CS 519
Cryptography and Network Security
Instructor: Ali Aydın Selçuk
Department of Computer Engineering, Bilkent University

Homework #6

Due December 13, 2012, beginning of the class

1. Problem 9.2.

2. Problem 11.3. (Note that compromise of a session key should not compromise any long term secrets.)

3. Problem 12.15.

4. Question 2, final exam of Fall 2010.