Homework #2
Due: Tuesday 10/4 Before Class

1. Problem 2, Page 143.
2. Problem 12, Page 145.
4. Problem 17, Page 145.
5. Problem 18, Page 145.
6. Problem 2, Page 182.
7. Problem 3, Page 182.
8. Problem 4, Page 182.
10. Section 6.4.1 describes a man-in-the-middle attack on the Diffie-Hellman key exchange protocol in which the adversary generates two public/private key pairs for the attack. Could the same attack be accomplished with one pair? Explain.
11. Problem 2, Page 236.
12. Problem 3, Page 236.
13. Problem 2, Page 255.

Before submitting this homework, you should keep a copy for yourself. I will post the solutions after the submission and you can check your answers.