Discussion 11:
Special Topics

TA: **Jerry Chen**
Email: **jerry.c@berkeley.edu**
TA Website: **jerryjrchen.com/cs61a**

Attendance

Sign in at bit.do/jerrydisc

OR

Come to me for check-in

Announcements

Final is coming up

- Use 50% of your time studying material since mt2
- Lots of review sessions during RRR week! Check the course calendar
    - I'm teaching a review on MapReduce next Tues in 405 Soda
- **Go to class on Friday! It'll be worth it :)**

CS 61A

Function Abstractions	Data Abstractions	Programming Paradigms
Control	Lists	OOP
HOFs	Recursive data structures	Function
Recursion	Growth	Declarative

Computer Science

There's more to CS than 61A!

(There's 61B)

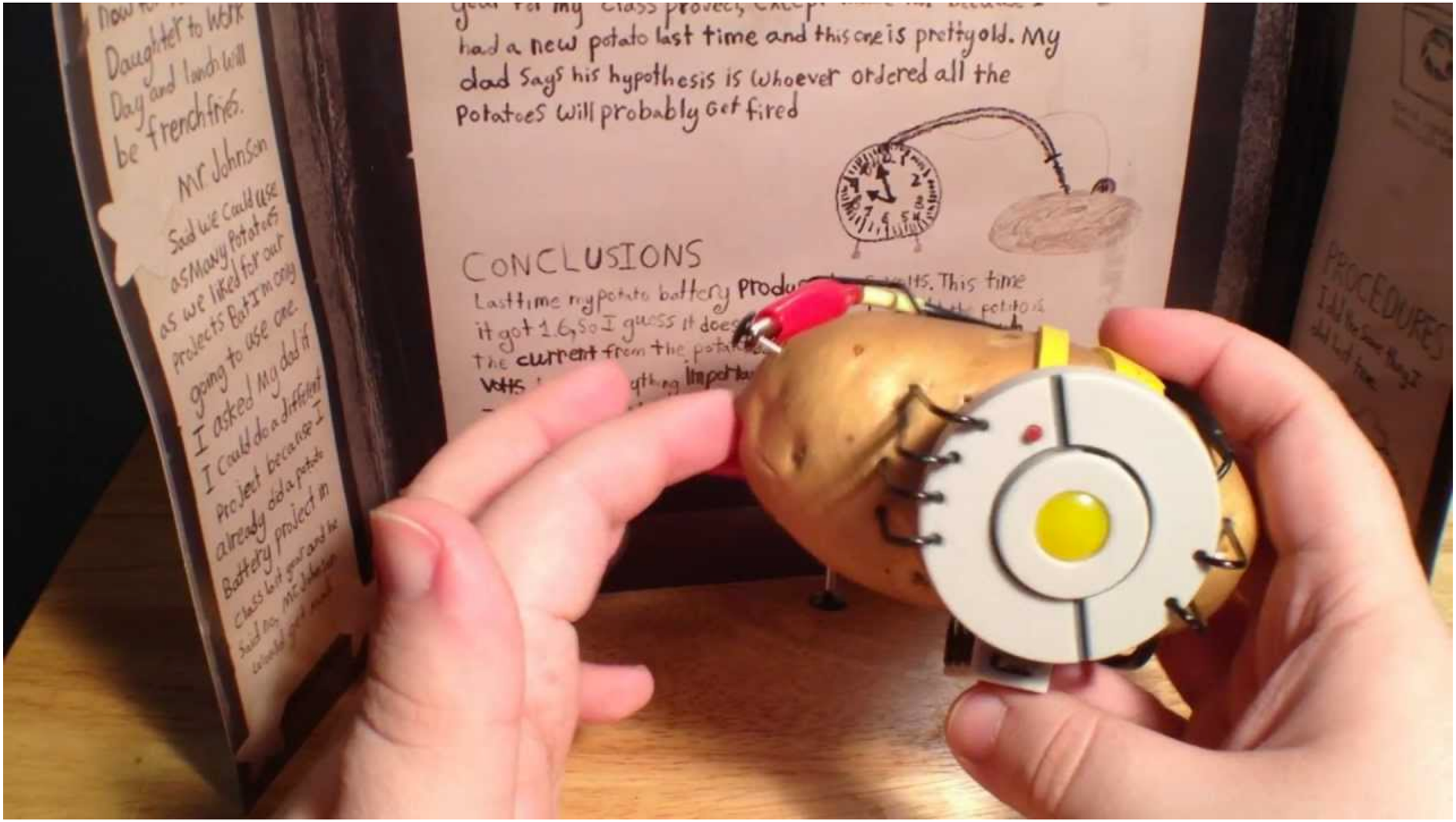
(Ok, ok... bad joke, I know)

Agenda

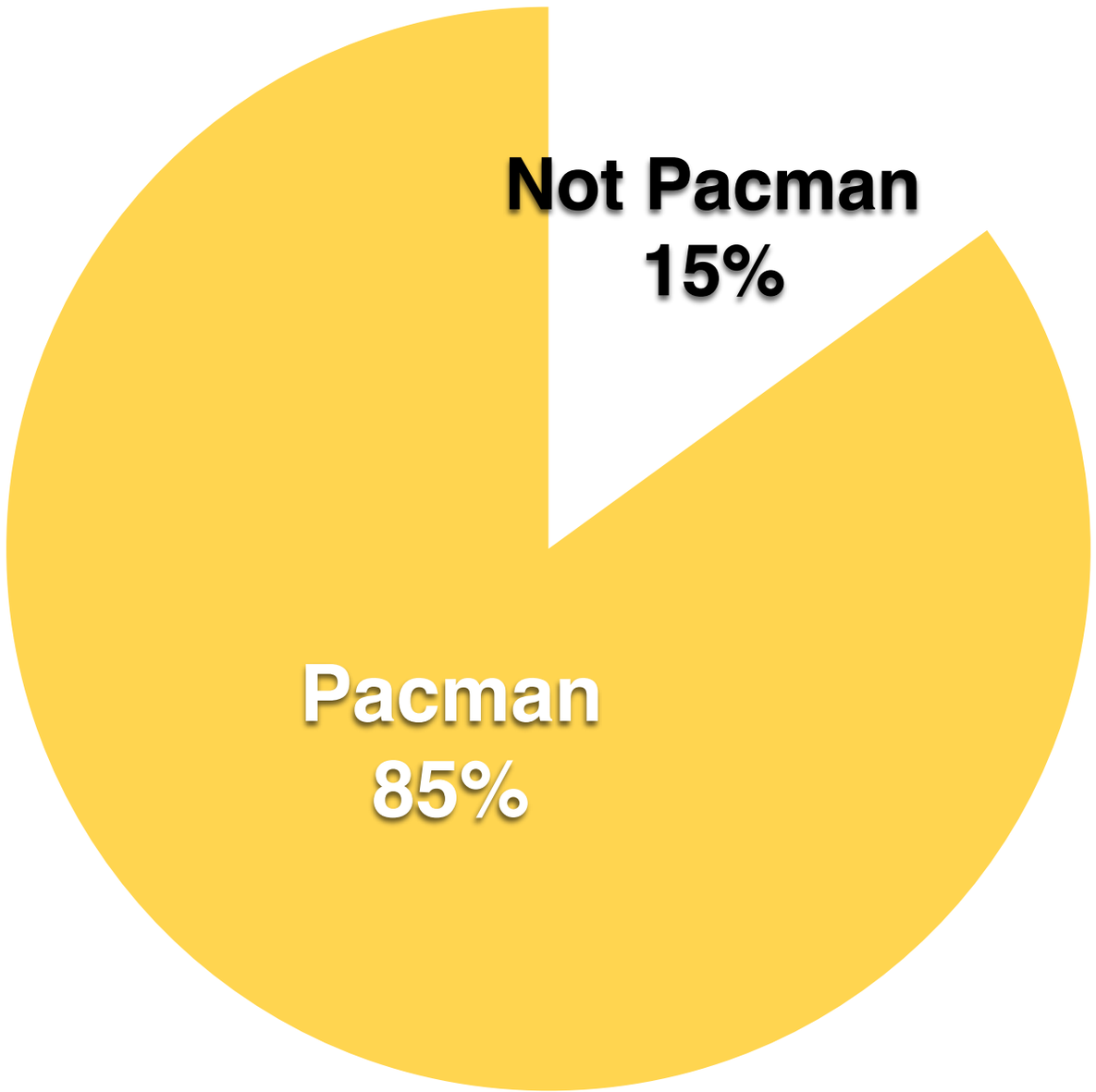
1. Very Cool Stuff
2. Cool Stuff
3. Open OH

