Problem Set 3

Due in class on Tuesday, October 11, 2005.

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

Problem 11: Euclidean Algorithm

Textbook, problem 3.13.4.

Problem 12: Divisibility

Textbook, problem 3.13.7.

Problem 13: RSA Encryption


Problem 14: RSA Chosen Ciphertext Attack

Textbook, problem 6.8.7.

Problem 15: Factoring by the $p - 1$ Method

Write a computer program to factor numbers using the $p - 1$ method, described in §6.4 of the textbook. Your program should be written in C, C++, or Java and should use one of the big number libraries—gmp (if written in C), gmp or ln3 (if written in C++), or class BigInteger in java.math (if written in Java). Use your program to solve the following:

(a) Textbook, problem 6.9.4.

(b) Textbook, problem 6.9.5.

Note: The downloadable computer files referenced in the textbook are for Maple, Mathematica, and Matlab, which we are not using in this course. However, I have typed the numbers to be factored for this problem into files prob15a.dat and prob15b.dat and put them on the Zoo in the folder /c/cs467/course/assignments/ps3. This will save you the trouble of copying them from the textbook and the aggravation of having your programs fail because of a data input error.