

## **COMP 690 E-commerce Fall 2006 Written Assignment 5**

Due in the digital drop box by Mon., Nov. 20, 11:00 PM

The following relate to the material in chapter 5 of your text.

- 1.** Which of the six dimensions of e-commerce security are supported by (1) symmetric key encryption, (2) public key encryption (without digital signatures and hash digests), and (3) public key encryption with digital signatures and hash digests? Justify yours answers. (This is essentially  $6 \times 3 = 18$  justifications—keep them brief and to the point.)
- 2.** It is generally agreed that the greatest security threats for an organization come from people inside the organization. Discuss ways an organization may protect against such threats. Consider especially how techniques discussed in the text to counter outside threats may be used to protect against insiders.
- 3.** Well-known techniques to provide nonrepudiation and authenticity typically rely on the fact that a person is associated with a platform or (in a larger system) an account. The problem is that someone else might use my PC or my account. Discuss ways to guarantee that the person using the platform or account is indeed the person authorized to use it. Your text discusses at least one way to do this. You have encountered other ways (most of which require you to remember something personal), and you can probably think of new ways. Try to find a weakness with each technique.

Problem 1 is worth more than problem 2, which in turn is worth more than problem 3. Typically, the answer to a problem that is worth more should be longer than the answer to a question that is worth less.