

Trondheim, November 16, 2006

Curriculum

TMA4155 Introduction to Cryptography, autumn 2006

The curriculum consists of the material covered in the lectures as well as the exercises and solutions. The following chapters in Trappe-Washington (2nd edition) mostly covers the curriculum:

- Chapter 1.
- 2.1-2.4, 2.7, 2.9, 2.10, (2.11),
- 3.1-3.7, (3.8).
- 4.1, 4.2, 4.5.
- 6.1, 6.3, 6.4, 6.7.
- 7.1, 7.2, 7.4, 7.5.
- 8.1, 8.4, 8.5.
- 9.1-9.5.
- Man-in-the-middle from 10.1.

The note on symmetric cryptography available from the web page covers some parts of the curriculum not covered by Trappe-Washington.

The chapters 2.11 and 3.8 as well as the material on the Hill cipher in 2.7 is supplementary material.