Problem Set 6

Due in class on Tuesday, November 8, 2005.

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

Problem 27: Primality Testing

(a) Implement the Miller-Rabin primality testing algorithm so as to handle numbers at least 256 bits long. As usual, your program should be writtein in C, C++, or Java and should use one of the suggested big number libraries. If your library already contains a probabilistic primality tester, *do not use it* (except for checking) – implement your own instead. But it's okay to use built-in implementations of modular exponentiation, random number generators, and the other arithmetic functions and predicates.

(b) Twin primes are pairs of primes of the form $(p, p+2)$, e.g., $(11, 13)$. (See http://mathworld .wolfram.com/TwinPrimes.html.) Use your program from part (a) to find the smallest $p > 2^{255} + 100$ such that $(p, p+2)$ is a twin prime.

Problem 28: ElGamal Variants

Textbook, problem 9.6.4.

Problem 29: Existental Forgery of ElGamal Signatures

Textbook, problem 9.6.5.

Problem 30: Hash Function Based on Squaring

Textbook, problem 8.8.2.

Problem 31: Hash Function Based on Matrices

Textbook, problem 8.8.10.