Problem Set 7

Due in class on Thursday, November 17, 2005.

In the problems below, “textbook” refers to Introduction to Cryptography with Coding Theory: Second Edition by Trappe and Washington.

Problem 32: Discrete log authentication
Textbook, problem 14.3.2.

Problem 33: Challenge-response protocol
Textbook, problem 14.3.3.

Problem 34: Schnorr identification scheme
Textbook, problem 14.3.4.

Problem 35: RSA-based authentication scheme
Textbook, problem 14.3.5.