Problem Set 2 (due October 11, 2005 – 11:59pm)
Submit electronically to tmorgan@ccs.neu.edu and CC me.

Important note: submissions late by x.y days will have a penalty of 10*x.y% (e.g., submissions late by 2.5 days late result in 25% grade reduction).

Problem 1:
Textbook page 70, exercise 2.2.

Problem 2:
Textbook page 71, exercise 2.13.

Problem 3:
Textbook page 72, exercise 2.14. Assume the keys and plaintext distribution is equiprobable.

Problem 4:
Textbook page 71, exercise 2.17.

Problem 5:
Textbook page 72, exercise 2.19.

Problem 6:
Implement the SPN encryption algorithm of example 3.1, page 76.

The following problems is required only for PhD students only. Optional for MS students.

Problem 7: Coin Weighing

Suppose one has *n* coins, among which there may or may not be one counterfeit. If there is a counterfeit coin, it may be either heavier or lighter than the other coins. The coins are to be weighed by a two-pan balance. In each use of the balance you may put any number of the *n* coins on the left pan and the same number of the right pan, and push a button to initiate the weighing. There are three possible outcomes: either the weights are equal, or the left are heavier, or the left are lighter.

a. Find a upper bound on the number of coins *n* so that *k* weighing will find the counterfeit coin (if any) and correctly declare it to be heavier of lighter.
b. (more difficult) What is the coin weighting strategy for $k = 3$ weighing and 12 coins?