Towards the exam

- Written exam: January 13, 2019, 08.00-13.00 in MA 8.
- You must be approved on the 3 projects before the exam.
- Bring a good calculator!
- The following material will be provided on the exam (do not bring it!): List of formulas, BM algorithm in different versions. See course webpage for details.

Exam: 5 exercises, 10 points each.
Grading: Grade 3: 20-29; Grade 4: 30-39; Grade 5: 40-50;

Reading instructions

- Lecture notes and slides (and subjects as covered on lectures).
- Project descriptions (sometimes one exam problem will treat something from the projects).
- Exercises with solutions.

At your disposal you have old exams and corresponding short solutions on the course webpage.

Exam problems

Typically we will select 5 out of the following 6 topics and give one problem from each:

- Classic crypto and Shannon's theory of secrecy (chapter 2-3)
- Stream ciphers and LFSR sequences (chapter 4)
- Attacks on ciphers, block ciphers and hash functions (last part of chapter 4, chapter 5(+chapter 8 in Nigel's book), hash functions text
- Public key crypto (chapter 6)
- Authentication and secret sharing (chapter 7-8)
- "The theory behind" (chapter 1 and parts of other chapters)

Continuation course: Mathematical Cryptology

- Available only as a PhD course;
- Treats topics like: Elliptic curves, discrete logarithms and corresponding cryptosystems, complexity theory and provable security, random oracles, more on public key crypto, more on hash functions and block ciphers,...
- If you want to do more crypto, it can be possible through a project course. Contact Thomas.

Related subjects

- Information theory path: EIT080 Information theory vt2; Coding theory EIT080 ht1;
- Security path: Computer security vt1; Web security ht1; Advanced Computer Security ht1, Advanced Web Security ht2;...
- Master's Thesis projects:
  - Companies: Ericsson, Sony, Advenica, ...
  - Department: many projects in crypto and security...
- Others:
  - PhD studies: depending on external projects.
    Currently about to recruit one PhD student in crypto and one in security!