Introduction to Cryptography

ITC 8240

Lecturer: Ahto Buldas
ahto.buldas@ttu.ee

Topics of the Course

- Classical ciphers and their cryptanalysis
- Theory of unbreakable ciphers (Shannon's theory and implications)
- Mini-course in Group Theory
- Public key cryptography (RSA, ElGamal, etc)
- Cryptographic protocols (key establishment, authentication, zero-knowledge proofs)
- Introduction to quantum computation and post-quantum cryptography

Grades

- 2 written tests
- 2 homeworks (before the written tests)
- grade = arithmetic mean of the grades of the written tests
- exams: like tests, possibility to improve the grades of both written tests (or just one of them)

Schedule

- **Lectures**: on Monday 16:00-17:30 U06A-201 (start: Sep 9)
- **Practice hours**: on Wednesday (start: Sep 11)
  - 10:00-11:30 SCI-059 (IVCM 12)
  - 12:00-13:30 ICT-A2 (IVCM 11)
  - 14:00-15:30 ICT-A2 (IAPM)

Prerequisites

Students who:

- are NOT cyber security students specialized in crypto, AND
- must take this crypto course (ITC 8240)

must do the math test on Thursday, Sep 5 12:00 U06A-229

- passed: take this crypto course (ITC 8240)
- failed: take the math course (ITC 8190)

Should I Take the Math Course?