so instead there are systems that are *almost* as secure but are faster.

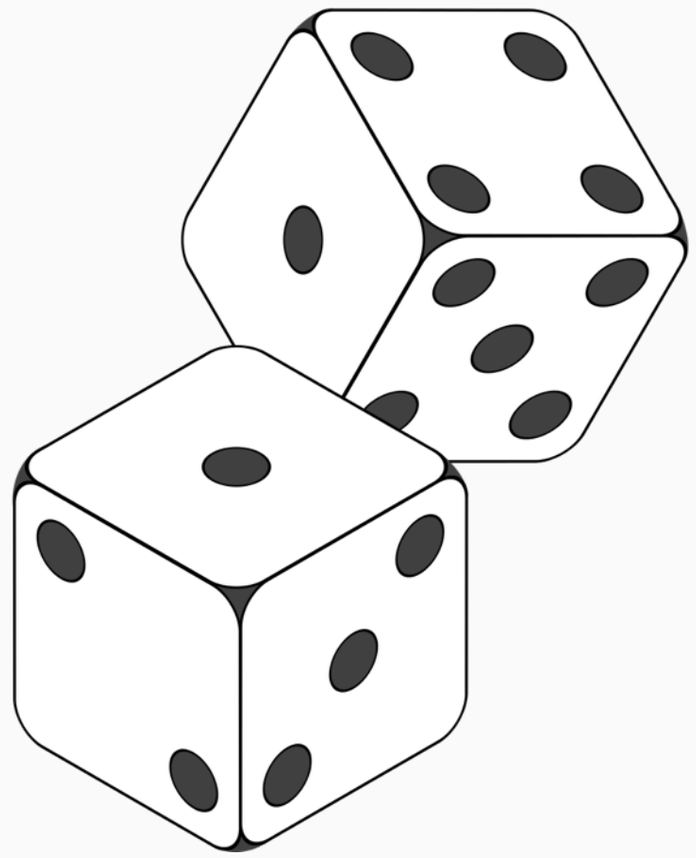
Some Questions (From Y'all)!

Q: How are there ever security breaches, then? If all this is secure?

A: Many modern crypto systems are actually a bit *slow*. Not crazy slow, but will take a few minutes. We don't really want to wait that long, practically, so instead there are systems that are *almost* as secure but are faster.

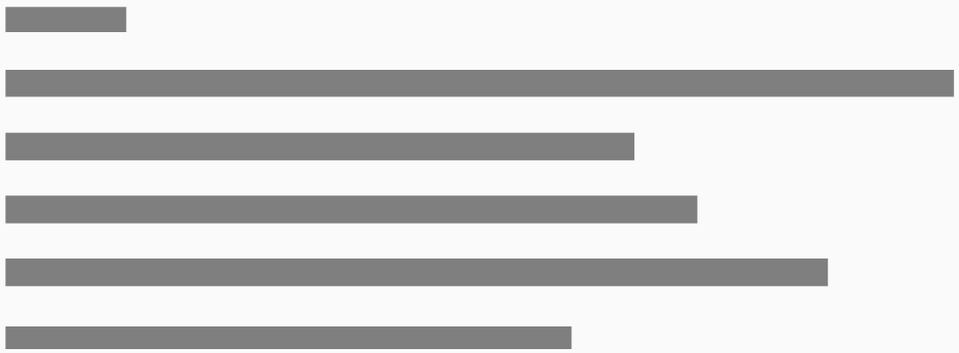
A: Someone could still videotape you writing your password or just guess it. These sorts of vulnerabilities are dealt with by the field of Security, not Cryptography.

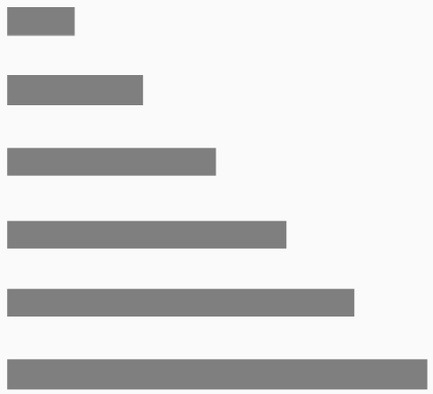
Randomness



Randomness

- Earlier notion of randomness from Theory!
- The higher the Kolmogorov complexity, the more random an object is.





Randomness

- But how about *events*? Really, we want this:

