Cryptography 4/17

Reagan Shirk

April 17, 2020

Public Key Encryption/Decryption

- Alice is trying to send a message to Bob. Alice encrypts the message with Bob's public key and Bob decrypts the message using his private key
- He mentioned needing to look at more than the books version of some algorithm but I didn't catch which algorithm, might've been pertaining to the project
- As long as Alice can trust that the public key is *really* associated with Bob, she has no concerns about her privacy because she knows that only Bob can decrypt the message
  - Problem becomes: how can she really believe that the public key is truly associated with Bob?
  - Authentication is much more important than privacy
    - If we get a message from Bob, how do we know that that message is *really* from Bob?
- I got distracted from looking at laptop multi-monitor attachments. Le Slide is tempting, and if there were more of the semester left I'd probs buy it

NTRU

- $E : \{0,1\}^n \to \{0, q-1\}^n$
- The polynomials have small coefficients and the encrypted text looks like a random polynomial
  - This is not an **onto** map
  - This means that encrypting a message is easy, but decrypting a message is hard
- You try to get a one way permutation with a trapdoor, but it's not easy to get with a lattice based system
  - This allows you to do a public key system as well as a signature
  - This is where RSA comes in

RSA

- This is a one way permutation with a trapdoor
- RSA was invented publicly by Rivest, Sharmir, and Adleman in 1977
- Clifford Cocks (lmao) 1973, GCHQ (UKs version of NSA)