T-79.5501 Cryptology
Spring 2007

Lecture 3 topics in the text book:

- Theorem 2.11.
- Theorems 1.1 and 1.2
- Sections 5.2.1, 5.2.2
- Section 6.4

Unicity distance

- Result and proof of Theorem 2.11
- Example from Handout 1:

http://www.tcs.hut.fi/Studies/T-79.5501/2007SPR/lectures/handout1.pdf

Number theory and Finite Fields

- Euler's totient function,
  - Definition 1.3
  - Theorem 1.2; for the proof of the multiplicative property see Handout 2:

http://www.tcs.hut.fi/Studies/T-79.5501/2007SPR/lectures/handout2.pdf

- Extended Euclidean Algorithm, Section 5.2.1
- Chinese Remainder Theorem, Section 5.2.2
- Finite fields, Section 6.4