## YALE UNIVERSITY DEPARTMENT OF COMPUTER SCIENCE

CPSC 467a: Cryptography and Computer Security

Handout #2 September 20, 2005

## Professor M. J. Fischer

## **Problem Set 1**

Due in class on Tuesday, September 27, 2005.

Work each of the following problems from the textbook, *Introduction to Cryptography with Coding Theory: Second Edition* by Trappe and Washington.. For each problem, show your work and justify your answer, whether or not the question specifically requests this.

**Problem 1: Affine Cipher** 

Textbook, problem 2.13.2.

Problem 2: Vigenère Cipher

Textbook, problem 2.13.11.

**Problem 3: Hill Cipher** 

Textbook, problem 2.13.13.

**Problem 4: LFSR Machine** 

Textbook, problem 2.13.20.

**Problem 5: Big Numbers** 

Textbook, problem 2.13.23.

**Problem 6: Entropy** 

Textbook, problem 15.6.9.