Cryptography 3/27

Reagan Shirk

March 27, 2020

Lattice-Base Cryptography

- You need/have a public key? I'm not sure, he just wrote public key down and boxed it in
- In this scenario, you have Alice and Bob trying to communicate with Eve and Mitt trying to intercept
  - Alice has an encryption key to encrypt her plaintext, the cypertext gets sent to Bob, and Bob decrypts the message with a decription key
  - One of the keys is public, in this case lets say that the encryption key is public and belongs to Bob
  - Anyone can send him an encryption message with the key
  - The decryption key is Bob's *secret key*
  - You want the decryption key to be *hard to compute* from the encryption key
- This is also known as Asymmetric Key Cryptography, because the encryption and decryption keys are different
  - Now imagine that Alice is sending an encryption session key to Bob, where the session key is the AES key
- He's lost me, sorry guys
- Cheng: "Does that make sense? Type yes if it does"
  - Me: "Oh, I'm a little confused. Maybe I'll type no"
  - Everyone in the class: "yes"
  - Me: "Oh, uh... nevermind"

Merkle-Hellman

- Subset-Sum Problem
  - Given n integers $\{M_1, M_2, \cdots, M_n\}$ and an integer S, decide whether there exists a subset $\alpha \subseteq \{M_1, \cdots, M_n\}$ such that $\Sigma_{i \in \alpha} i = S$
  - Example:
    - $\{73, 54, 7, 12, 17, 38, 115\}$, in this set we can see that $n = 7$. Is there a subset of these numbers such that $S = 100$? Nah, we got 101 though. What algorithm did we run in our brains? Brute force. Lets us know that this is actually a pretty hard question
      - Apparently there is a way to get 100 out of the sum of a subset of these numbers, but Cheng is the only one who knows which subset it is.
    - The solutions aren't unique, you can have different subsets for the same S
  - Here we have another one way function
    - 7 bit string → sum
    - Input to output, easy. Output to input, hard.
    - I just dropped the call because my internet connection is unstable, so between that and all of the video freezing I'm on the struggle bus lemme tell ya
- Trapdoor One-Way Function
  - Once it's encrypted, Bob can decrypt it because Bob has the trapdoor. But Eve and Mitt can't decrypt it