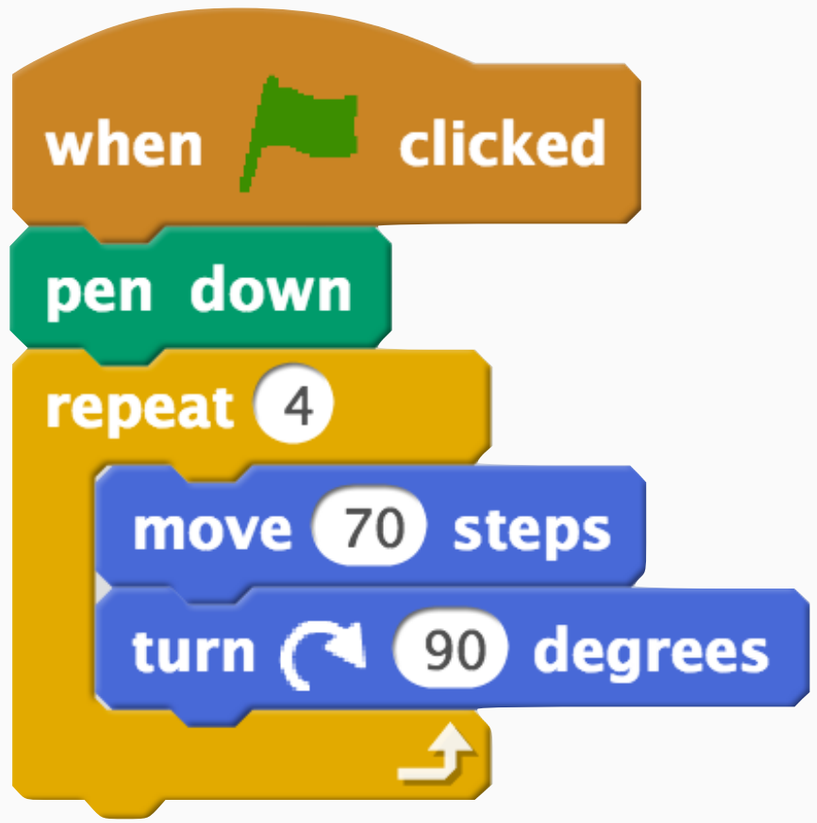
Randomness

- But how about *events*? Really, we want this:

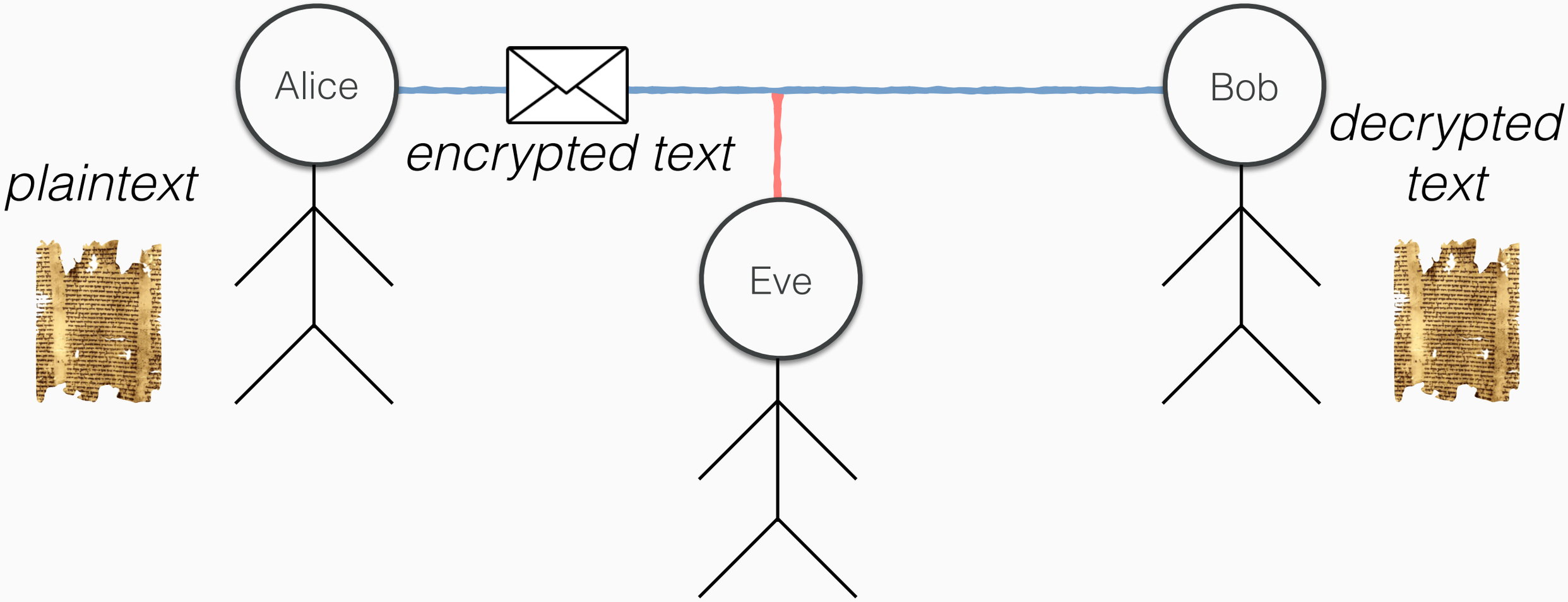
- But suppose we didn't have this block. How could we write a block to carry out random operations?

Randomness

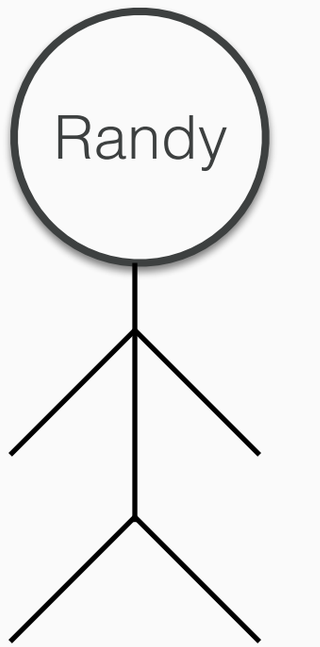
- Everything has been so *deterministic*:

