Institut for Matematik og Datalogi
Syddansk Universitet

May 25, 2005
JFB

Cryptology – F05 – Lecture 15

Lecture, May 20

We finished the zero-knowledge proof of graph nonisomorphism. Then, we covered bit commitments which are computationally binding and unconditionally concealing. Finally, we covered secret sharing from the notes by Goldwasswer and Bellare, and briefly introduced secure pseudorandom number generators.

Lecture, May 27

We will have a review of the course.

Announcement

Hjælp dine medstuderende, dygtiggør dig selv og få penge for det. Søg! Der er normalt relativt få ansøgere, så det er ofte muligt at få et instruktorat, selv om man ikke er langt i studiet. Hvis du har spørgsmål, så henvend dig gerne på IMADA. Ansøgningsproceduren er beskrevet på det officielle opslag, der kan findes via www.jobs.sdu.dk 14 dage inden ansøgningsfristen. Hvis du allerede er ansat som instruktor i efteråret 2005, leverer du ansøgning om tildeling af timer ind på IMADA's sekretariat (se opslag på gangene). Ansøgningsfrist: 9. juni 2005 kl. 12:00.