Homework Assignment #1A

Note

This assignment is due 2:20PM Tuesday, October 5, 2010. Please write or type your answers on A4 (or similar size) paper. Put your completed homework on the instructor's desk before the class starts. For late submissions, please drop them in Yih-Kuen Tsay's mail box on the first floor of Management Building II. Late submission will be penalized by 20% for each working day overdue. You may discuss the problems with others, but copying answers is strictly forbidden.

Problems

1. Solve the following exercise problems in Stallings' book (5th edition): 1.1 (5 points), 2.1 (10 points), 2.8 (10 points), 3.1(b) (5 points), 3.3 (10 points), 4.14 (5 points), 4.16 (10 points), 4.17 (10 points), 4.19(a)(b) (10 points), 4.26 (with $m(x) = x^2 + 1$; 10 points), 4.27 (with $m(x) = x^3 + x^2 + 1$; 10 points).

2. We have discussed in class a known plaintext attack on the Hill cipher. What are the criteria on the known plaintext-ciphertext pairs for the attack to succeed? Please be as precise as possible and explain the reasons for such criteria. (5 points)