Homework 5
Introduction to Information Security (266-642)
Due Date: April 18, 2003 (Friday)

Note: You can talk to your classmates, instructor, and TA about the problems. However, unless stated otherwise, problems should be written up individually. University of Wisconsin rules for academic misconduct apply.
This is a long homework (200 points), so it has a higher weight. Please start early.
In the homework, "the Stallings book" refers to [Sta03] 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 (Authentication Protocols [40 points]):
Part A [20 points] Problem 13.1 from the Stallings book.
Part B [20 points]: Problem 13.2 from the Stallings book.

Question 2 (DSA [60 points]):
Part A [20 points] : Assume that Alice uses the same random number k to sign two messages M and M'. Demonstrate that if Oscar knows the two signatures, he can derive the private key x.
Part B [20 points]: Show that knowing the random number x is *equivalent* to knowing the random number k, i.e., if Oscar knows x, he can find k and vice-versa.
Part C [20 points]: Problem 13.13 from the Stallings book.

Question 3 (Kerberos [60 points]) : For this question you have to read the explanation of Kerberos version 5 and appendix 14A from the Stallings book. Moreover, please read my note on interrealm authentication in Kerberos version 5.
Part A [20 points] : Problem 14.1 from the Stallings book.
Part B [20 points] : Problem 14.2 from the Stallings book.
Part C [20 Points]: Suppose there is a "trust relationship" between realms in the CS and Biology department. Bob, who a is user in the CS realm, wants to access a server V in the Biology realm. Show the various steps required for Bob to authenticate himself to V.

Question 4 (X.509 [40 points]):
Part A [20 points]: Problem 14.3 from the Stallings book.
Part B [20 points]: Consider the CAs arranged in a hierarchy as shown in Figure 1. Show the various certificates used to "navigate" the hierarchy. Show the chain that "validates" the public key of `Alice` to `Bob` and vice-versa.

References

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

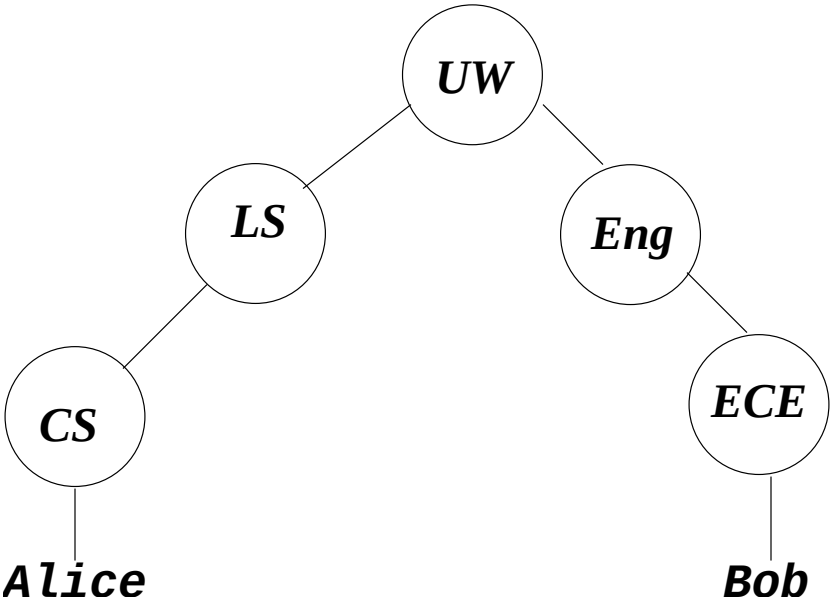

Figure 1: Hierarchy of certificate authorities.

[Sta03] William Stallings. *Cryptography and Network Security: Principles and Practice*. Prentice Hall, 2003.