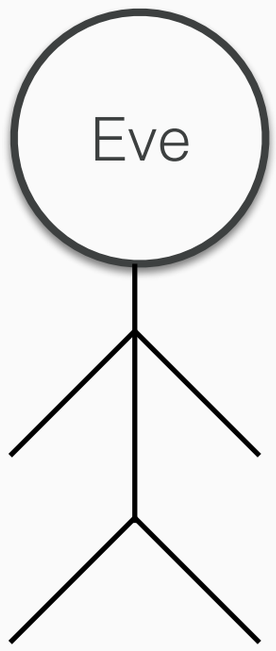


Randomness & Crypto

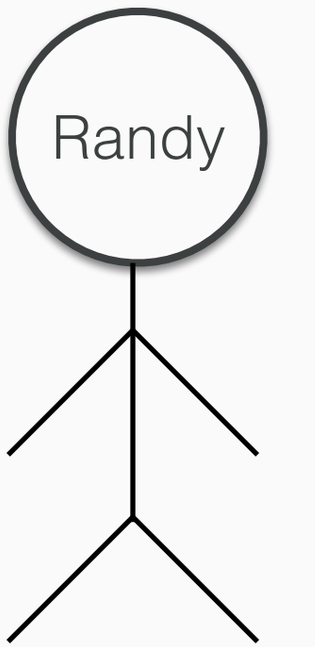


Randomness & Crypto

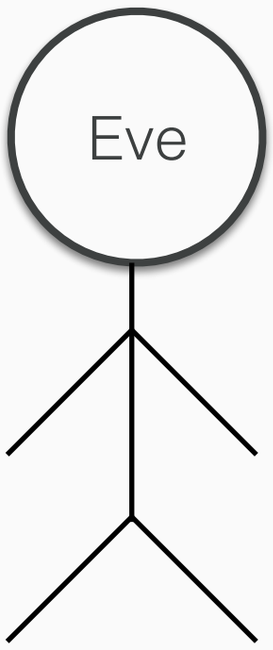




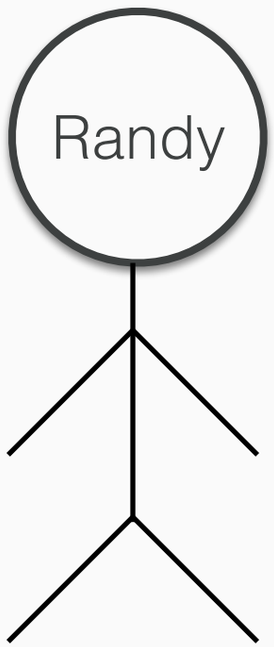
Randomness & Crypto



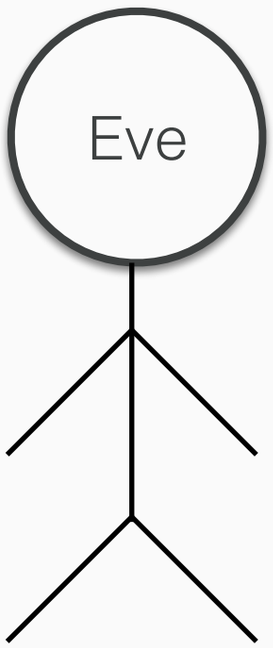
"I have figured out a way to simulate random coins!"



