Cryptography 3/23

Reagan Shirk

March 23, 2020

AES

- Four steps:
  - Add key
  - S-box transformation
  - ???
  - Mix Column
- A type of symmetric key cipher
  - This means that you have your plaintext that gets encrypted, then you send the ciphertext over the channel
  - You have the encryption key when the plaintext is encrypted and a decryption key when the ciphertext gets decrypted
  - Called symmetric key cipher because you can derive one from the other very easily
  - To use a symmetric key cipher, we need shared secrets
    - Secret = key
  - Doesn't work without sharing the key
  - You need key exchanging
    - Assumption is that the communication channel is insecure
    - Diffie-Hellman came up with an idea to allow us to exchange keys without a secure channel

Diffie-Hellman

- $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$
  - p is **large**, $> 2^{1000}$
  - g is a generator in $\mathbb{F}_p^*$
    - g has a large order
    - if g is a generator, it'll have an order of $p - 1$, but sometimes it isn't very necessary, you can have g with order $\frac{p-1}{2}$. If p is large, then $\frac{p-1}{2}$ will also be large
- We are assuming a passive attack. The steps for encryption are:
  - Find a random x such that $0 < x < \mathrm{ord}(g)$
  - Compute $X = g^x \bmod p$
- The steps for decryption are:
  - Find any random y such that $0 < y < \mathrm{ord}(g)$
  - Compute $Y = g^y \bmod p$
- Discrete logarithm:
  - If $X = g^x \bmod p$, from X compute x
  - $x \to X$ is a one way function. Why?
    - Going from $x \to X$ is a really easy problem, but going from $X \to x$ is very hard
  - One way functions are very important in cryptography
    - One direction takes a second, other directon takes millions of years
  - Back to the steps above, for encryption it is needed to camculate $K = Y^x \bmod p$
    - How do we know p? p is public information- everyone knows p
    - How do we know Y? it gets sent to us from the person doing decryption (Alice and Bob for those who pay a decent amount of attention, Alice is doing the encryption and Bob is doing the decryption)

- Decryption needs to compute $K' = X^y \bmod p$
- Theorem: $K = K'$
  - We want to prove that they are equal, and that this can be true while still having a secure process

Proof

$$\begin{aligned} Y^x \bmod p &= (g^y)^x \bmod p \\ &= g^{xy} \bmod p \\ X^y \bmod p &= (g^x)^y \bmod p \\ &= g^{xy} \bmod p \end{aligned}$$