Cryptography 3/25

Reagan Shirk

March 25, 2020

Diffie-Hellman

- I don't really know what all of these exponentials are supposed to assist us with, nor do I know how we got them aside from the fact that it involves Fermat's Little Theorem. Ya girl is lost. Send help.

$$p = 13$$
$$g = 2$$
$$2^1 = 2$$
$$2^2 = 4$$
$$2^3 = 8$$
$$2^4 = 3$$
$$2^5 = 6$$
$$2^6 = 12$$
$$2^7 = 11$$
$$2^8 = 9$$
$$2^9 = 5$$
$$2^{10} = 10$$
$$2^{11} = 7$$
$$2^{21} = 1$$

- Backtracking to what we did on Monday...?
  - Eve (the hacker) knows: p, g, X, Y
  - She wants to find out K (which is equal to $g^{xy} \bmod p$)
  - This is hard because $X = g^x \bmod p$ and $Y = g^y \bmod p$ are both discrete logarithms, which means they're one way
  - This is a Diffie-Hellman problem
  - Discrete Logarithm $\geq$ Diffie-Hellman
    - I think this is supposed to mean that discrete logarithm is harder than diffie-hellman
- Possibly Important for the Final
  - Something about g not being a multiplicative generator for the whole group? I don't really know what that means
  - If g generates a very small group, someone interrupted him before he could complete this sentence, but I think the rest was that it would make the discrete logarithm easy to solve? Dude I'm so lost rn. Cheng is a good guy but I never have any idea of what he's talking about

Man in the Middle Attack

- I missed some of the information, but it appears that Eve is trying to steal communication from Alice and Bob, like usual. And now there's a new guy, Mitt, who appears to also be in communication with Alice and Bob, maybe he's the man in the middle?

- Example:
  - You're chillin like a villan in Starbucks (why am I like this) and you see WiFi called "Free Public Wifi", and you assume that it's the Starbs WiFi so you connect. Plot twist: some rando in the corner has labeled his personal hotspot as "Free Public WiFi" and turned off the password, so you're now connected to this randos WiFi and he has access to all your shit now. This is a man in the middle attack, because the man in the middle is the rando giving you internet access.
- Lesson to learn: don't connect to random ass WiFi
- Apparantly there's a woman in the middle attack that is much more powerful *insert eyeroll here*
- Is this shit passive or active? Active
- How do you counter this attack? You include a signature with your message
  - You need to somehow produce a digital signature that can convince Bob that the message is from Alice