Homework April 18, due April 25

1. Read chapters 20, 21

2. (2 pts) Chapter 21, problem 3

3. (2 pts) Chapter 21, problem 5

4. (2 pts) Chapter 21, problem 6

5. (2 pts) Chapter 21, problem 10

6. (2 pts) Chapter 21, problem 11

7. (2 pts) Chapter 20, problem 7

8. (2 pts) Chapter 20, problem 6

9. (3 pts) (credit to Kenny Fong for noticing this bug in the book). The protocol in section 16.5.2 suffers from the weakness discussed in class. What if the protocol were changed so that what was asked was "find a message whose digest has the bottom 27 bits equal to x"? How would one ensure that it wasn't just any message, but one that will enable Bob to verify the message as a valid cookie? And would that protocol fix the weakness that Kenny Fong reported?