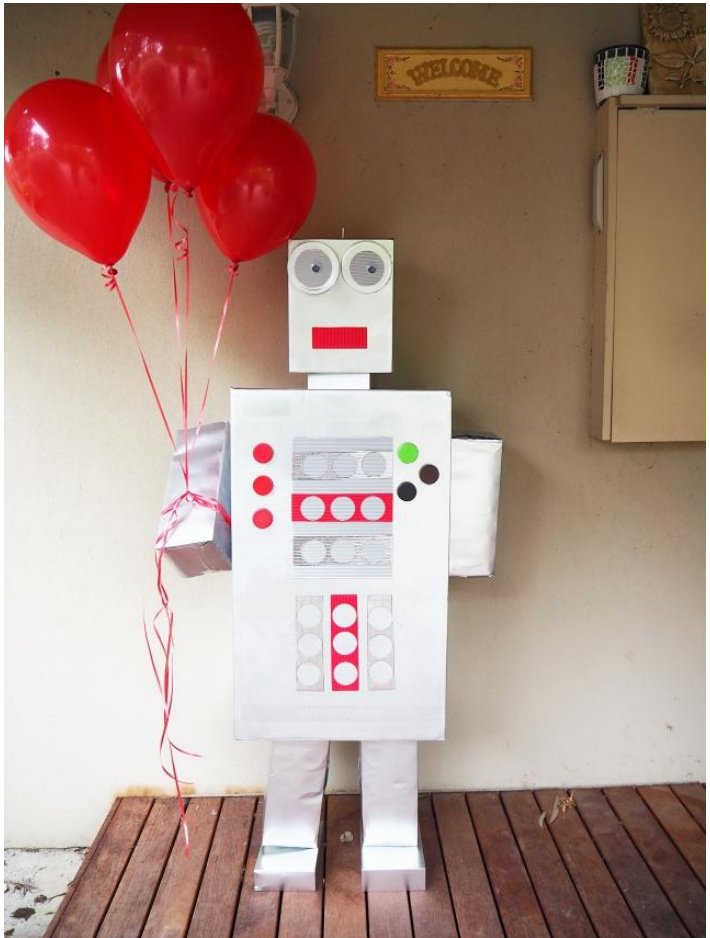
LAST DAY OF CLASS! 05.16.22

- Revisit security: encoding vs. encryption vs. hashing vs. obfuscation
- Workshop the “Work Plan” portion of your final proposal
- Reflection on your project idea so far
- Next semester!



encoding vs. encryption

- Both use algorithms to **map**, **transform** data from one form to another
- **Encoding** = uses a reversible method to change data from 1 format to another so that a system can receive it easily

- Base64 example: binary to text data
  - Many things can be input! Text, image, audio . . .
  - Example w/text: “proton” -> cHJvdG9u

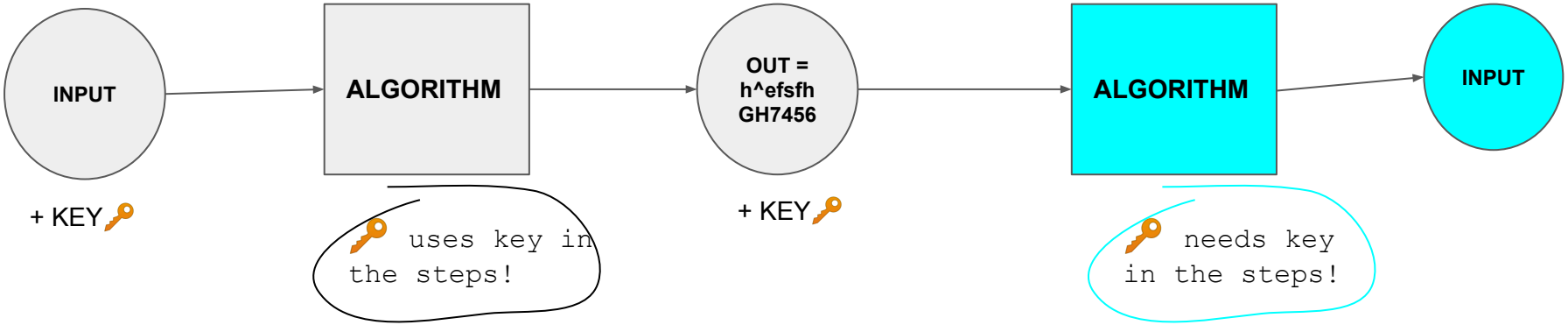
ENCODING: “proton” to base64, algorithm

- First: ASCII to binary, tables
  - p = 01110000
  - r = 01110010
  - 01110000 01110010
- Next: convert 8 bit binary to 6 bit:
  - 011100 001110 010… etc
- Next: convert 6 bit binary to decimal (“base 2”)
  - 0 1 1 1 0 0 = 28 (2^5 2^4 2^3 2^2 2^1 2^0)
  - 0 0 1 1 1 0 = 14
- Finally: convert decimals to base64, tables
  - cHJvdG9u
- Why? Your system needs text, but you want to send img; compact way to send text if it needs to be binary first; etc.

