Problem Set 4

Due on Monday, November 3, 2008.

In the problems below, "textbook" refers to Douglas R. Stinson, *Cryptography: Theory and Practice, Third Edition*, Chapman & Hall/CRC, 2006.

Problem 1: Homomorpohic Mapping χ

Textbook, problem 5.5.

Problem 2: Chinese Remainder Theorem

Textbook, problem 5.6.

Problem 3: Primitive Root

Textbook, problem 5.9.

Problem 4: RSA Speedup

Textbook, problem 5.13.

Problem 5: RSA Insecure Against Chosen Ciphertext Attack

Textbook, problem 5.14

Problem 6: RSA Common Modulus Failure

Textbook, problem 5.16.