ECE: Information and Network Security
Homework 4
Spring 2006

Chapter 8: Book Problems 3, 4

Chapter 10: Book Problems 4, 5, 6

Supplemental Problems:

1. Suppose Bob is a server, and Alice is a client. Bob is not allowed to store any challenges he issues to Alice (perhaps he is resource limited). To bypass this issue, the following protocol is proposed in which Alice sends back the challenge (nonce) to Bob:

$$A \rightarrow B : ID_A$$

$$B \rightarrow A : r$$

$$A \rightarrow B : \{r, E_{K_{AB}}(r)\}$$

where r is the nonce, and K_{AB} is a key shared between Alice and Bob. Does this protocol achieve mutual authentication? Is it secure?

2. Consider the following authentication protocol. Alice generates a random message r and encrypts it with the key K she shares with Bob, and sends

$$A \rightarrow B : E_K(r)$$

to Bob. Bob deciphers it and adds 1 to r and sends

$$B \rightarrow A : E_K(r+1)$$

to Alice. Alice deciphers and compares it with r. If the difference is 1, she knows that her correspondent shares the same key and is therefore Bob. If not, she assumes that her correspondent does not share K and so is not Bob. Does this protocol authenticate Bob to Alice? Why or why not?