CSE 5351 Homework 4

Due: Thursday, February 22 by class time

1. Consider a variant of CBC-mode encryption where the sender simply increments the IV by 1 each time a message is encrypted (rather than choosing IV at random each time). Show that the resulting scheme is *not* CPA-secure.

2. Show that the CBC mode of encryption does not yield CCA-secure encryption (regardless of the pseudorandom permutation used).

3. What is the effect of a single-bit (transmission) error in the ciphertext when using the CTR, OFB, CFB, CBC modes of operation? More precisely, answer the following question:

   The ciphertext is $c = (c_0, c_1, c_2, \ldots, c_t)$, where $c_0 = IV$. Suppose c_q contains a transmission error for some $0 \le q \le t$. Which plaintext blocks m_i will be recovered *incorrectly*?

4. Continuing with the padding-oracle attack discussed in class, show how will you as the adversary recover the next byte, *y*?

5. Modify the padding-oracle attack (that we have discussed) to attack the CTR-mode encryption. To answer this question, use the example on the slides and show how to find out the padding length *b* and how to recover the byte *w*. In particular, what changes will you make to slides 101 and 102?