Randomness & Crypto

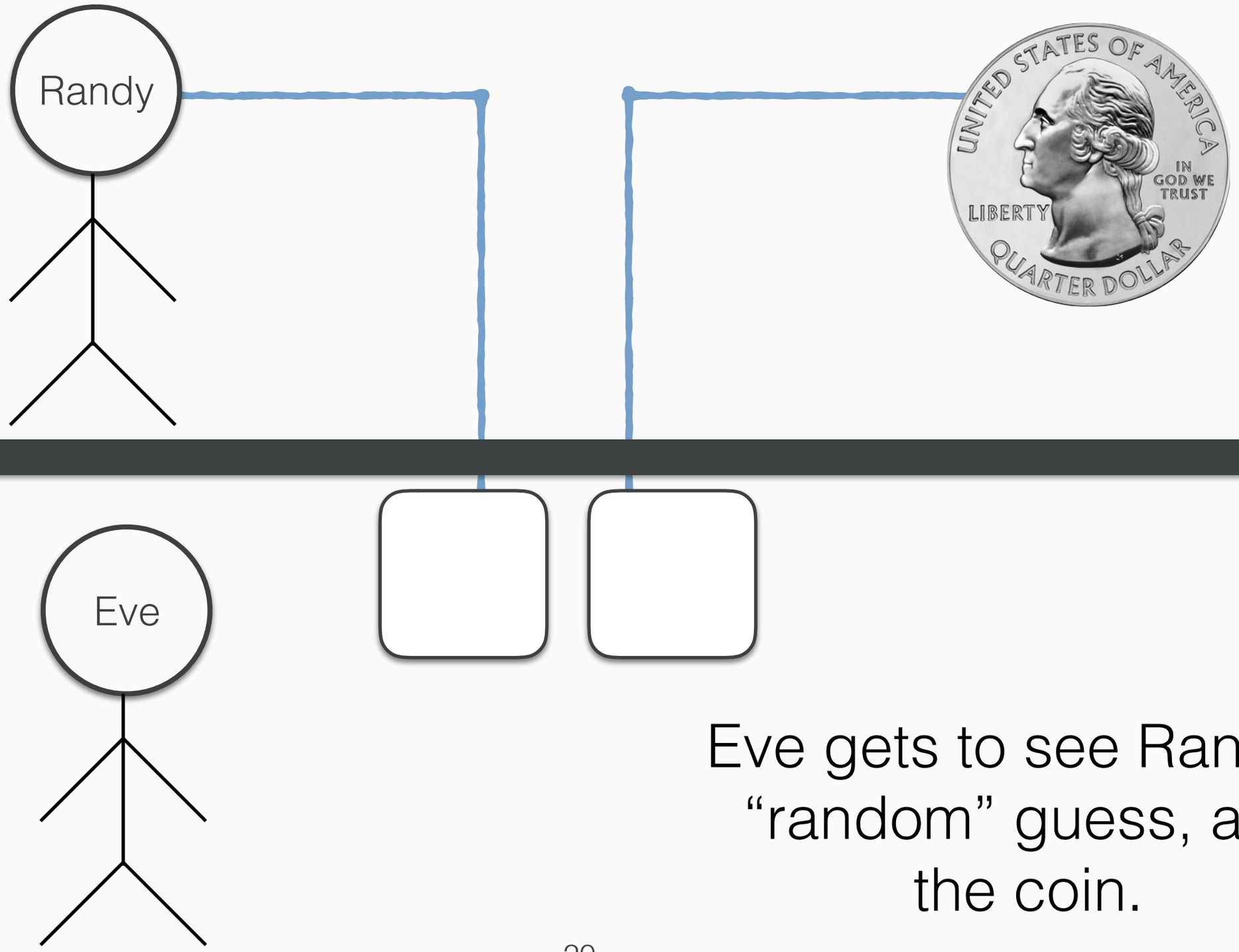


"I have figured out a way to simulate random coins!"



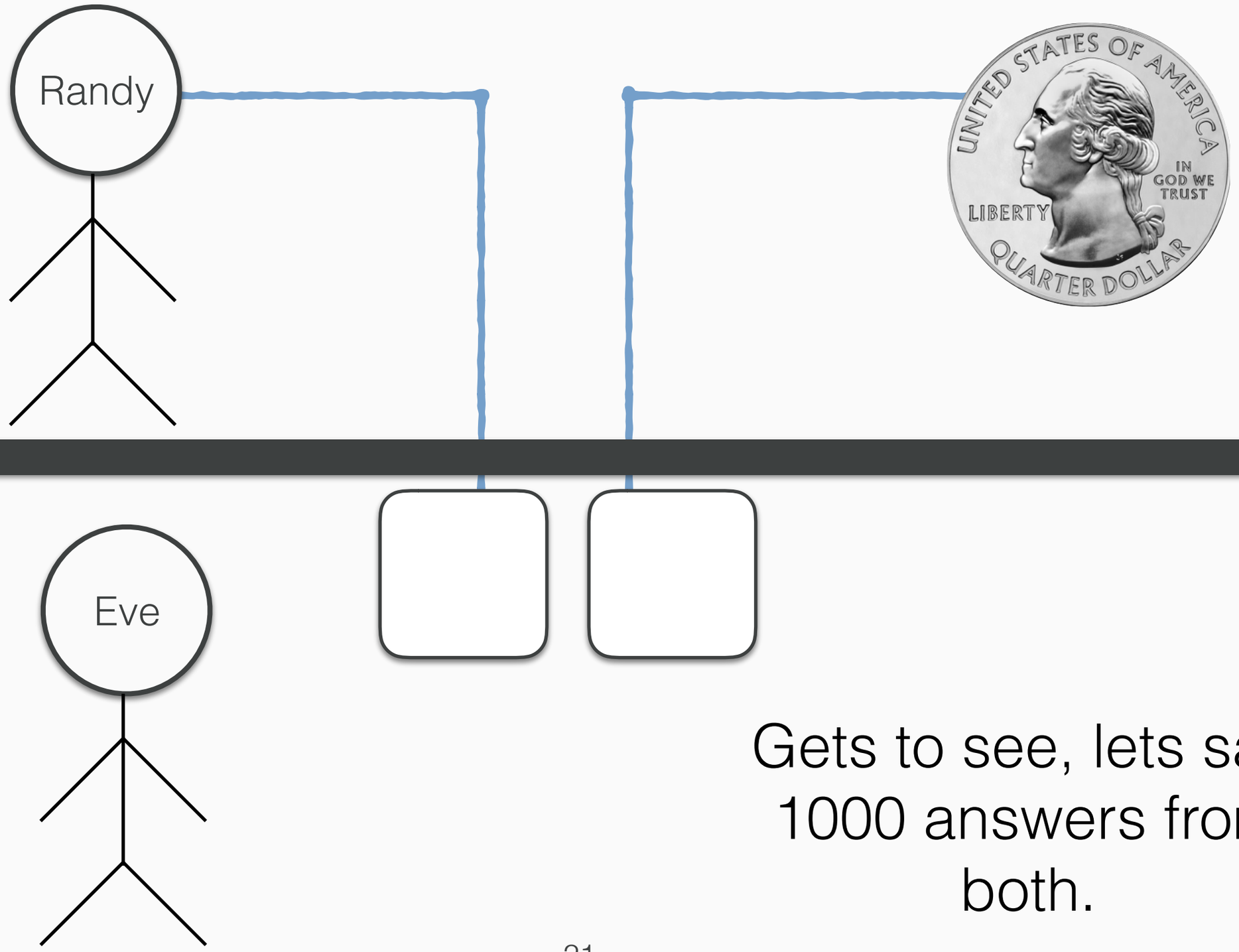
"No way…"

