

CSE 5351 Homework 4

Due: Tuesday, February 11 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. 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 $c = (c_0, c_1, c_2, \dots, c_t)$, where $c_0 = IV$. Suppose c_q contains a transmission error for some $0 \leq q \leq t$. Which plaintext blocks m_i will be recovered *incorrectly*?

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