Homework 8, due April 27
Network Security book, chapters 1 and 2

1. What is the dedication to the book?
2. 2-3 (page 55)
3. Give a use of a cryptographic hash that relies on the property that it be infeasible to produce two messages with the same message digest?
4. Would the following be a good secret key integrity check? Append your secret to the message and do a checksum. As someone pointed out, if someone sees a message with a proper integrity check, it allows you to recover the secret (assuming the checksum is at least as large as the secret). How can you recover the secret in this case?

How about instead having a secret which is much larger than the checksum (say a 32 bit checksum and a 256 bit secret)? What is the problem with having the checksum be the sum of all the 32-bit words of the data and secret?
5. Suppose I want to tell you, before anyone else hears, what the name of the next CEO will be, from a list of, say, 200 potential candidates. I send you a message, encrypted with your public key, that consists of the name of the to-be-selected CEO. Suppose someone eavesdrops on the message. Will they be able to discover who the next CEO is without knowing your private key (but knowing your public key)?
6. What is binary 10101010 XOR 11110000? Call that answer “A”. What’s A XOR 11110000? What’s A XOR 10101010?
7. Suppose your encryption scheme is to take your message and XOR it with a “one-time-pad”, (a previously agreed-upon and somehow securely agreed-upon by both sides), where the one-time-pad is at least as long as the data. Assuming the one-time-pad was generated by truly random data, what fraction of the bits in the one-time-pad will be 0’s? Once it gets XOR’ed with the data, how many bits in the data will change? Would an encryption scheme be more secure if there were a way of ensuring that ALL bits in the data change after encryption?
8. If you’re encrypting in CBC mode, and ciphertext block #k is lost before it reaches the destination, but all other ciphertext blocks arrive, how many of the plaintext blocks will the recipient be able to recover?
9. Assume a good cryptographic algorithm. Assume a breakthrough in computer speed that suddenly makes computers 100 times faster. Assume both the good guys and bad guys now have faster computers. Does this work to the advantage of the good guys, the bad guys, or neither? Why?
10. Why does the RSA algorithm require the modulus not to be prime?