Randomness & Crypto



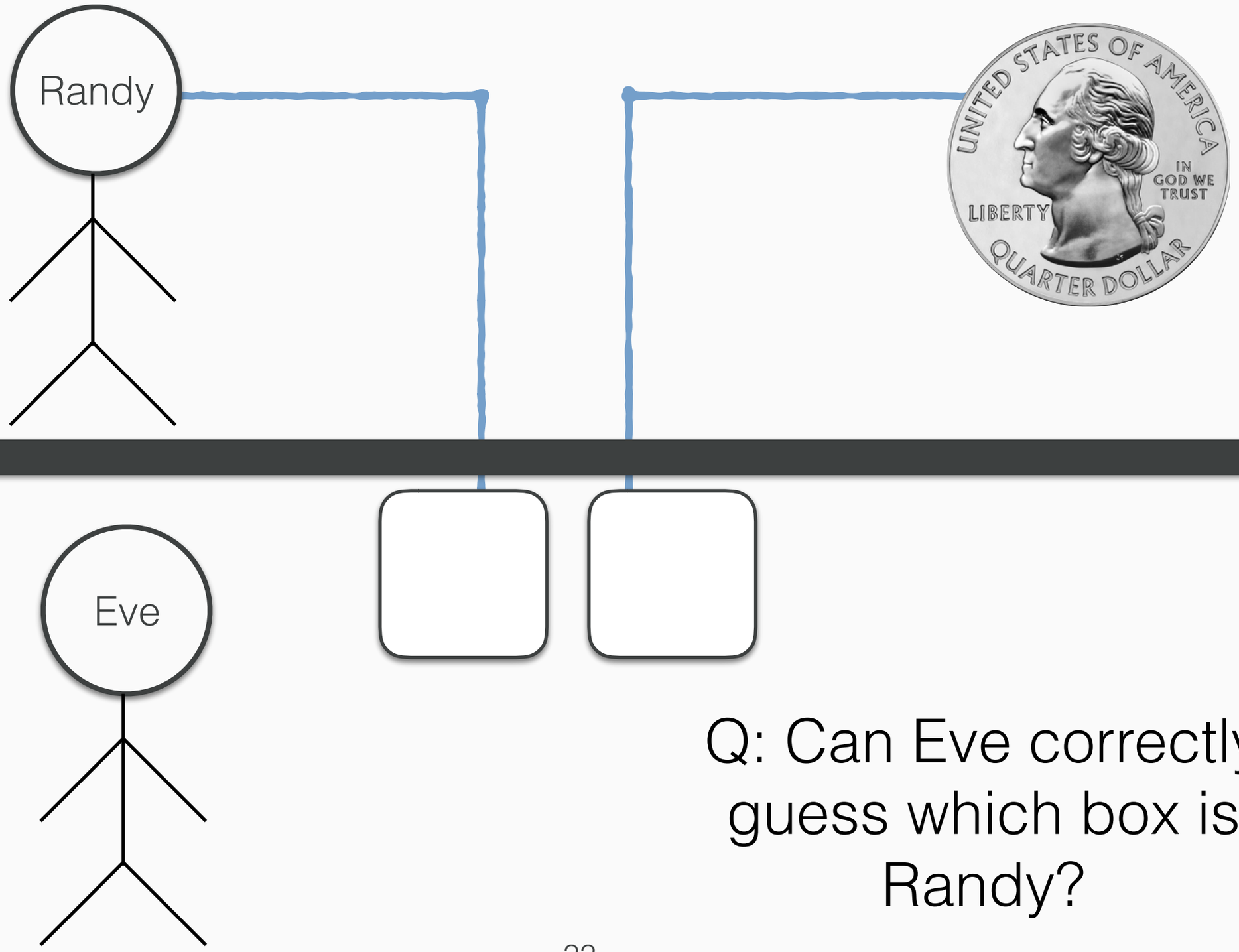
Eve gets to see Randy's "random" guess, and the coin.

Randomness & Crypto



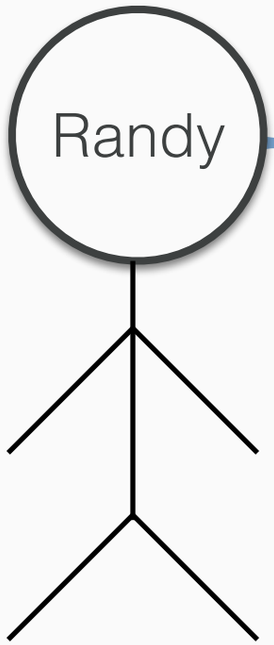
Gets to see, lets say, 1000 answers from both.

