Institut for Matematik og Datalogi
Syddansk Universitet

December 8, 2016
JFB

Cryptology – E16 – Reading List

- Problems from the lecture notes.
- Nigel P. Smarl: Cryptography Made Simple, Springer, 2016, as corrected in the errata.

  Sections 1.1, A.6, A.7, A.8 (plus notes and slides on algebra).
  Section 1.3.
  Sections 7.1–7.4, page 164.
  Chapter 9.
  Section 11.2-11.5, plus the proof of Lemma 2.3 and the birthday bound on page 24.
  Sections 12.1–12.2.
  Sections 13.1–13.4
  Section 6.2.
  Chapter 14.
  Chapter 15.
  Chapter 2 (except section 2.5).
  Section 3.1.
  Sections 11.7, 11.8.2, 11.9.
  Sections 16.1–16.5.3.
  Sections 4.1, 4.1, 4.3, 4.5, with emphasis on curves of characteristic $p > 3$.
  Sections 19.1 and 19.4, with correctness from 19.2.
  Section 20.2.
  Chapter 21.
- Slides on RSA, primality testing, and zero-knowledge (available in hard copy from me).
- Slides on protocols, especially zero-knowledge (available in hard copy from me).