Not expected to understand everything (anything)!
But ask questions if you're interested :)

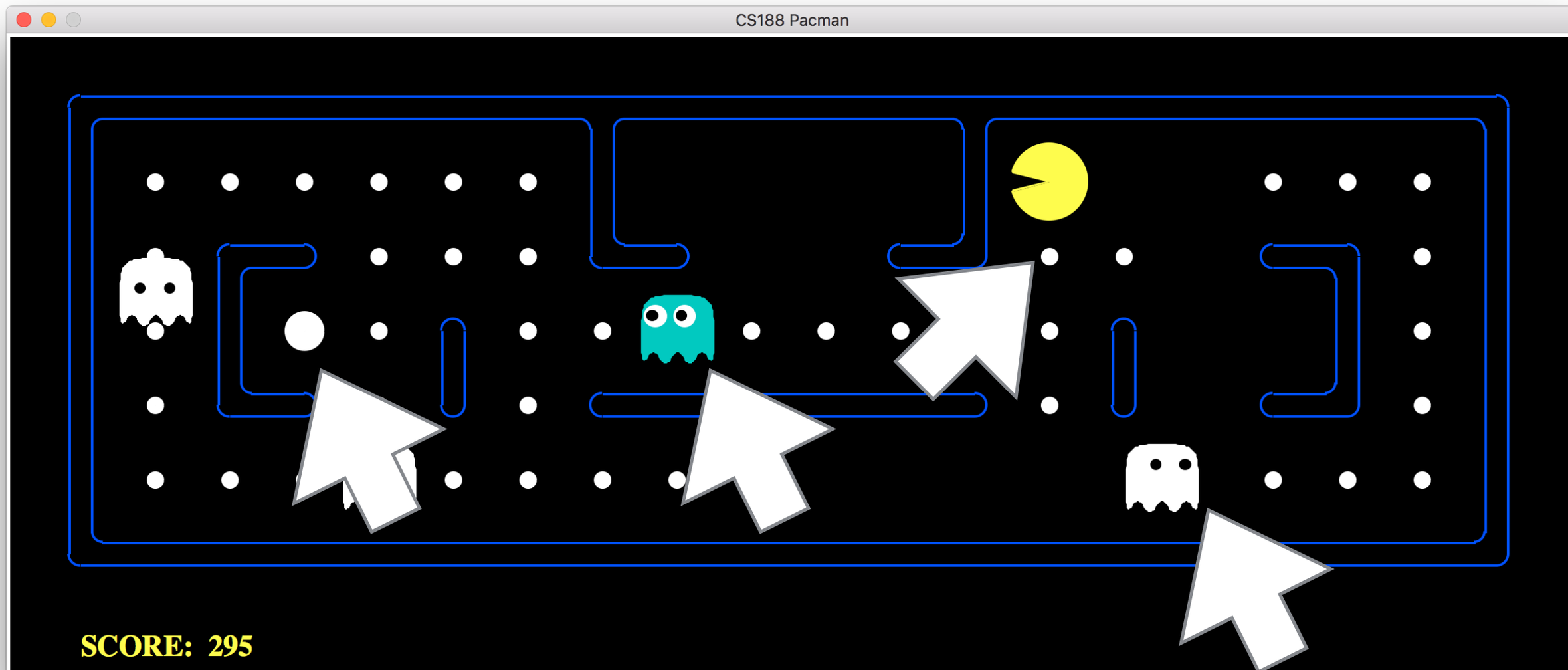
Artificial Intelligence



Pacman



Pacman



"Features"

Pacman

Reinforcement Learning

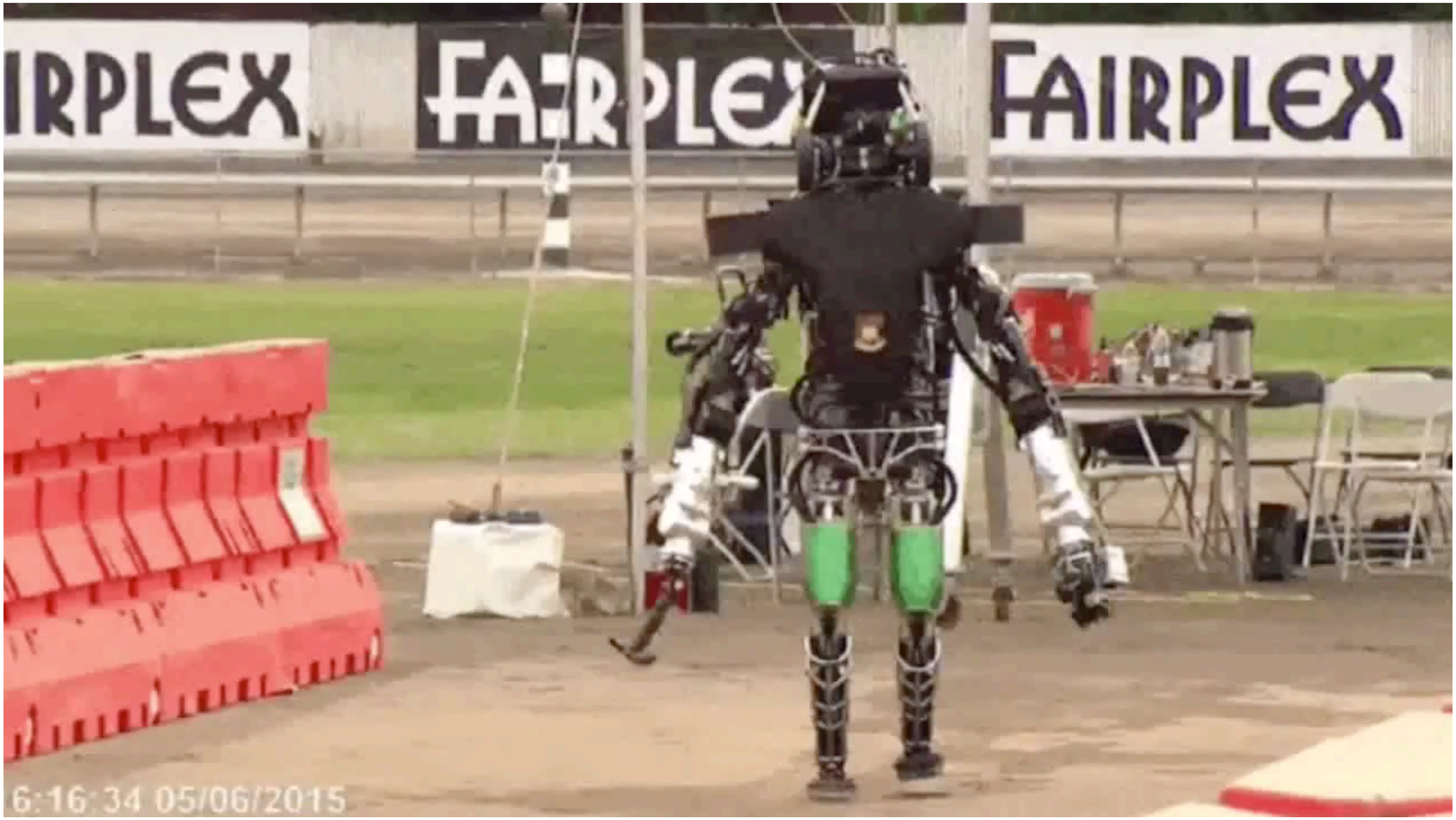
- Specifically, Q-learning
- Big idea: observe **features**, learn how important they are (**weights**)
- Computer learns the weights through trial and error

Pacman

Finally, play!

