Practice Homework for the Final
Introduction to Information Security (266-642) [Spring 2008]
Due Date: None

In the homework, "the Stallings book" refers to [Sta06] and "the Handbook" refers to [MOV97] (I have linked the Handbook to the class homepage. You can download it for free.) Unless otherwise stated each part of a question has equal weight.

Question 1 (X.509:

Part A: Problem 14.3 from the Stallings book.

Part B: Consider the CAs arranged in a hierarchy as shown in Figure 1. Show the various certificates used to "navigate" the hierarchy. Demonstrate the chain that "validates" the public key of `Alice` to `Bob` and vice-versa.

Question 2

Part A: How do SYN-cookies protect a server from flooding attacks?

Part B: In a distributed-reflected denial-of-service attack, whose address is sent as the Source-IP of the SYN? Whose address is sent as the Source-IP of the SYN/ACK? Explain your answer. Use the following terminology:

M (Malicious Flood Generator)
R (Reflection Server (Innocent Bystander))
V (Victim of the Attack)

Question 3 (Authentication Protocols):

Problem 15.4 from the Stallings book.

Question 4 (SSL):

Part A: Problem 16.1 from the Stallings book.

Part B: Problem 16.2 from the Stallings book.

References

[MOV97] A.J. Menezes, P.C. Van Oorschot, and S.A. Vanstone. *Handbook of Applied Cryptography*. CRC press, 1997.

[Sta06] William Stallings. *Cryptography and Network Security: Principles and Practice*. Prentice Hall, 2006.

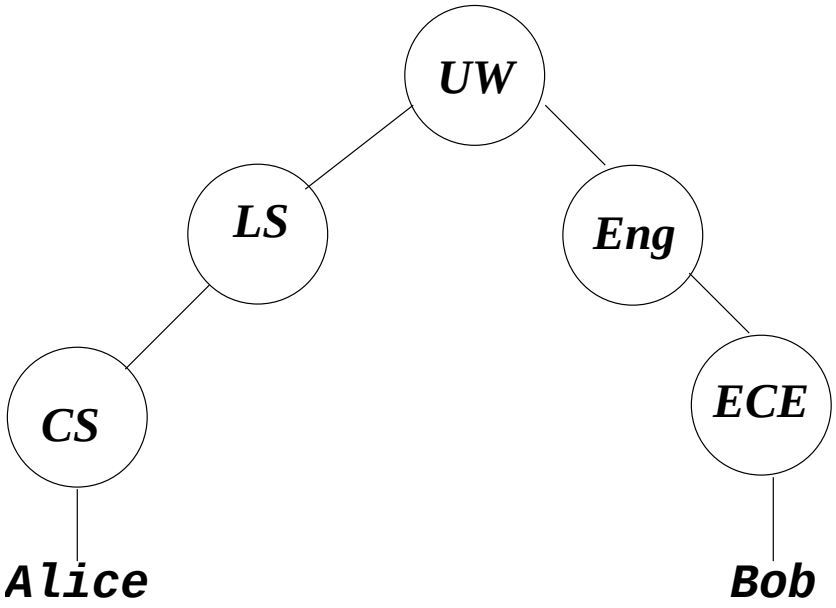

Figure 1: Hierarchy of certificate authorities.