CS355: Cryptography

Homework #4

Due date & time: 10:30am on November 4, 2005. Hand in at the beginning of class (preferred), or email to the TA (wangq@purdue.edu) by the due time.

The Late Policy and Additional Instructions for HW1 still apply. Ask for clarifications if you have questions about them.

Problem 1 (20 pts) Exercise 21 in Section 3.13 of the textbook. (Page 107)

Problem 2 (10 pts) Exercise 24 in Section 3.13 of the textbook. (Page 108)

Problem 3 (10 pts) Exercise 25 in Section 3.13 of the textbook. (Page 108)

Problem 4 (10 pts) Exercise 2 in Section 6.8 of the textbook. (Page 192)

Problem 5 (5 pts) Exercise 3 in Section 6.8 of the textbook. (Page 192)

Problem 6 (5 pts) Exercise 4 in Section 6.8 of the textbook. (Page 192)

Problem 7 (5 pts) Exercise 7 in Section 6.8 of the textbook. (Page 193)

Problem 8 (5 pts) Exercise 8 in Section 6.8 of the textbook. (Page 194)

Problem 9 (10 pts) Exercise 9 in Section 6.8 of the textbook. (Page 193)

Problem 10 (5 pts) Exercise 10 in Section 6.8 of the textbook. (Page 193)

Problem 11 (5 pts) Exercise 11 in Section 6.8 of the textbook. (Page 193)

Problem 12 (10 pts) Exercise 15 in Section 6.8 of the textbook. (Page 194)