Computer Security

Reagan Shirk

September 22, 2020

Takeaways from Quiz

- Two of the questions were wrong
- The problem with ECB is that it lacks diffusion
- Question 2:

*Untitled - Notepad

File Edit Format View Help

```
M = 1100 1001
K = 0101
K' = 1010
A = 1100
B = 1001
C = 1001
f(B, K) = B XOR K' = 1001
                 XOR 1010
                   = 0011
D = A XOR f(B, K) = 1100
                XOR 0011
                  = 1111
M' = 1001 1111
```

Modes of Operation

ECB/CBC

- Does encryption or decryption take longer?
  - Encryption. You can do decryption in parallel, you can't do encryption in parallel
- There was a whole bunch of conversation that I couldn't follow

Output Feedback Mode (OFB)

- The difference is that we use IV to generate encryption and then XOR with the plaintext...?
  - There's an IV that creates a one time pad of encryption keys that is independent from the rest of encryption/decryption
- If $M_2 = M_3$, will $C_2 = C_3$? No
- If we flipped one bit in C_3, what's the impact on M_3? The corresponding bit in M_3 will be flipped
- Can you encrypt/decrypt in parallel? Yes to both
- Error propegation? No
- The IV must be different each time

Cipher Feedback Mode (CFB)

- Ciphertext of previous block goes into the encryption key of the next block
- If $M_1 = M_2$, will $C_1 = C_2$? No
- If we flipped one bit in C_3, what's the consequence? The corresponding bit in M_3 will be flipped.
- Can we encrypt/decrypt in parallel? No to encrypt, yes to decrypt
- Error propegation? Yes, if there was a plaintext error that error would propegate through that ciphertext and all of the following. If there was a ciphertext error, the error would propegate for the current block and the one after it

Counter Mode (CTR)

- We increment IV for each encryption key
- It's very concise
- Information leakage: No..? Didn't catch that
- Can we predict plaintext result of a bit of the ciphertext is flipped? Yes.
- Can we encrypt/decrypt in parallel? Yes to both
- Error propegation? Nah