Problem Set 4

Due on Wednesday, March 24, 2010.

In the problems below, "textbook" refers to Wade Trapp and Lawrence C. Washington, *Introduction to Cryptography with Coding Theory, Second Edition*, Prentice-Hall, 2006.

Problem 1: Divides and mod

Textbook, exercise 3-7.

Problem 2: Chinese Remainder theorem

Textbook, exercise 3-10.

Problem 3: Euler theorem

Textbook, exercise 3-12.

Problem 4: Order

Textbook, exercise 3-20.

Problem 5: Rabin cryptosystem

Textbook, exercise 3-27.

Problem 6: Adaptive chosen ciphertext attack against RSA

Textbook, exercise 6-7.

Problem 7: Same modulus attack on RSA

Textbook, exercise 6-16.

Problem 8: RSA puzzle

Textbook, exercise 6-23.