ENCODING: anyone can read!

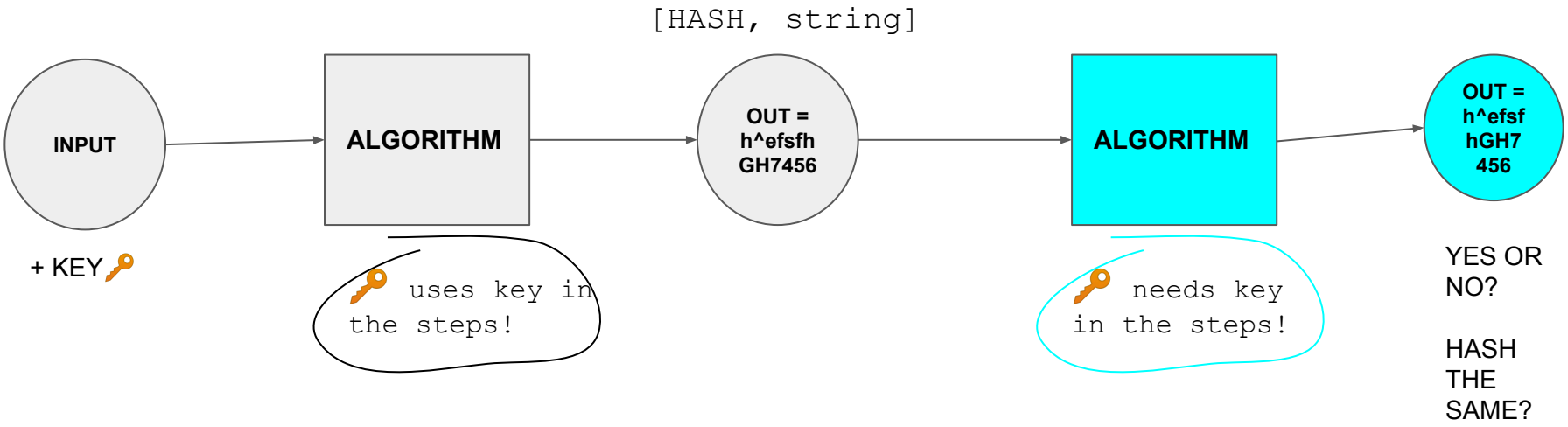
- Simple "decode" tools to base64, publicly available

ENCRYPTION: mapping data to a new format via an algorithm, to **scramble it**, so only someone with the **key** can unscramble or decrypt it



BRUTE FORCE:
27,337,893,038,406,611,194,430,009,974,922,940,323,611,067,429,756,962,487,493,203 years.

HASHING: using algorithm to transform arbitrary data into fixed data format, using a **key** - another system can check this "signature" to see if anything has been **tampered with**



