Problem Set 2 (due October 11, 2004)

Submit electronically to ati@ccs.neu.edu and CC me.

Problem 1:

1. Describe an encryption scheme that you might have used as a kid to communicate securely, and that you thought is fairly secure. If you never did, then imagine a scheme or discuss with your little cousin ☺
2. Discuss the deficiencies of that scheme and how it might be broken.

Problem 2:
Textbook page 70, exercise 2.1.

Problem 3:
Textbook page 71, exercise 2.11.
Interpret that result.

Problem 4:
Textbook page 71, exercise 2.16.

Problem 5:
Implement the SPN encryption algorithm of example 3.1, page 76.

The following problems are only for graduate students only.

Problem 6:
Textbook page 70, exercise 2.4.

The following problems is only for PhD students only.

Problem 7:
Textbook page 72, exercise 2.20.