

**Comprehensive exam** Cryptographic protocols

**Syllabus** Protocols with three and more participants, byzantine agreement, simulation of broadcasting, impossible protocols. Authentication, key exchange. Protocols using symmetric and/or asymmetric encryption. Famous protocol vulnerabilities. Formal verification of protocols. The Büchi automaton, Dolev-Yao model, BAN logic, spi-calculus, model verification, automated proof theory.

- Bibliography**
1. Ronald Cramer, Ivan Bjerre Damgard, Jesper Buus Nielsen, Secure Multiparty Computation and Secret Sharing, Cambridge University Press, 2015
  2. Colin Boyd, Anish Marthuria: Protocols for Authentication and Key Establishment, Springer-Verlag, 2003.
  3. Adam Young, Moti Young: Malicious Cryptography, John Wiley & Sons, Inc., 2004
  4. Abadi, Gordon, A Calculus for Cryptographic Protocols: The Spi Calculus, I&C 148(1):1-70 (1999)