CS 198 Codebreaking at Cal
Spring 2023 Homework

HW 3

Question 1

Briefly explain why using AES-ECB as an AES mode of operation is a bad idea. What should you use instead?

Question 2

Consider a stream cipher whose internal keystream is **perfectly random aside from the 2nd bit, which equals** 1 **with probability** 0.7 **and** 0 **with probability** 0.3. The encryption mechanism is the same as a pseudo-OTP:

$$\text{Enc}(M) = \text{PRNG}(\text{len(M)}) \oplus M$$

where PRNG(b) outputs b random bits. In this case, the second bit of PRNG(b) is biased as stated previously.

1. Find the *SSAdv* of an adversary (the advantage in the semantic security game). Recall that
$$\text{SSAdv} = P[m'_b = m_b] - 0.5$$
for the adversary's guess of m'_b.
2. Explain precisely how an adversary is able to achieve the advantage you responsed with in part 1).

Fun fact, this exploit is similar to that found in the RC4 stream cipher!

Question 3

Alice has encrypted two messages to Bob: AES-CTR(K, M_1, IV) and AES-CTR(K, M_2, IV). Eve is able to learn the value of M_1, but still needs to discover M_2.

Unfortunately for Alice, she has made a critical mistake: the IV in both ciphertexts is the same! Show how Eve can recover M_2. You can assume both messages are only one block long, but this doesn't change anything about the attack (just makes for easier math).

Question 4

Another popular mode of AES encryption is Cipher Feedback, or CFB. Encrypting a message with AES-CFB has the following definition (where M_i is the ith block of the message and C_i is the ith block of ciphertext):

$$C_0 = IV$$
$$C_i = E_K(C_{i-1}) \oplus M_i$$

1. Write the decryption function to recover M_i.
2. Is encryption with AES-CFB parallelizable? (In other words, can we encrypt a block of the message without knowing the encryption of other blocks?)
3. Is decryption with AES-CFB parallelizable? (In other words, can we decrypt a block of the ciphertext without knowing the decryption of other blocks?)

Question 5

Alice decides to switch to AES-CFB mode after her earlier problems. She sends Bob two messages, AES-CFB(K, M_1, IV) and AES-CFB(K, M_2, IV) (M_1 and M_2 are not the same messages as earlier). However, she doesn't learn from her mistakes and once again reuses the IV!

1. Suppose Eve does not know M_1 or M_2. Can she recover either message?
2. Now suppose Eve learns M_1. Can she recover M_2? If not, can she learn anything about it?
3. With IV reuse, is AES-CFB IND-CPA secure? Explain your answer.

Contributors:

- Ryan Cottone
- Will Giorza