# Homework 6 – Due Tuesday, February 28

1. Textbook, page 229, Problem 7.11.

2. (*This is a repeat of a question from the last homework, with CBC mode replaced with CBC-CTS mode. Hint: It may not be clear from Figure 7.18 in the book, but the part of the ciphertext marked "X" in that diagram does not need to be transmitted.*) You are developing an application in which you have to regularly send packets that are 36 bytes (288 bits) long using AES. If you use CBC-CTS mode, how much data do you need to transmit? Be sure to explain the reasoning behind your answer (show your work).

3. A secure PRNG should have unpredictable future outputs if it is generating bits from an unknown seed, and many cryptographic applications have been broken in practice because of PRNGs that don't satisfy this property. Consider a hardware version of the CTR-mode PRNG described in the book (pages 243 and 244), but with the following change: rather than the seed being used for both $K$ and the initial value of $V$, the seed is only used to initializes $V$ while $K$ is a fixed secret embedded in the hardware and only known to the manufacturer.

   (a) Show how the manufacturer can predict all future outputs, given just the first 128 bits of pseudorandom output. Explain precisely what the attacker/manufacturer does to predict future outputs. (Note: This is called a "backdoor"!)

   (b) Do you think that this PRNG is secure against an attacker that does not know $K$? Try to give some reasoning/justification for your answer, but I'm not expecting a detailed argument.