Problem Set 4

Due on Monday, November 3, 2008.


Problem 1: Homomorphic Mapping $\chi$
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.