Computer Security

Reagan Shirk

September 24, 2020

Modes of Operation

- We don't need to memorize all of these, just have to understand how they work? I didn't entirely follow what he was saying
- We don't need to memorize, we need to understand how to analyze
  - If the question is about CBC, we will be given the graphic for how CBC works
- Fam I haven't been paying attention I'm sorry

Triple DES

- Triple DES = DES three times
- One of the major limitations of DES is that the key length is too short, so what happens if we apply DES *multiple times* to increase the strength of encryption?
  - Using the same key - doesn't help much because the keyspace is the same. Still able to be broken by brute force attack
  - Using the different key - the total keyspace increases to 112 bits instead of 56 when encryption is run twice, does this increase the key strength? Yeah but still suseptible to meet-in-the-middle attack

Meet in the mmiddle attack

- Choose a plaintext P and generate a ciphertext C, using double DES with $K_1 + K_2$
  - Encrypt P using single-DES for all possible 2^{56} values K_1 to generate all possible ciphertexts for P, store these in a table indexed by ciphertext values
  - Decrypt ... missed it
- I'm going to review slides and come back to this, I kinda know how it works but I haven't been on my focus game today