Problem Set 3

Due on Tuesday, October 17, 2006.

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

Problem 9: Linear Diophantine Equations

Problem 10: Euclidean Algorithm
Textbook, problem 3.13.5.

Problem 11: Quadratic Diophantine Equation

Problem 12: Chinese Remainder Theorem
Textbook, problem 3.13.10.

Problem 13: RSA Encryption
Textbook, problem 6.8.2.

Problem 14: RSA Attack
Textbook, problem 6.8.3.

Problem 15: RSA Decryption Exponent
Textbook, problem 6.8.5.

Problem 16: Factoring