Homework Assignment #1A

Note

This assignment is due 2:10PM Tuesday, October 2, 2012. Please write or type your answers on A4 (or similar size) paper. Drop your homework by the due time in Yih-Kuen Tsay's mail box on the first floor of Management Building 2. 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), 2.12 (10 points), 3.1(b) (5 points), 3.3 (10 points), 3.12 (10 points), 4.13 (do this for Z_{13} instead; 5 points), 4.14 (5 points), 4.19(a)(c) (10 points), 4.26 (10 points), 4.27 (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. (10 points)