T-79.5502 Advanced Course in Cryptology

Spring 2006, Period IV

Instructor: Kaisa Nyberg

General

- **Room:** B353 reserved Tue and Thu 14-16
- **Lectures:** mainly March 14 – April 6 (with some dates cancelled)
- **Seminar:** presentations mainly April 20 – May 4
- **Exam:** Thu May 11, at 16-19, T1
- **Mandatory prerequisites**: either *T-79.5501 Cryptology* or *T-79.503 Foundations of Cryptology* taken and passed
- **Textbook:** Wenbo Mao: Modern Cryptography, Theory and Practice, Prentice Hall, New Jersey, 2004

Lecture topics

1. **Tue Mar 14:** Introduction. Two problems: (1) Security of the coin flipping , and (2) Authentication (Ch 1 - 2)

   Thu Mar 16: no lecture
2. **Tue Mar 21:** Computational complexity in cryptology (Ch 4)
3. **Thu Mar 23:** Insecurity of text-book crypto (Ch 8 -10)

   Tue Mar 28: seminar
4. **Thu Mar 30:** Authentication, Simmons theory. Confidentiality vs. Authentication. Unconditionally secure authentication. Protocols and attacks (Ch 11, Section 17.2.1)
5. **Tue Apr 4:** Formal and Strong Security Definitions I (Sections 14.1-4)
6. **Thu Apr 6:** Formal and Strong Security Definitions II (Sections 14.5-6)

Seminar Agenda

Tue Mar 28 Mikko Kiviharju: ID-based authentication frameworks and primitives (Ch 13)

Thu April 20 Vesa Vaskelainen: RSA-OAEP (Section 15.2 + papers)

Tue April 25 Aleksi Hänninen: Cramer-Shoup public-key cryptosystem (Section 15.3 + papers)

Thu April 27

- Santeri Saarinen: Strong and provable secure ElGamal type signatures (Section 16.3 + papers)
- Alessandro Tortelli: RSA and Rabin signatures, signcryption (Section 16.4-5 + papers)

Tue May 2 Samuli Larvala: Bellare-Rogaway model (Section 17.3 + papers)

Tue May 4

- Mika Silander: Interactive proof system and examples (Section 18.2 + papers) and
- Sami Kauppinen: Zero-knowledge properties and protocols (Section 18.3 + papers)