Problem Set 5

Due in class on Tuesday, November 1, 2005.

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

Problem 22: Factoring RSA Modulus

Alice's public RSA key is $n = 3737, e = 77$. Eve discovers that $d = 3413$. Use the method of lecture notes 12, section 1.3, to factor n. You may use a calculator or computer if you wish, but you should show the steps of the algorithm in finding the factors.

Problem 23: Solving Diophantine Equations

Textbook, problem 3.14.2 (computer problem).

Problem 24: Finding Primitive Roots

Textbook, problem 3.13.21.

Problem 25: Legendre Symbol

Textbook, problem 3.13.29.

Problem 26: Jacobi Symbol

Textbook, problem 3.13.30.