Use the weights you learned to pick the best move

Artificial Intelligence



A Compilation of Robots Falling Down at the DARPA Robotics Challenge
IEEE Spectrum

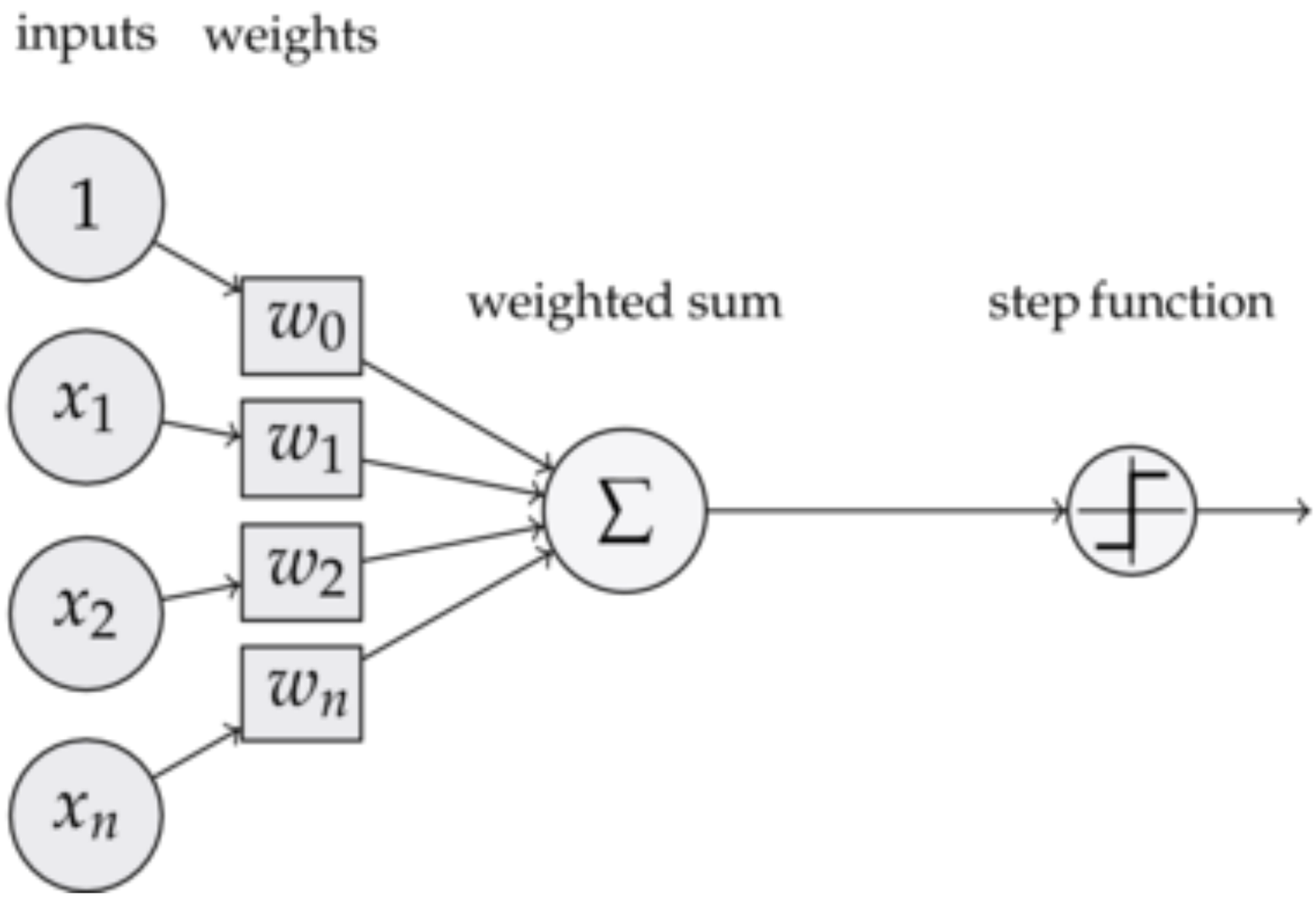
Artificial Intelligence

Socks

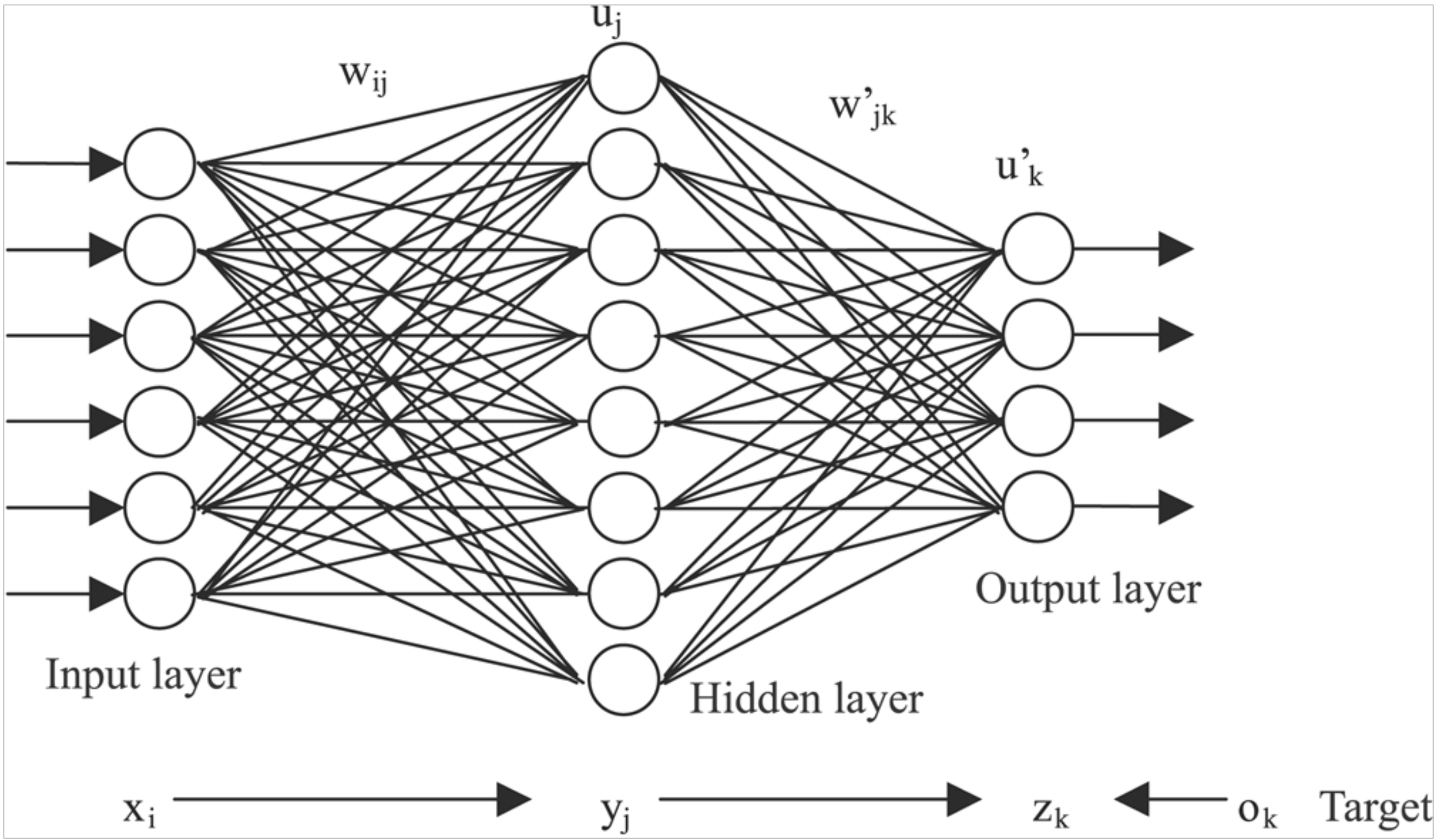
Artificial Intelligence

Neural Networks

- Learn the weights **and** the features!



