

Cryptology – E06 – Week 14

Announcement

Instruktører: Hjælp dine medstuderende, dygtiggør dig selv og få penge for det. Søg I dag!

Der er ofte gode muligheder for at få et instruktørats, selvom man ikke er langt henne i studiet. Hvis du har spørgsmål, så henvend dig gerne på IMADA. Ansøgningsproceduren er beskrevet på: www.jobs.sdu.dk. Hvis du allerede er ansat som instruktør i efteråret 2006, leverer du ansøgning om tildeling af timer ind på IMADAs sekretariat (se opslaget vedr. bilag mm.)
ANSØGNINGSFRIST: 20.12 2006 KL. 12:00.

Lecture, December 7

We covered up through section 13.2.1 of chapter 13 and up through Theorem 10.6 of section 10.4 of chapter 10.

Lecture, December 14

We will finish section 10.4 and cover through section 14.2 of chapter 14.

Lecture, December 21

We will finish chapter 14 and give some examples of zero-knowledge proofs.

Problem session December 18

1. Do problem 10.6.

2. Do problem 14.1, though rather than computing the entire matrix, explain the labels for the rows and columns and compute where there are ones in the column labeled $2 + 3x$.
3. Do problem 14.2.
4. Come with any questions you have about the exam.