Homework 1, due at next lecture

1. Acquire the book. (57 pts :-) per copy!)
2. Read chapters 1 and 2
3. (1 pt) What is the dedication to the book?
4. Tell me your background. How much do you know about networking? About cryptography? (Note: you will not be graded on this answer!)
5. (2 pts) Chapter 2, problem 3:
   Suppose Alice, Bob, and Carol want to use secret key cryptography to authenticate each other. Compare the security of having a single shared secret that they all share with the security of having each of them use their own secret (Alice authenticates to either Bob or Carol by proving knowledge of K_A, Bob with K_B, and Carol with K_C).
6. (2 pts) Chapter 2, problem 6
   Assume a cryptographic algorithm that is linear in the length of the key to perform “good guy operations”, e.g., encryption, decryption, key generation, integrity check generation, integrity check verification; and that it is exponential in the length of the key to perform “bad guy operations”, e.g., brute force breaking. Suppose advances in computation make computers an order of magnitude faster. Does this work to the advantage of the good guys, the bad guys, or neither?
7. (4 pts) Assuming a very large message, and public user keys, describe what information would be included in each of the following:
   . Bob sending an unencrypted, signed message to Alice
   . Bob sending an unencrypted, signed message to multiple recipients (say Alice and Carol)
   . Bob sending an encrypted, signed message to Alice
   . Bob sending an encrypted, signed message to Alice and Carol

   Explain efficiency issues, and alternate methods that would work but be less efficient.

8. (4 pts) Assuming a very large message, and shared keys between each pair of users, describe what information would be included in each of the following:
   . Bob sending an unencrypted, integrity protected message to Alice
   . Bob sending an unencrypted, integrity protected message to Alice and Carol
   . Bob sending an encrypted, integrity protected message to Alice
   . Bob sending an encrypted, integrity-protected message to Alice and Carol

   As with problem 7, explain how the particular encoding you choose makes it efficient in terms of bandwidth and computation, and contrast it with alternatives.

9. (1 pt) If you want nonrepudiation, would it be easier to use public or secret user keys? How about plausible deniability? Why?