Artificial Intelligence



Artificial Intelligence

Neural Networks

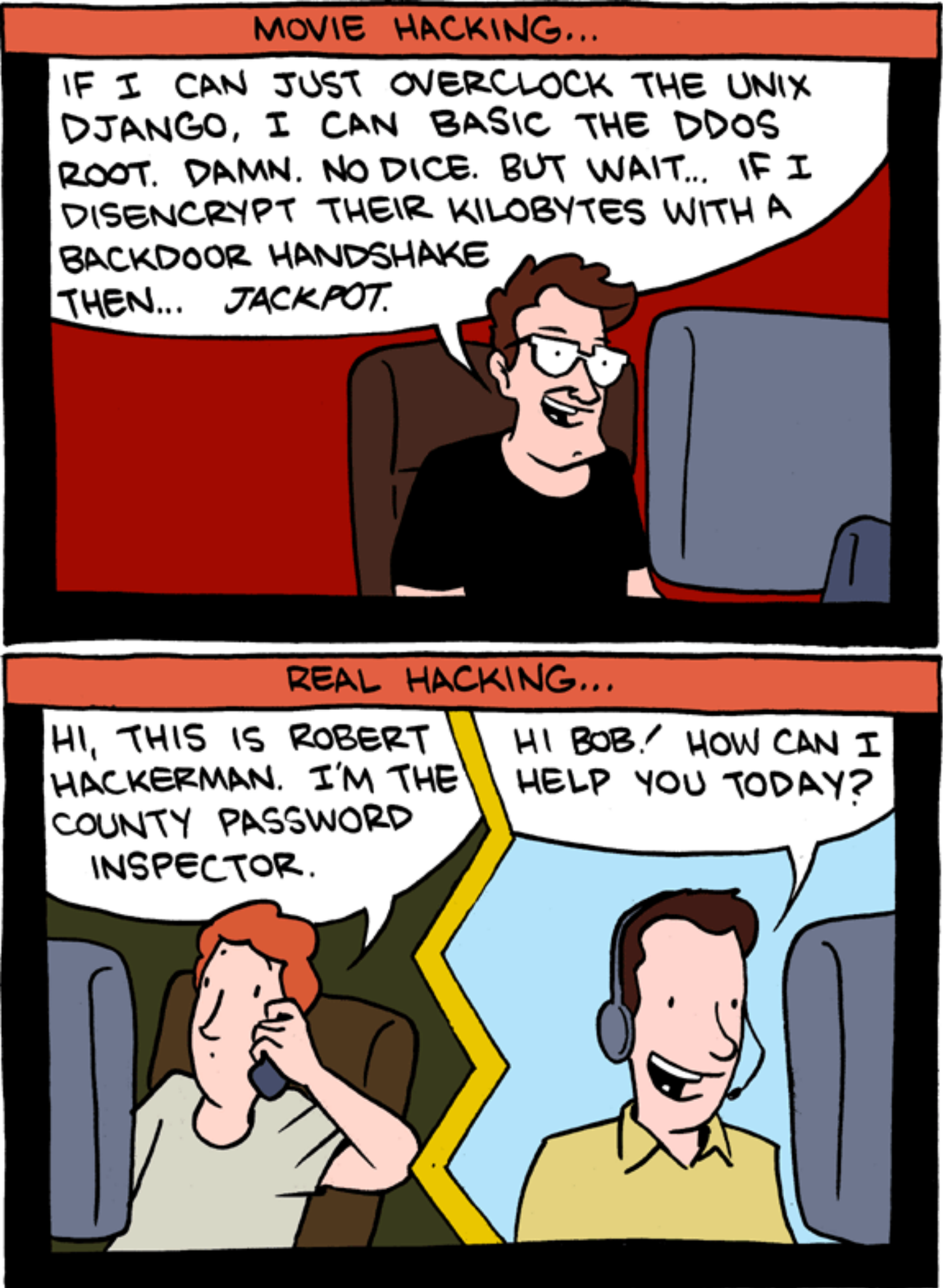
http://playground.tensorflow.org/

https://quickdraw.withgoogle.com

When classification goes wrong: https://youtu.be/mSFHKAvTGNk?t=16m48s

More learning: https://www.youtube.com/watch?v=xOCurBYI_gY

Computer Security



Phishing & scams are one of the more common types of attacks today

http://www.smbc-comics.com/?id=2526

Encryption

Caesar Cipher

Original	Encrypted
"Sunset tomorrow is at five oclock."	"Vxqvhw wrpruurz lv dw ilyh rforfn."
"We will attack at sunset tomorrow "	"Zh zloo dwwdfn dw vxqvhw wrpruurz "

Are we done?

