Institut for Matematik og Datalogi
Syddansk Universitet

April 15, 2002
JFB

Computer Security – F02 – Lecture 10

Lecture, April 9

We will finish chapter 10 and begin on chapter 12 in the textbook.

Lecture, April 16

We will finish chapter 12 and begin on chapter 11 in the textbook.

Lecture, April 23

Brian Vinter will lecture on secure languages, compilers, sandboxing, etc. This will cover sections 11.5 and 11.6 in the textbook.

Discussion section, April 25

- Do problems 12.2, 12.3, 12.4, 12.5, 12.6, 12.9, and 12.11.
- Consider the DSA algorithm on page 210. How is it similar to El Gamal? Why does the verification work?
- Consider the table comparing RSA and DSA on page 211. How could verifications for RSA be so much faster than computing signatures? Does the table say anything about which one is better? Note that the table does not compare their relative security.

Announcement

Matalogifest

Information concerning the next Matalogifest, to be held on Saturday, May 4, can be found at

http://www.imada.sdu.dk/∼ jones/matalogi/