Problem Set 4

Due in class on Tuesday, October 25, 2005.

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

Problem 16: Chinese Remainder Theorem

Textbook, problem 3.13.10.

Problem 17: Modular Exponentiation

By making appropriate use of Euler's theorem, the following two problems are readily solved *without use of a computer or calculator*. Solve these problems by hand, and show your work.

(a) Textbook, problem 3.13.12.

(b) Textbook, problem 3.13.13.

Problem 18: ElGamal Cryptosystem

Textbook, problem 7.6.11. In solving this problem, use the version of the ElGamal cryptosystem that is presented in the book, which differs slightly from the one presented in class.

Problem 19: Finding Square Roots

Textbook, problem 3.13.25.

Problem 20: Blum Primes

Show that -1 is a quadratic residue modulo an odd prime p iff $p \equiv 1 \pmod 4$.
[Hint: Apply the Euler criterion.]

Problem 21: Rabin Cryptosystem

Textbook, problem 3.13.27.