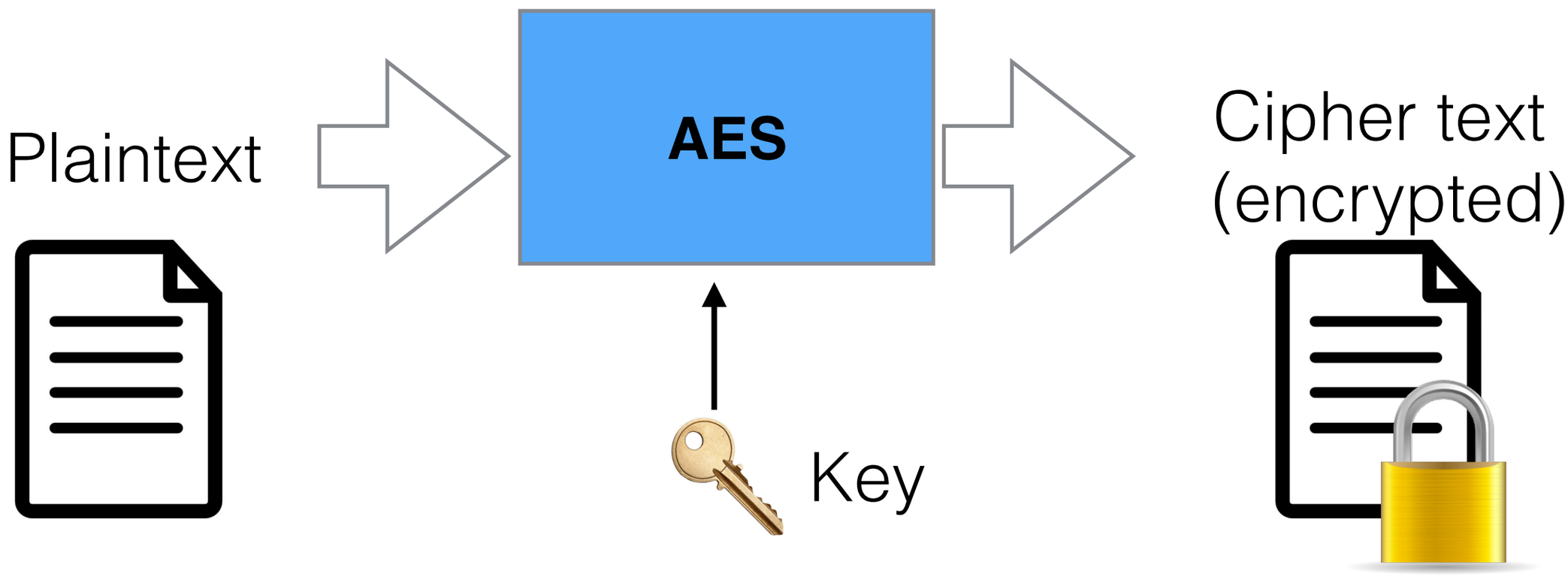
Encryption

Caesar Cipher

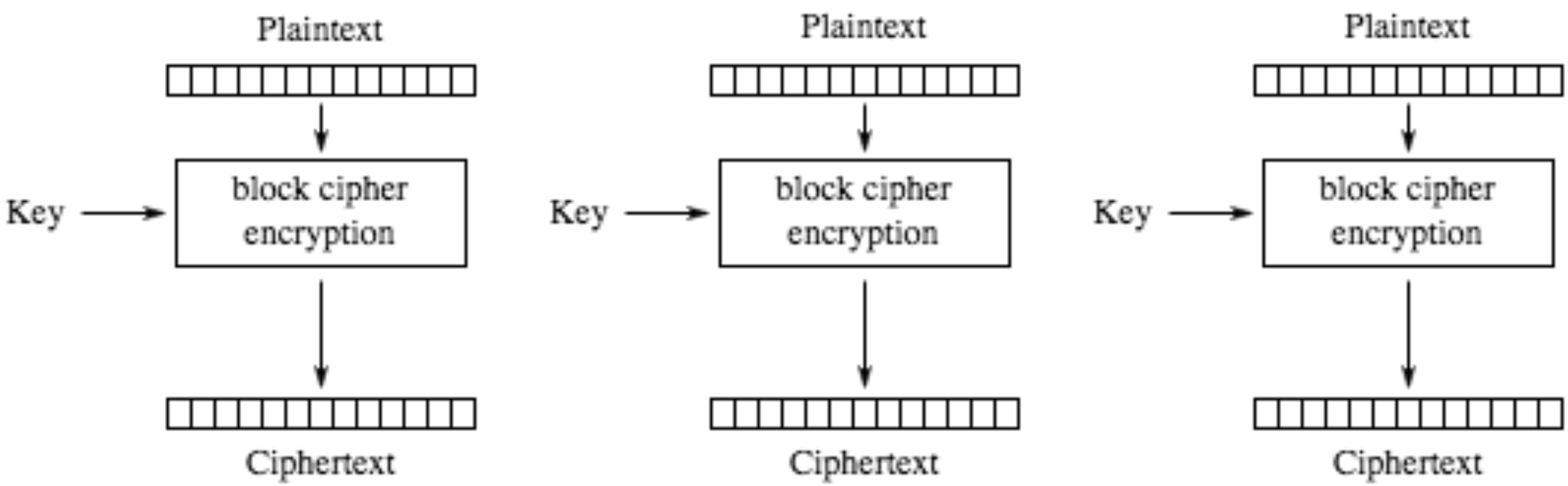
Original	Encrypted
"Sunset tomorrow is at seven oclock." "We attack at sunset tomorrow "	"Vxqvhw wrpruurz lv dw vhyhq rforfn." "Zh dwwdfn dw vxqvhw wrpruurz "

Encryption

AES (Advanced Encryption Standard) is a **block cipher**



Encryption



Electronic Codebook (ECB) mode encryption

Encryption

AES ECB

Original	Encrypted
"Sunset tomorrow is at seven oclock." "We attack at sunset tomorrow "	(not the actual ciphertext) eb e3 15 9f 80 19 6d b9 b3 13 a0 08 9b 59 17 0a 03 2f a0 14 a6 ac b2 d2 08 c9 f2 82 40 87 46 cb eb e3 15 9f 80 19 6d b9 b3 13 a0 08 9b 59 17 0a

Are we done?

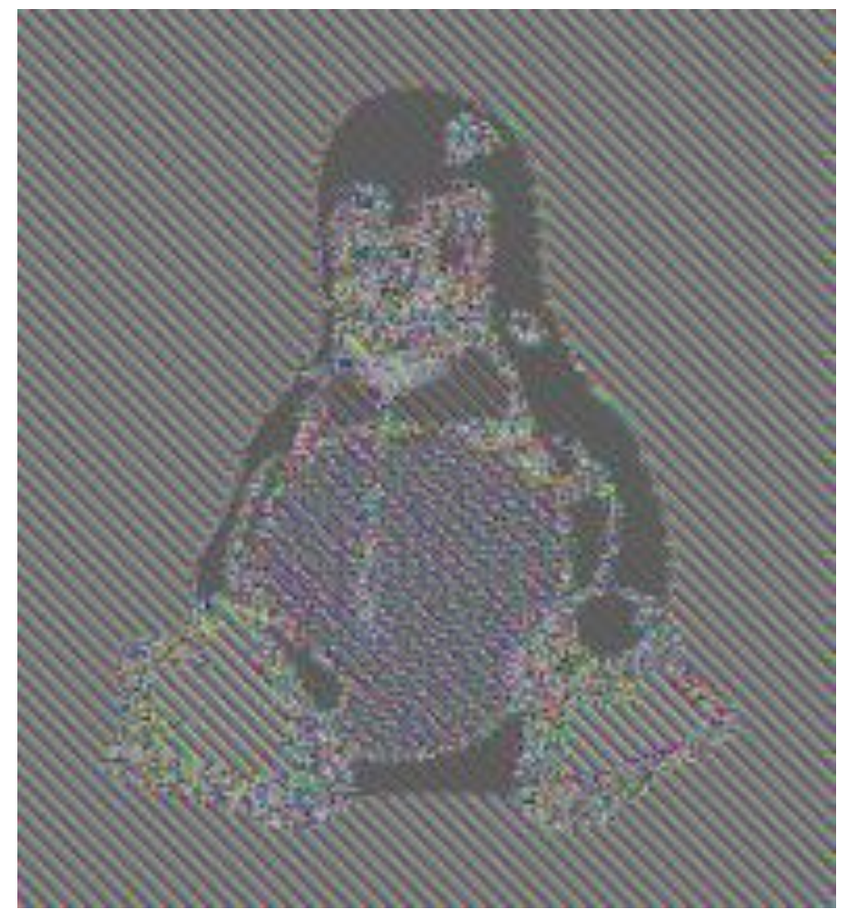
Encryption

AES ECB

Original	Encrypted
"**Sunset tomorrow** is at seven oclock." "We attack at **sunset tomorrow** "	**eb e3 15 9f 80 19 6d b9 b3 13 a0 08 9b 59 17 0a** 03 2f a0 14 a6 ac b2 d2 08 c9 f2 82 40 87 46 cb **eb e3 15 9f 80 19 6d b9 b3 13 a0 08 9b 59 17 0a**

