CS 198 Codebreaking at Cal
Spring 2023 Makeup Assignment

Week 1

Question 1

Assuming IVs are not reused, explain why AES-CBC mode is IND-CPA secure.

Question 2

True or false: The Pseudo-OTP cipher is secure even if we use a low-entropy seed for the PRNG. (If true, explain why. If false, what would an attack look like?)

Question 3

Up until now, we've been focusing on *confidentiality*, a property of ciphers meaning that no one other than the intended recipient can decrypt something we send. However, we haven't yet discussed *integrity*, a property that guarantees any tampering with our message is detected. The ciphers we've discussed so far may provide condifentiality, but they don't necessarily provide integrity!

1. Suppose Alice uses the pseudo-OTP stream cipher to encrypt a message M to Bob, generating a ciphertext C. Mallory intercepts the transmission, and she wishes to tamper with the ciphertext so that the ciphertext Bob receives, C', decrypts to some message M' that Mallory chooses. Explain how Mallory can generate C' if this attack is possible, or explain why it's not possible.

2. Now suppose we have the same situation as above, but Alice uses AES-ECB to encrypt her message instead. Explain why Mallory can no longer create C' so that Bob decrypts it to a message of her choosing.

3. Even though Mallory can't make M' whatever she wants when Alice uses AES-ECB, she can still affect what Bob decrypts. Suppose Alice's message is "Mallory owes Alice $100" and that each word is a separate block and is padded to the block size AES uses. Give an example of a message Mallory could cause Bob to receive once he decrypts the ciphertext, and explain how she would modify the ciphertext to do this.

Question 4

Alice decides to design a new cipher similar to AES-CBC with one change. The encryption formula is the following (note that E_K represents one AES block encryption with key K):

$$
\begin{aligned}
C_0 &= IV \\
C_i &= E_K(M_i \mathbin{\&} C_{i-1})
\end{aligned}
$$

where M_i is the ith block of the message, C_i is the ith block of the ciphertext, IV is randomly chosen, and & is the bitwise AND operator.

1. Provide the decryption formula for this cipher, or explain why this is not possible.
2. Is this cipher still IND-CPA secure?

Contributors:

- Ryan Cottone, Will Giorza