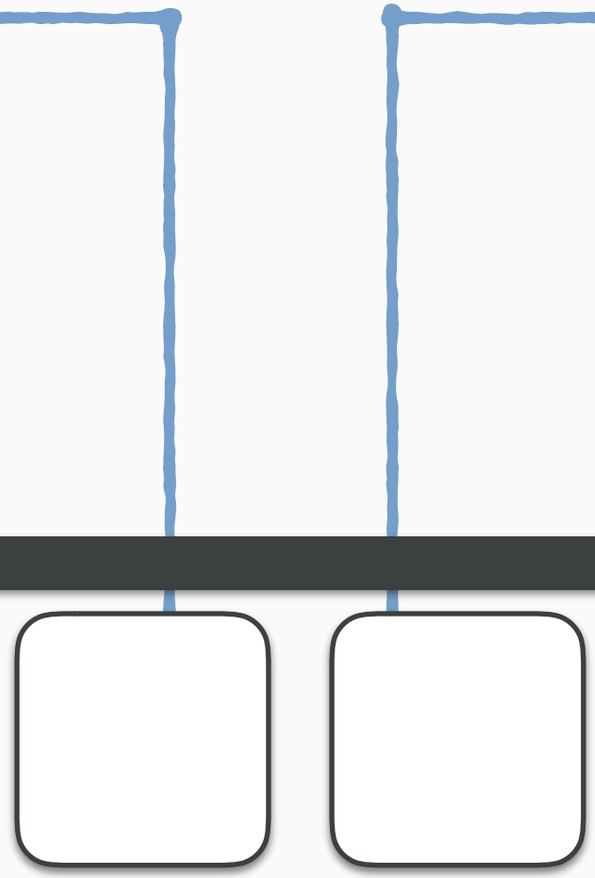
Randomness & Crypto

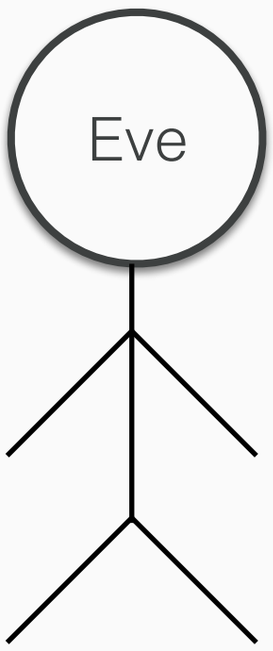


Q: Can Eve correctly guess which box is Randy?

Randomness & Crypto







Q: Can Eve correctly guess which box is Randy?

If Eve can be right more than 1/2 the time, Randy isn't Random

(Psuedo)-Randomness

- **Definition:** A process is *pseudorandom* if an adversary, Eve, cannot distinguish the process from a truly random process!

(Psuedo)-Randomness

- **Definition:** A process is *pseudorandom* if an adversary, Eve, cannot distinguish the process from a truly random process!
- **Q: Can humans do this?**

“Truly” Random?

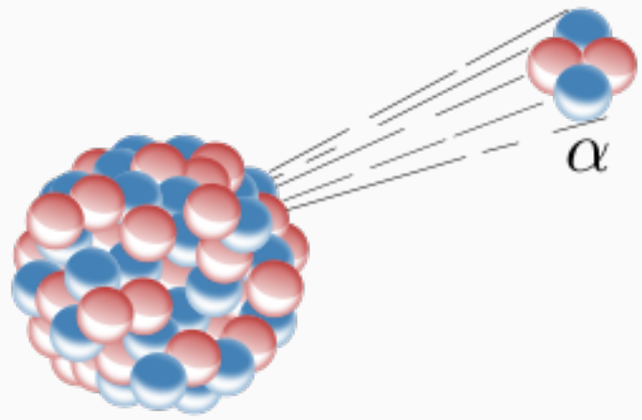
True Randomness?

We may regard the present state of the universe as the effect of its past and the cause of its future. An intellect which at a certain moment would know all forces that set nature in motion, and all positions of all items of which nature is composed, if this intellect were also vast enough to submit these data to analysis, it would embrace in a single formula the movements of the greatest bodies of the universe and those of the tiniest atom; for such an intellect nothing would be uncertain and the future just like the past would be present before its eyes.

- Pierre Simon Laplace, A Philosophical Essay on Probabilities

“Truly” Random?

- We consider many phenomena in the world to exhibit *truly* random behavior.
- Anything that does not follow a pattern.
- Examples:
  - Atmospheric White Noise
  - Coin Flips
  - Radioactive Decay



Psuedorandomness

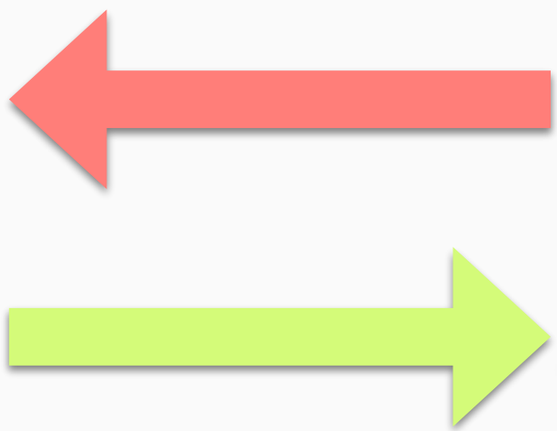
- **Definition:** A process is *pseudorandom* if an adversary, Eve, cannot distinguish the process from a truly random process!
- Q: So how do we achieve this?

Psuedorandomness

- **Definition:** A process is *pseudorandom* if an adversary, Eve, cannot distinguish the process from a truly random process!

- Q: So how do we achieve this?

- A: One Way Functions!



OWFs as Pseudorandom Generators

- Intuition: If it's easy for you to figure out why something happened, then it's not really random.

- One Way Function: It's hard to figure out the input, given the output.

- Conclusion: we can extend One Way Functions to create Pseudo Random Number Generators!

OWFs as Pseudorandom Generators

- Intuition: If it's easy for you to figure out why something happened, then it's not really random.

- One Way Function: It's hard to figure out the input, given the output.

- Conclusion: we can extend One Way Functions to create Pseudo Random Number Generators!

Cryptography vs. Security

- Cryptography is about the study of things like One Way Functions, Randomness, and Diffie-Helman Key Exchange.

- It teaches us that, if a “hacker” wants to break into our systems, they’re not going to do it by trying to break our One Way Function.