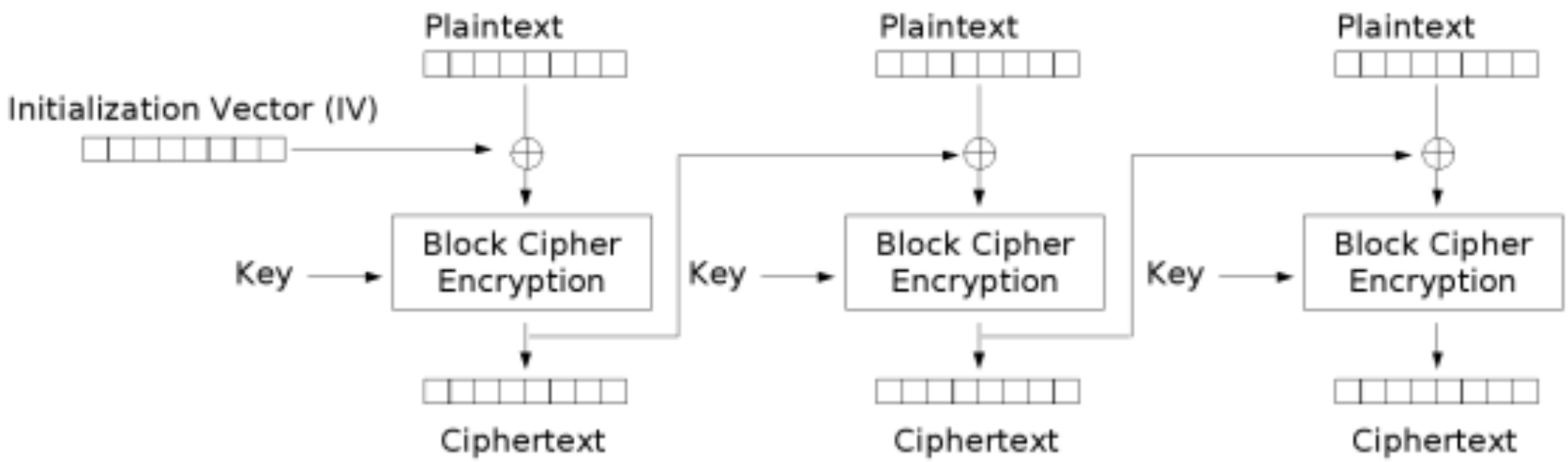
Encryption

Security is all about the details!



Encryption

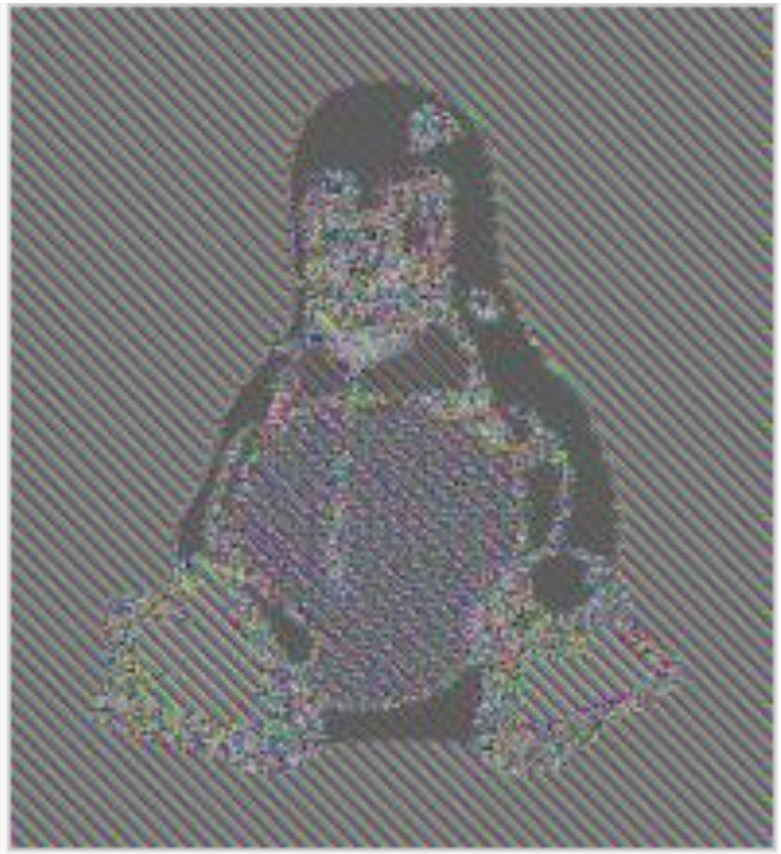
(One) Solution



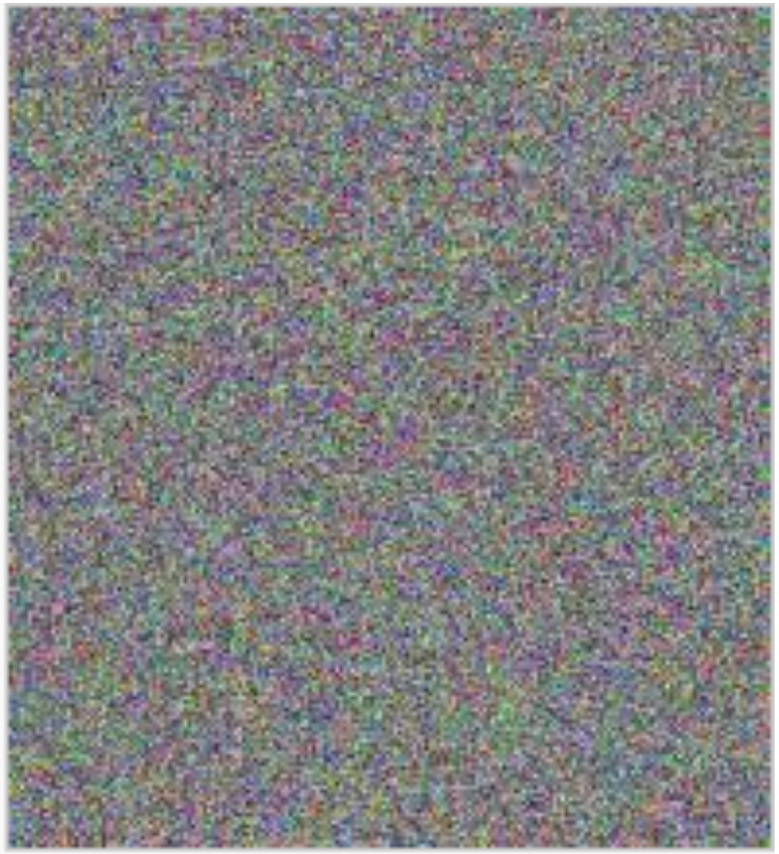
Cipher Block Chaining (CBC) mode encryption

Encryption

Original image



Encrypted using ECB mode



Modes other than ECB result in pseudo-randomness

Encryption

AES CBC

Original	Encrypted
"Sunset tomorrow is at seven oclock." "We attack at sunset tomorrow "	a3 a7 c1 48 a4 43 be 5b b5 f5 4f f4 44 42 53 d6 f3 56 17 b7 45 2c c5 05 63 92 42 6a 0e 6a 42 7d b4 7e e1 9d 70 63 cf 64 2d f7 61 b1 16 2e bc 20

Are we done?

Encryption

- We still leak the **length and timing of our message**
- **Identity of sender and recipient** are known
- An attacker could **replay** old messages
- What if we **leak the key**?
- Etc.