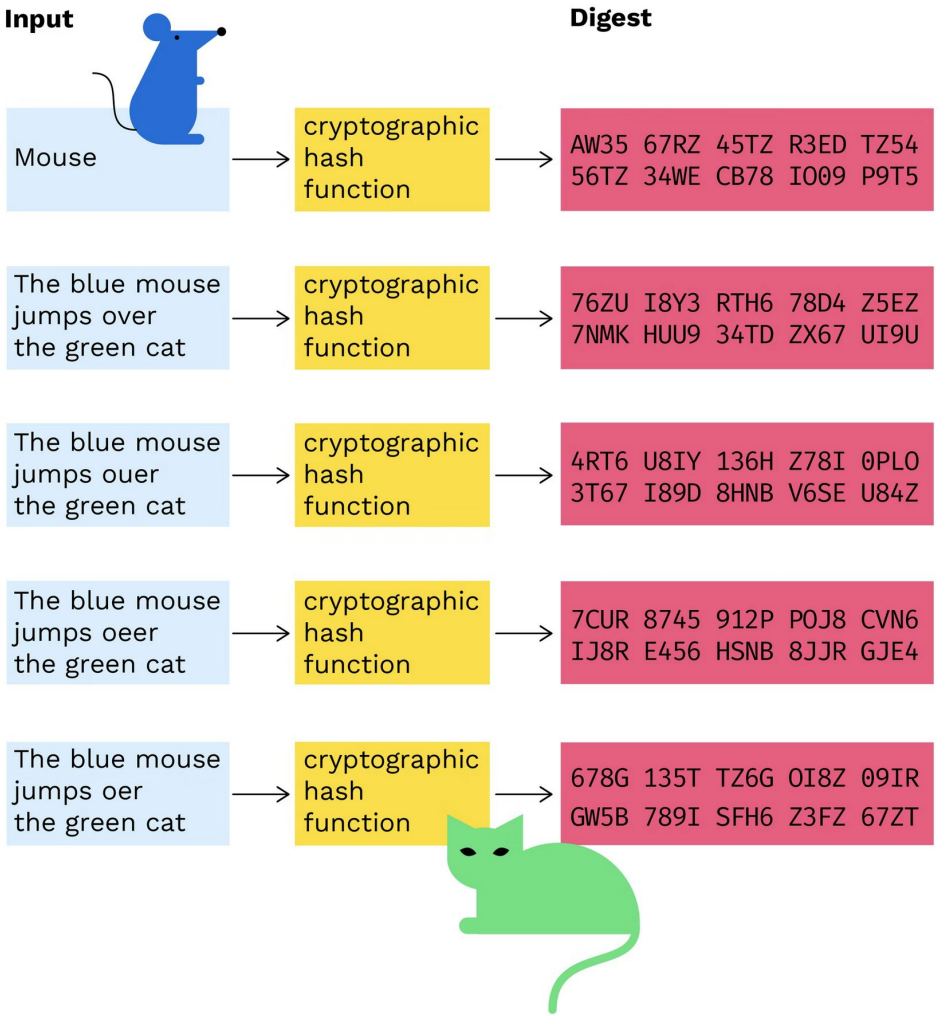
Encryption

(used to protect sensitive information)

Hashing

(used to validate information)

