CPSC 525/625: Principles of Computer Security (F23)
Instructor: Ryan Henry <ryan.henry@ucalgary.ca>

UNIVERSITY OF CALGARY

Name: Alex Stevenson UCID: 30073617

Worksheet 0x11

1. Suppose you are given a well-formed AES256-CBC ciphertext $c = IV\|c_1\|c_2\|\cdots\|c_{n-1}\|c_n$ in which the *second last* block c_{n-1} ends with

   `0x0fd5e0050f4fcd82`

   while the *last* block c_n ends with

   `0x05e0c8550a21363c`.

   Upon XORing the last byte of c_{n-1} by `0x06`, an "explicit-feedback" padding oracle indicates that the resulting ciphertext has valid padding (but an invalid MAC).

   (a) How long is the padding in the original (unmodified) ciphertext c. Show your work.

   Dk(0x3c) XOR 0x82 = ?
   Dk(0x3c) XOR 0x82 XOR 0x06 = 0x01
   Dk(0x3c) XOR 0x82 = 0x01 XOR 0x06
   Dk(0x3c) XOR 0x82 = 0x07

   The padding in the unmodified ciphertext is 7 bytes.

   (b) Suppose the padding length was P ($1 \le P \le 16$). How can you modify the given bytes of c_{n-1} and c_n to produce a ciphertext whose last P bytes are each $P+1$? (That is, how do you perturb the ciphertext so that the padding length is *almost* $P+1$.)

   Specifically, describe precisely how to should perturb the given values to affect this change

   The last 7 bytes of `Dk(c_n) XOR c_n-1` is equal to 0x07. For each of them, you can XOR by 0x07 to get 0x00, then XOR by 0x08 in order to set them all to 0x08 (this is equivalent to XORing by 0x0f)

   and state the result of having performed the above-described perturbations

   Altering c_{n-1} to be 0x0fdaef0a0040c28d (XORing each of the last 7 bytes with 0x0f) will result in the plaintext of `Dk(c_n) XOR 0x0fdaef0a0040c28d = 0x??08080808080808`
   This is almost valid padding, and allows us to find the unknown byte of plaintext

   (c) Suppose after performing the perturbations above, the find that XORing $(P+1)$th-last byte of c_{n-1} by `0x26` produces a ciphertext that the "explicit-feedback" padding oracle indicates has valid padding (but an invalid MAC). What is the last byte of the original plaintext?

   Dk(0x05) XOR 0x0f XOR 0x26 = 0x08
   Dk(0x05) XOR 0x0f = 0x08 XOR 0x26
   Dk(0x05) XOR 0x0f = 0x2e

   The last byte of the original plaintext is 0x2e

Name: Alex Stevenson UCID: 30073617

2. Suppose you are given a well-formed AES256-CBC ciphertext $c = IV\|c_1\|c_2\|\cdots\|c_{n-1}\|c_n$ in which the *second last* block c_{n-1} ends with

`0x3b46dfcc047bdc16`

while the *last* block c_n ends with

`0xa6e7b4860f0227f1`.

Upon XORing the last byte of c_{n-1} by each of `0x00`, `0x01`, `0x02`, ..., `0x0f` and querying a "timing-channel" padding oracle 5 times for each of the resulting ciphertexts, you receive the following response times (in nanoseconds)

byte	1	2	3	4	5
0x00	5.80e+1	2.40e+1	1.30e+1	2.40e+1	4.00e+1
0x01	7.40e+1	5.60e+1	5.50e+1	5.60e+1	8.70e+0
0x02	3.10e+1	6.20e+1	2.60e+1	3.40e+1	3.20e+1
0x03	5.60e+1	7.90e+1	6.60e+1	5.60e+1	3.40e+1
0x04	4.40e+1	8.40e+1	3.70e+1	1.10e+2	5.90e+1
0x05	3.50e+1	6.00e+1	1.70e+1	1.70e+1	3.40e+1
0x06	3.60e+1	4.10e+1	7.40e+0	6.30e+1	2.70e+1
0x07	7.90e+1	1.80e+1	7.20e+1	4.50e+1	3.50e+1
0x08	8.70e+1	5.20e+1	7.10e+1	4.40e+1	3.80e+1
0x09	3.20e+1	2.00e+1	7.90e+1	1.00e+2	1.50e+1
0x0a	2.10e+1	1.60e+1	3.70e+1	2.30e+1	5.40e+1
0x0b	8.20e+1	1.00e+2	1.30e+2	8.50e+1	6.10e+1
0x0c	2.80e+0	1.20e+2	1.90e+1	4.80e+1	4.10e+1
0x0d	5.70e+1	4.60e+1	5.60e+0	6.30e+1	3.70e+1
0x0e	1.50e+1	6.80e+1	1.10e+2	3.50e+1	7.00e+1
0x0f	4.20e+1	8.70e+1	3.70e+1	9.00e+1	4.00e+1

What is the most likely padding length in the original (unmodified) ciphertext? Justify your answer as rigorously as you know how. (Some actual statistical analysis could be useful here, but less formal reasoning is fine if statistics is not your forte.

The byte with the longest average timing is 0x0b (9.16e+1), which has consistently very long times compared to other tested bytes. All of the other bytes have average timings that range from 3.02e+1 to 5.96e+1 with a slight outlier with byte 0x04, which has an average timing of 6.68e+1.

Thus
Dk(0xf1) XOR 0x16 XOR 0x0b = 0x01
Dk(0xf1) XOR 0x16 = 0x01 XOR 0x0b
Dk(0xf1) XOR 0x16 = 0x0a

The most likely padding length in the original ciphertext is 10 bytes long