Security

Super Mario World: Arbitrary Code Injection At AGDQ 2014, Performed Live

Conclusion

Artificial Intelligence

- Humans create "features", computer learns "weights" through trial and error
- Neural Nets - learn both features **and** weights

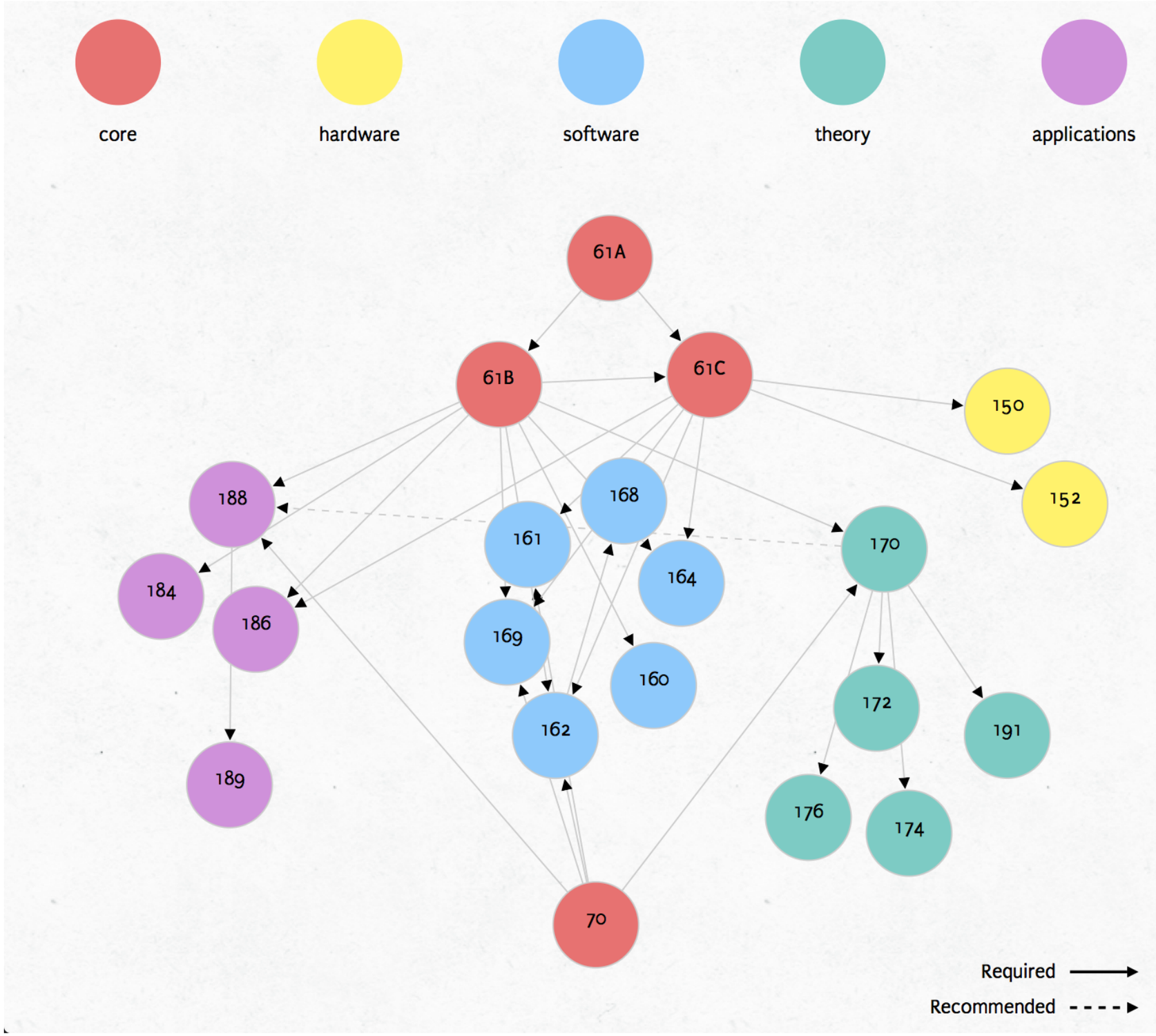
Security

- It's all in the details!
- Hard to be perfectly secure, determine what you need

Courses

CS 188	**Artificial Intelligence**
CS 161	**Computer Security**
CS 168	Introduction to the Internet
CS 170	Algorithms
CS 162	Operating Systems
CS 189	Machine Learning

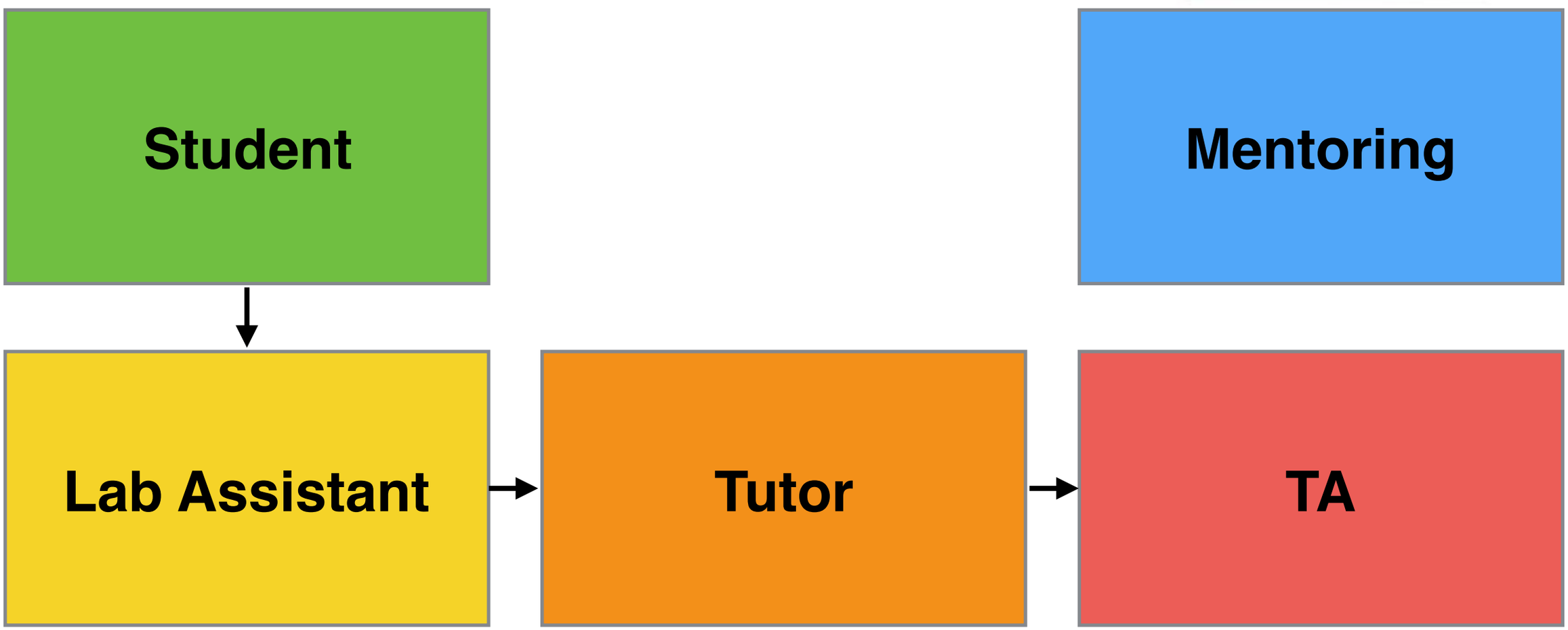
HKN's CS Course Map



https://
hkn.eecs.berkeley.edu/
courseguides

The End

Liked 61A? Stick around!



Final Thoughts

Thanks for a wonderful semester!

