Institut for Matematik og Datalogi
Syddansk Universitet

May 5, 2008
JFB

Cryptology – F08 – Week 13

Lecture, April 30

We continued with zero-knowledge, from the notes and slides, and began on chapter 9, covering up through the presentation of Protocol 9.1 in the textbook.

Lecture, May 7

We will finish chapter 9 in the textbook and begin on chapter 10.

Lecture, May 13

We will cover sections 10.1, 10.2, and 10.5.4 of chapter 10, section 11.2 of chapter 11, and section 13.1 of chapter 13..

Lecture, May 15

We will begin on quantum cryptography from Charles H. Bennett, Franois Bessette, Gilles Brassard, Louis Salvail, and John Smolin, "Experimental Quantum Cryptography", J. of Cryptology 5, 1992. This can be found online through SDU's library.

Problem session May 14.

1. Continue with any unfinished problems from last week.
2. What group would you use for Diffie-Hellman Key Predistribution?
3. How might you remove the possibility of a Man-in-the-Middle attack in the Diffie-Hellman Key Agreement Scheme?

4. Do problem 10.1 d.

5. Do problem 10.7.

6. Do problem 10.8.