- But that doesn’t mean a hacker couldn’t just guess our password! Considerations like these are a part of the more general field of *security*, not cryptography.

Security

- Let's look at one problem: password cracking.
- Cryptography tells us if we play by the rules and use all the nice tools we went over Wednesday, that Eve can't listen to Bob and Alice's communication.
- Computer Security tells us, "don't use the word '*password*' as your password".

Problem: Password Cracking

- INPUT: A user on Facebook/Amazon/Netflix/etc.
- OUTPUT: That user's password.

Password Cracking Idea

- Machine Learning Approach! Treat it like classification.

Any thoughts? How might we do this?

Password Cracking Idea

- Machine Learning Approach! Treat it like classification.

Any thoughts? How might we do this?

Training Data? Features?

Password Cracking Idea

- Machine Learning Approach! Treat it like classification.
- Features: user's age, name, location, interests, etc.
- Training Data: user data + user's password.

Password Cracking Idea

- Machine Learning Approach! Treat it like classification.
- Features: user's age, name, location, interests, etc.
- Training Data: user data + user's password.
- Idea: maybe all people named "Petunia" use passwords that involve their name.

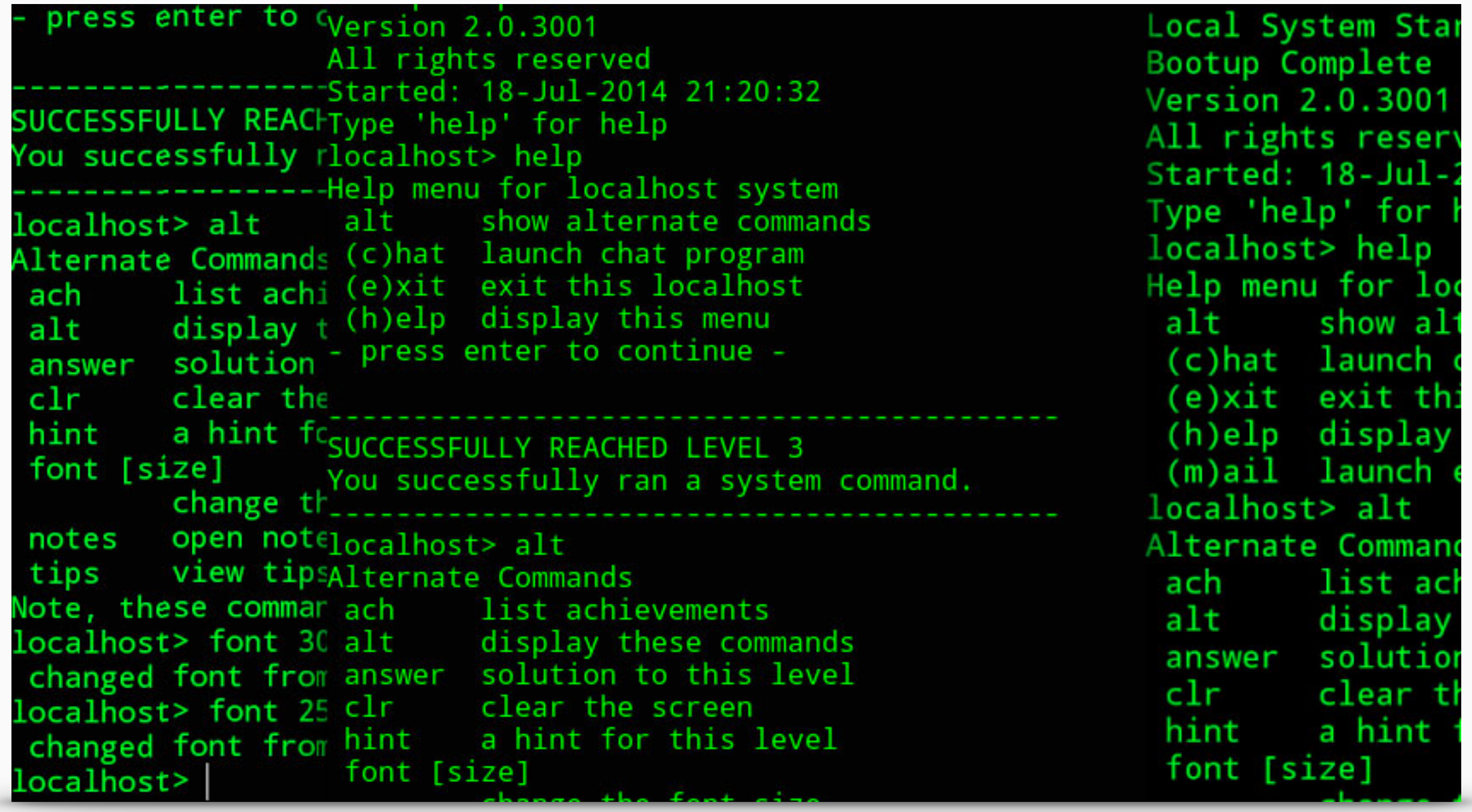
Most Common Passwords

- 123456
- password
- 12345678
- qwerty
- abc123
- 123456789
- 111111
- 1234567
- iloveyou
- photoshop
- adobe123
- 123123
- admin
- 1234567890
- letmein
- 1234
- monkey
- shadow
- sunshine

Password Cracking

- Idea one: machine learning!
- Idea two: guess the top 20, 50, 1000, or so passwords.
- Idea three: try replacing I's with 1's, O's with 0's, etc.
- Q: How many do you think we'd get?

