#ret #hw

1 | **Crypto :clap: graphy** **clap**

Try to use some of the cryptographic tools we're been talking about. **Keep notes on what you do and learn, and submit them here.** Here are some suggestions for things to try:

- n – Send an encrypted email to another person in the class, such that only they can read it. What tools exist to let you do this, and how well do they work?
- n – Send an email to another person in the class that has been cryptographically signed. What tools exist to let you do this, and how well do they work?
- n – If you have a website that does not currently support https, use https://letsencrypt.org/getting-started/ (Links to an external site.) to create a certificate for your site.
- n – Figure out what Certificate Authorities your browser trusts.
- m – Hash some string (or have a partner do it). Test out the properties of the hashing function, noting how much the output changes from small input changes. Write a program that will try some brute force solution to figure out the string by finding a matching hash. Observe how the length of time varies based on the string you use and the way you structure your search. Try this with different hash functions, to see the differences in speed.
- n – Look at the different accounts you have and see what level of security they provide.
  - already done – Try turning on two-factor authentication, if you have that option.
  - Look at their security questions and figure out roughly how many different options there are, assuming you answer honestly. For instance, it if it is asking for the model of your first car, get an estimate of how many different car models have ever been made.
  - already done – Think about how secure your password is, relative to how attackers would try guessing. Is it a dictionary or relatively common word? Is it all lower case letters, or do you also include uppercase letters, numbers, and/or symbols? Think about how large a search space is needed to find your password. Do some research on current recommendations on password length and generation.
- m – Try encrypting and decrypting files. What are the different tools out there that provide this service? What do encrypted files look like?
- already done – Generate a public/private key pair for yourself. Put the public key on our test laptop so that you can SSH into your account without typing a password. You could also use this key for your Github account, if you have one.