Institut for Matematik og Datalogi
Syddansk Universitet

December 6, 2010
JFB

Introduction to Computer Science
E10 – Lecture 19

Lecture, December 6, 8:15–10, U37

We finished sections 7.5 and 7.6 in the textbook. Then we covered up through section 11.2 in chapter 11.

Lecture, December 9, 14:15–16, U71

We will continue with chapter 11 in the textbook.

Lecture, December 13, 8:15–10, U37

We will finish chapter 11 in the textbook.

Discussion section: December 20, 15:15-17, in U48a

Discuss the following problems from the textbook in groups of 3 to 4. (Think about these problems before coming to discussion section.)

1. Questions 1 and 2 on page 347.
2. Questions 1 and 2 on page 354.
3. Question 3 on page 362.
4. Questions 1, 2, 3, 4, and 6 on page 371.
5. Questions 4, 5 and 6 on page 375.
6. Questions 1 and 3 on page 376
7. Issues 1, 3, 5, and 6 on pages 386–387.

Assignment due 8:15, December 21

Late assignments will not be accepted. Working together is not allowed. (You may write this either in English or Danish.) Submit a single PDF file through the Blackboard system and include your name on the first page. If you submit this assignment more than once, use the same identification number both times. Remember to explain your answers (and show your work, including the steps for encoding and decoding).

1. Use the primes 13 and 17 to create keys (public and private) for use in RSA. Encrypt 23 with your keys. Decrypt the result. See the "Supplementary notes on RSA" from Lecture 12 for an algorithm for fast modulo exponentiation, which is used in the encryption and decryption.

2. Do problem 44 on page 569.