Fall 2010 – CS 686 Special Topics - Security and Privacy
Assignment 1
Due at 11:59pm on Friday, Oct. 1

1. (10 points) Problem 2.2
2. (20 points) Problem 2.11
3. (30 points) Problem 3.6
4. [Optional: 15 points] Research WPA and WPA2 flaws and answer the following questions in your choice of an attack. Brute-force attack or dictionary attacks are not valid answers. For example, password cracking on WPA-PSK using dictionary attack is not a valid answer. WPA-TKIP vulnerability and WPA2 Hole196 are good candidates.
   (a) (5 points) Give the name of the attack of your choice. Describe what assumptions are made for this attack to work. Discuss how realistic these assumptions are. (For example, dictionary attack assumes the password is a word in the provided dictionary. This can be realistic if the dictionary is sufficiently big.)
   (b) (10 points) Describe what countermeasures can be deployed to prevent this attack.