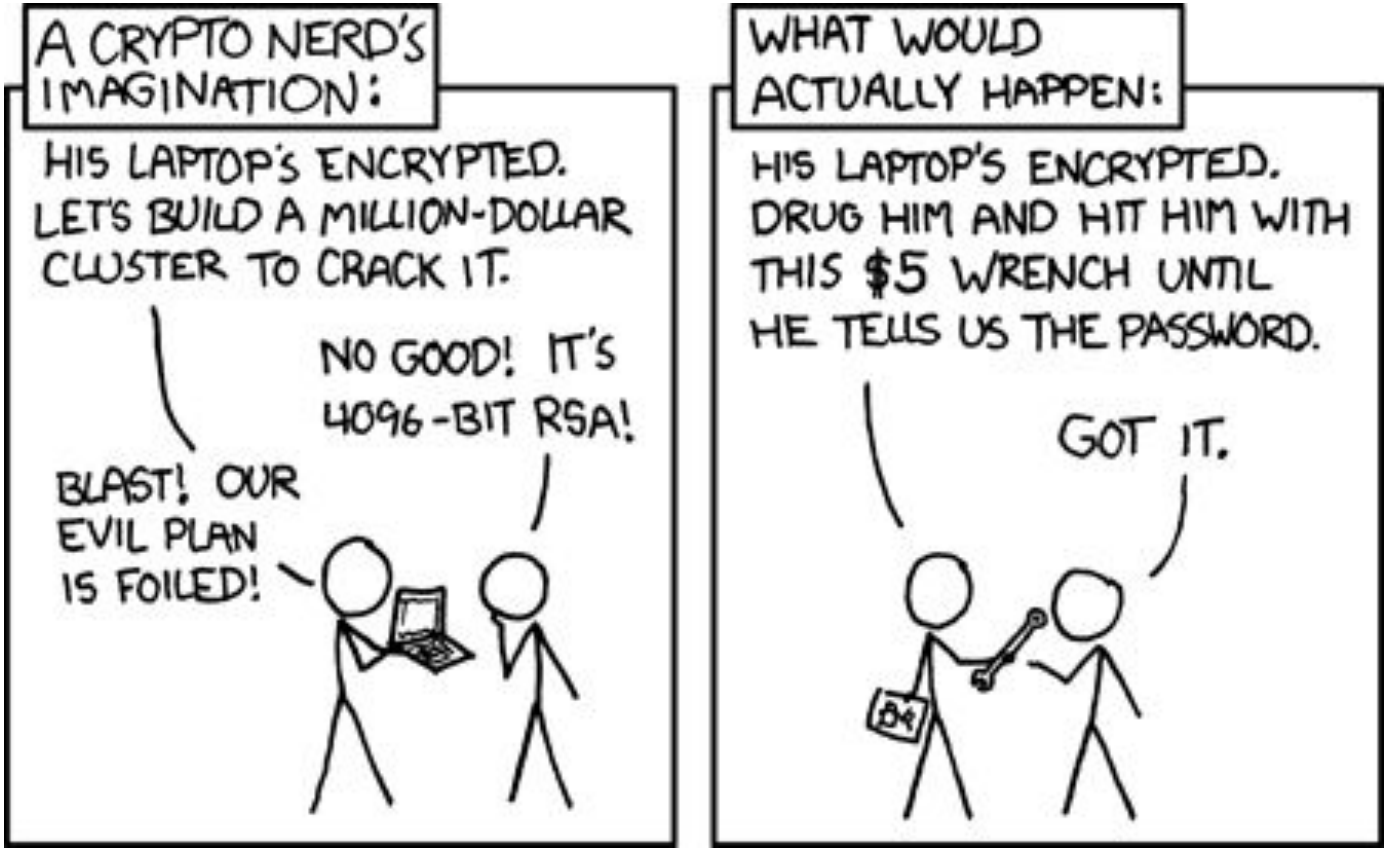
okta


Input
Digest
Mouse
cryptographic hash function
AW35 67RZ 45TZ R3ED TZ54 56TZ 34WE CB78 IO09 P9T5
The blue mouse jumps over the green cat
cryptographic hash function
76ZU I8Y3 RTH6 78D4 Z5EZ 7NMK HUU9 34TD ZX67 UI9U
The blue mouse jumps ouer the green cat
cryptographic hash function
4RT6 U8IY 136H Z78I 0PLO 3T67 I89D 8HNB V6SE U84Z
The blue mouse jumps oeer the green cat
cryptographic hash function
7CUR 8745 912P POJ8 CVN6 IJ8R E456 HSNB 8JJR GJE4
The blue mouse jumps oer the green cat
cryptographic hash function
678G 135T TZ6G OI8Z 09IR GW5B 789I SFH6 Z3FZ 67ZT

OBFUSCATION: purposefully making something hard to guess or hard for a human to understand, but otherwise not protecting it

Example:
https://mysite.com/mySecret/5sfsdgfjk35490/sdfhkh235909f/sdfjkj2234989fdsfjk_dfjskdjf23952893589ugisjfdlskflslk34 …


IF YOU RELY ON SECURITY THROUGH OBSCURITY
INSTRUCTOR
YOU'RE GOING TO HAVE A BAD TIME


A CRYPTO NERD'S IMAGINATION:
HIS LAPTOP'S ENCRYPTED. LET'S BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.
NO GOOD! IT'S 4096-BIT RSA!
BLAST! OUR EVIL PLAN IS FOILED!
WHAT WOULD ACTUALLY HAPPEN:
HIS LAPTOP'S ENCRYPTED. DRUG HIM AND HIT HIM WITH THIS $5 WRENCH UNTIL HE TELLS US THE PASSWORD.
GOT IT.

movies

🛠️🤖 WORKSHOP TODAY: “Work Plan”

- Pairs/small groups
- Explain step-by-step your work plan to your partner, paying close attention to what tools/languages you plan on needing and using
- Listener: encourage your partner to be as **specific** as possible! Names of databases, APIs, etc.
- Use Mural, write which tools you will be using, find a way to sign your names https://app.mural.co/invitation/mural/test17018/1652738777051?sender=u5002dd0578da7f9a25309972&key=d9411949-e6ad-4016-823d-42ed096742d6

Semester Reflection

- Revisit: https://criticalengineering.org/ & https://manifesto.responsiblesoftware.org/

- Think back to when you initially had this project idea (or another one) - what have you learned? What has changed? Where has your knowledge grown? Where has your vision of this idea in the world grown more complicated?

- What is your biggest question about your build and project for next semester, right now?

🛠️🤖 NEXT SEMESTER: BUILD!

- Meeting once a week to check in on each other's project
- Accountability group, lab collective, progress - we can define this format
- Give each other resources, learn together a process or concept that someone needs
- User testing!
- Demos, prototypes, and presentations with feedback