Institut for Matematik og Datalogi
Syddansk Universitet

December 6, 2006
JFB

Cryptology – E06 – Week 13

Lecture, November 30

We covered the Blum-Goldwasser Public-key Cryptosystem from chapter 8 and sections 10.1, 10.2, and 10.5.4 of chapter 10. We also covered section 11.2 and most of section 13.1.

Lecture, December 7

We will cover up through section 13.2.1 of chapter 13 and section 10.4 of chapter 10.

Lecture, December 14

We will cover chapter 14.

Problem session December 11

1. Do problem 13.2.
2. For the access structure in 13.3.a, give two distinct methods of destributing shares.
3. Do problem 10.4.