Institut for Matematik og Datalogi
Syddansk Universitet

May 19, 2003
JFB

Cryptology – F03 – Note 14

Lecture, May 13

We went through examples of zero-knowledge proofs.

Lecture, May 20

We will cover bit commitments which are computationally binding and unconditionally concealing. Then, we will cover secret sharing and oblivious transfer from the notes by Goldwasswer and Bellare, and introduce secure pseudorandom number generators.

Recall that the exam will be June 16.

The pensum is all subjects covered in the lectures and discussion sections. The relevant sections in the textbook and handouts are all mentioned in the weekly notes.