Cryptography 4/27

Reagan Shirk

April 27, 2020

RSA (Textbook)

- It looks like Cheng is having some connectivity issues and no one can hear him but I don't think he cares lol
- 11 minutes later he turns off his video, it seems that it has helped quite a bit

No message attack

- Producing a message/signature pair that can convince people
  - i.e. passes the $s^e \bmod n \overset{?}{=} m$
  - Attacker can start with a signature and produce a message, $s^e \bmod n \to m$

Cryptographical Hash Function

- $h : \{0,1\}^* \to \{0,1\}^n$
- This function has the properties:
  - One way
    - Easy to go one way, hard to go another
  - Collision resistant
    - $\exists x_1 \neq x_2$ such that $h(x_1) = h(x_2)$
  - Second-preimage resistant
    - Given x_1, it is hard to find $x_2 \neq x_1$ such that $h(x_1) = h(x_2)$
- The first property is easy to understand, but the second and third are hard because people don't understand the difference between the two
  - He explained the difference between the two but I didn't catch it so I'll have to look it up
- The hash function has to be efficient