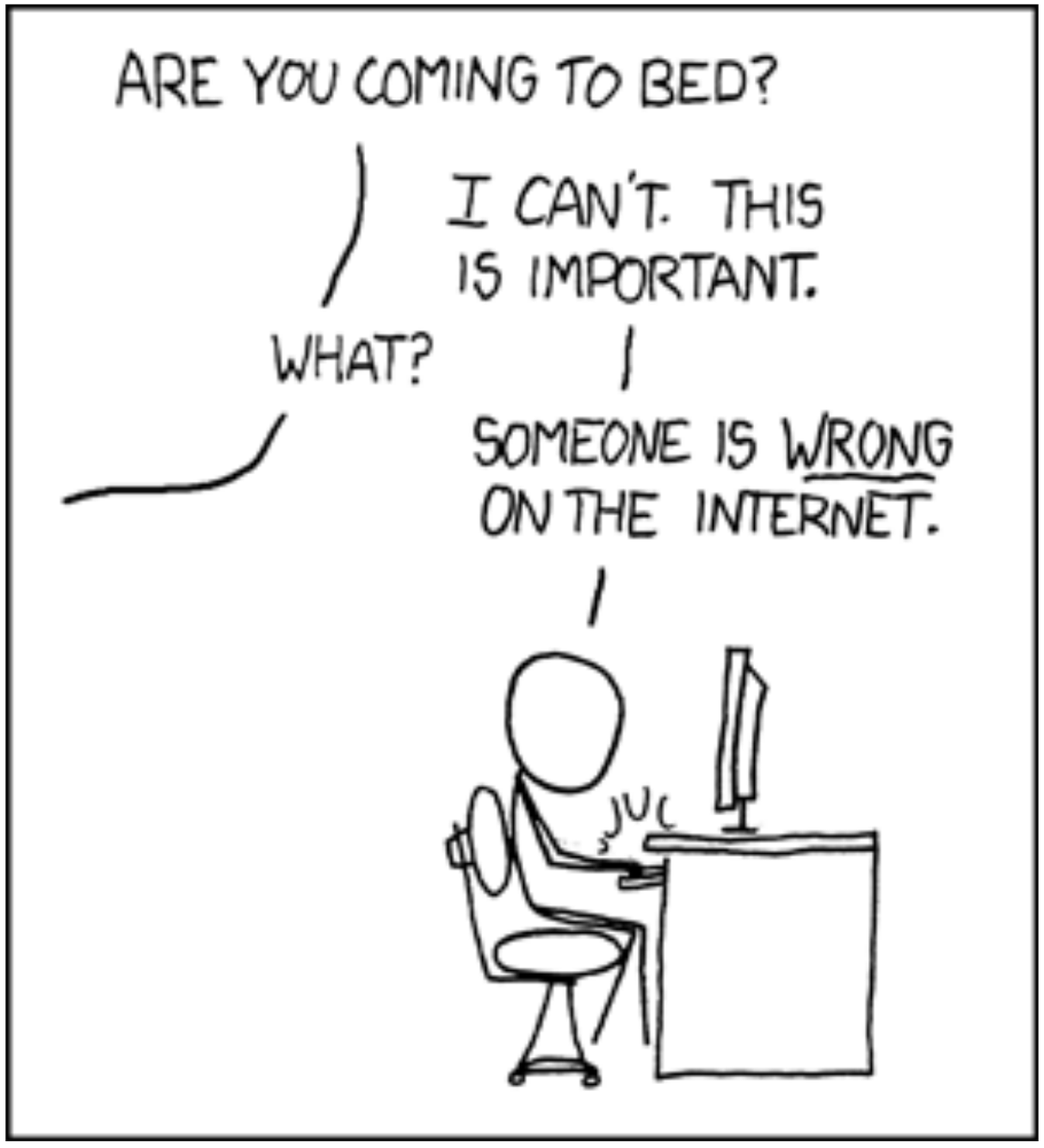
I sincerely hope you enjoyed your time in 61A.

As always, feel free to reach out to me with any questions.

Please please please fill out course evaluations!

Bonus

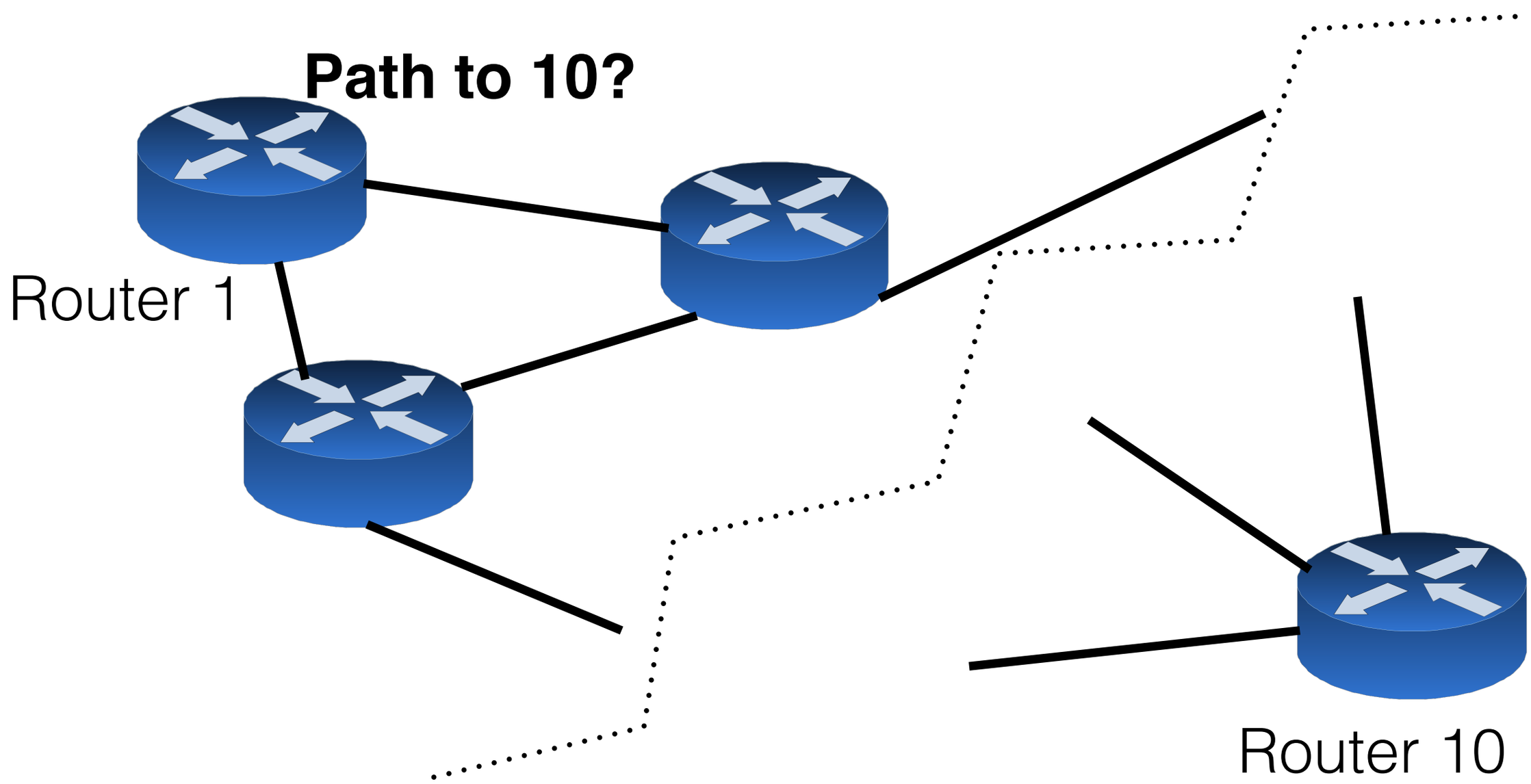
The Internet



http://xkcd.com/386/

The Internet

Imagine you are a router/link on Berkeley's network…



Computer Networks

You have just been passed your "routing information":

Find the path from router #1 to router #10!

1. You have 5 minutes

2. Don't leave your seat or show your slip of paper to anyone else

3. If you didn't get a slip of paper, sit back and enjoy the chaos (and maybe think of solutions)

Computer Networks

(One) Solution:

1. Destination stands, announces neighbors, **(distance 0)**

2. Neighbors stand one at a time, announces their neighbors and distance **(distance 1)**

   - **Remember who called you!** Respond to the closest "caller" and **do not stand up twice.**

3. etc…

4. Once source stands, work back up to destination!