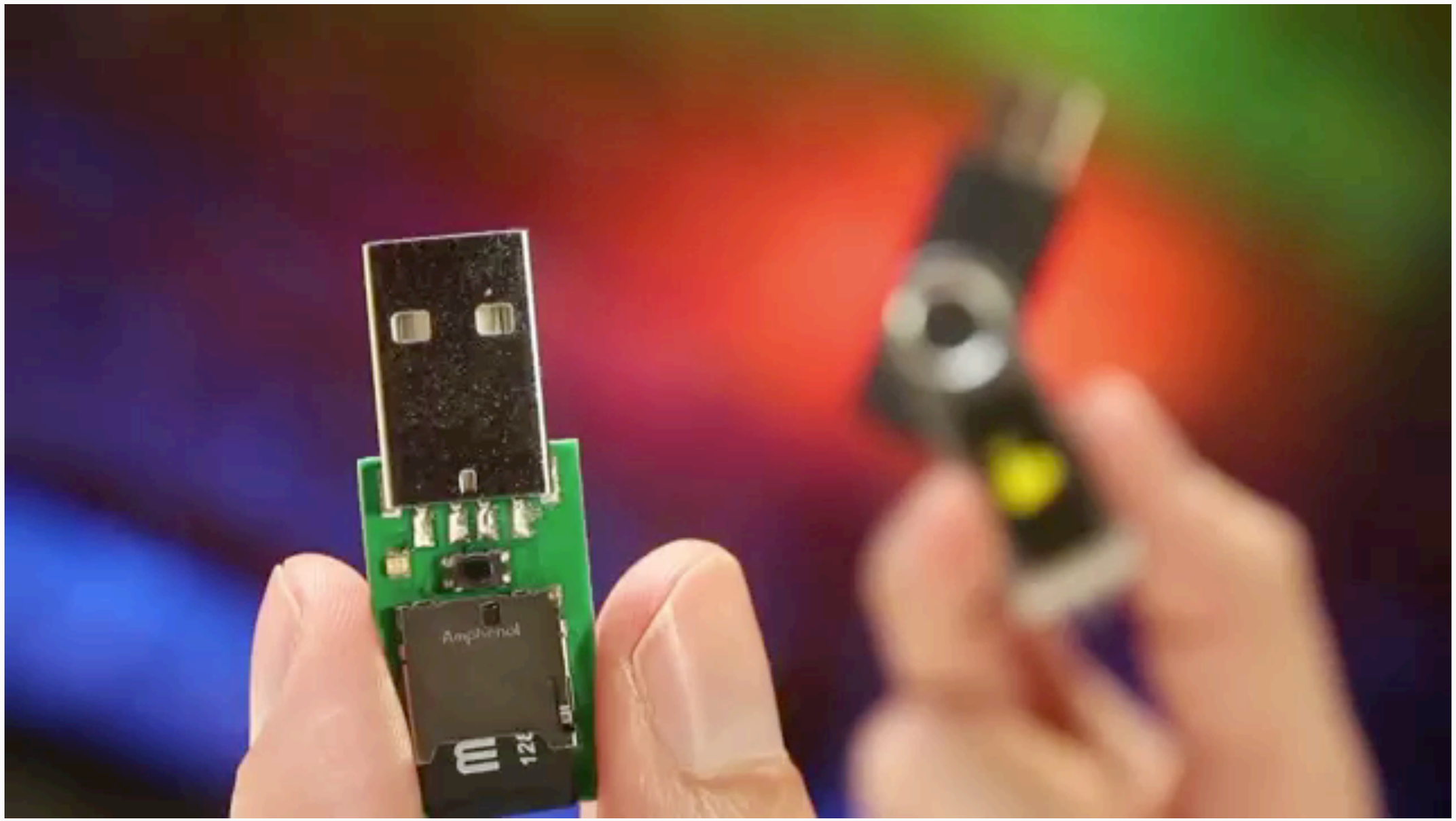
Hacking


- press enter to
Version 2.0.3001
All rights reserved
Started: 18-Jul-2014 21:20:32
Type 'help' for help
localhost> help
Help menu for localhost system
alt show alternate commands
(c)hat launch chat program
(e)xit exit this localhost
(h)elp display this menu
- press enter to continue -
SUCCESSFULLY REACHED LEVEL 3
You successfully ran a system command.
localhost> alt
Alternate Commands
ach list achievements
alt display these commands
answer solution to this level
clr clear the screen
hint a hint for this level
font [size]
localhost>
Local System Star
Bootup Complete
Version 2.0.3001
All rights reserv
Started: 18-Jul-2
Type 'help' for h
localhost> help
Help menu for loc
alt show alt
(c)hat launch c
(e)xit exit thi
(h)elp display
(m)ail launch e
localhost> alt
Alternate Comman
ach list ach
alt display
answer solutio
clr clear th
hint a hint
font [size]

Hacking


The Visual Microphone:
Passive Recovery of Sound from Video
Abe Davis
Michael Rubinstein
Neal Wadhwa
Gautham J. Mysore
Fredo Durand
William T. Freeman

Hacking



Chickens and Eggs…

- Security folks develop systems of defense: let's say, wrapping everything in metaphorical cardboard.
- Hackers, in response, bring box cutters.
- Security folks, in response, get metal cages.
- Hackers, in response, bring fence cutters.
- And so it goes…

Have a great weekend!