CSCI 4331/6331

Quiz 4

Name(s):

1 Padding Oracle Attack

All modes of operations we covered in class assume that $|m|$ is a multiple of the block length (so m can be divided into blocks), but this does not have to be the case. When this is not the case, padding is used to make messages a multiple of the block-length L. But, it is also necessary to be able to distinguish padding from the message.

To do so, let b denote the number of bytes necessary to pad m to the nearest multiple of L. A standard method for this padding is to append to m the string consisting of the byte containing b appearing b times. That is, if we want to pad by 4 bytes, we will append the string $0x04040404$ on to the message.

We will consider what happens when this padding method is used together with CBC-mode encryption. We will consider the case of a 2-block message m. Remember that in CBC-mode given a message $m = (m_1, m_2)$, the ciphertext is computed as

$$c = (IV, c_1 = F_k(IV \oplus m_1), c_2 = F_k(c_1 \oplus m_2)).$$

We slightly modify the decryption procedure to check that the padding is done correctly. Specifically, we will decrypt m as normal, and then check that the last b bytes of the message are equal to $0xb$. If not, decryption returns an error.

In this quiz, you are asked to show that this padding essentially allows a CCA attack on CBC-mode encryption, and makes it insecure. Please answer the following questions to uncover the attack:

1. Describe how by changing c, you can cause it to decrypt to a different message. (Hint: Consider what happens if you change c_1.)

2. Describe how you can use this to learn the number b of padding bytes at the end of the message. (Hint: Remember that the decryption procedure outputs an error if the message has incorrect padding. Think how you can find the location of the first byte of padding by observing whether decryption succeeds.)

3. Now, assume that you know the value of b, the number of padding bytes, describe how you can learn the last byte of the message (Hint: Consider how to make the last byte of m look like a padding byte).

4. How can you learn the rest of the bytes of m_2?

5. (Challenge) What about the bytes of m_1?