Institut for Matematik og Datalogi
Syddansk Universitet

February 9, 2005
JFB

Cryptology – F05 – Lectures 1 and 2

Textbook

Douglas R. Stinson, *Cryptography: Theory and Practice*, Second Edition, Chapman and Hall/CRC, 2002. There will also be supplementary notes.

Format

The course will be taught by Joan Boyar. The lectures will be in English. Discussion sections will usually be on Wednesdays. The Wednesday class scheduled for February 16 will mostly be a lecture on algebra (see the notes on the course's homepage). On Wednesdays we will begin at 8:45 and not have a break.

There will be assignments which must be approved in order to take the written exam in June. The assignments are considered "exam projects". Thus, you may not work with anyone not in your group. The assignments must be turned in on time. There will be a chance to redo at most one assignment (of the three or four), if it is either late or not good enough the first time.

The weekly notes and other information about the course are available through the WorldWideWeb. Use the URL:

http://www.imada.sdu.dk/~joan/crypt/index.html.

Lecture, February 11

We will begin with an introduction to the course. Then, we will cover sections 1.1.1–1.1.3 and 1.2.1–1.2.2 in the textbook. We may also cover the Vigenere cipher if there is time.

Lecture, February 16

We will cover the discrete math notes on algebra (starting on page 181) from the home page for the course.

Lecture, February 18

We will continue with chapter 1 in the textbook, skipping the Hill Cipher and begin on chapter 2.