**Summary**
This course reviews some failure cases in public-key cryptography. It introduces some cryptanalysis techniques. It also presents fundamentals in cryptography such as interactive proofs. Finally, it presents some techniques to validate the security of cryptographic primitives.

**Content**
1. **Cryptographic security models**: security notions for encryption and authentication, game reduction techniques
2. **Public-key cryptography**: Factoring, RSA problem, discrete logarithm problem, attacks based on subgroups
3. **Interactive proofs**: NP-completeness, interactive systems, zero-knowledge
4. **Conventional cryptography**: differential and linear cryptanalysis, hypothesis testing, decorrelation
5. **Proof techniques**: random oracles, leftover-hash lemma, Fujisaki-Okamoto transform

**Keywords**
cryptography, cryptanalysis, interactive proof, security proof

**Learning Prerequisites**

**Required courses**
- Cryptography and security (COM-401)

**Important concepts to start the course**
- Cryptography
- Mathematical reasoning
- Number theory and probability theory
- Algorithmics
- Complexity

**Learning Outcomes**
By the end of the course, the student must be able to:
- Assess / Evaluate the security deployed by cryptographic schemes
- Prove or disprove security
• Justify the elements of cryptographic schemes
• Analyze cryptographic schemes
• Implement attack methods
• Model security notions

Teaching methods
ex-cathedra

Expected student activities
• active participation during the course
• take notes during the course
• do the exercises during the exercise sessions
• complete the regular tests and homework
• read the material from the course
• self-train using the provided material
• do the midterm exam and final exam

Assessment methods
Mandatory continuous evaluation:
• homework (30%)
• regular graded tests (30%)
• midterm exam (40%)

Final exam averaged (same weight) with the continuous evaluation, but with final grade between final_exam-1 and final_exam+1.

Supervision
Office hours No
Assistants Yes
Forum No
Others Lecturers and assistants are available upon appointment.

Resources
Bibliography

Ressources en bibliothèque
• Algorithmic cryptanalysis / Joux
• Communication security / Vaudenay
• A computational introduction to number theory and algebra / Shoup

Websites
• http://lasec.epfl.ch/teaching.shtml