# COM-501 Advanced cryptography

Vaudenay Serge

Cursus	Sem.	Туре	Language of	English
Computer science	MA2, MA4	Opt.	teaching Credits Session Semester	English
Cyber security minor	E	Opt.		6 Summer Spring
Cybersecurity	MA2, MA4	Opt.		
Data Science	MA2, MA4	Opt.	Exam	Written
Quantum Science and Engineering	MA2, MA4	Opt.	Workload 180h Weeks 14	
SC master EPFL	MA2, MA4	Opt.	Hours	4 weekly
			Lecture	2 weekly
			Exercises	2 weekly

## 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. The cryptograhic zoo: definitions, cryptographic primitives, math, algorithms, complexity

2. **Cryptographic security models:** security notions for encryption and authentication, game reduction techniques, RSA and Diffie-Hellman security notions

- 3. Public-key cryptanalysis: side channels, low RSA exponents, discrete logarithm, ElGamal signature
- 4. Interactive proofs: NP-completeness, interactive systems, zero-knowledge
- 5. Symmetric-key cryptanalysis: differential and linear cryptanalysis, hypothesis testing, decorrelation
- 6. 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



Number of positions

- 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	Yes
Others	Lecturers and assistants are available upon appointment.

## Resources

## Bibliography

• Communication security: an introduction to cryptography. Serge Vaudenay. Springer 2004.

• A computational introduction to number theory and algebra. Victor Shoup. Cambridge University Press 2005.

• Algorithmic cryptanalysis. Antoine Joux. CRC 2009.

## Ressources en bibliothèque

- Algorithmic cryptanalysis / Joux
- A computational introduction to number theory and algebra / Shoup
- Communication security / Vaudenay

# Websites

• https://lasec.epfl.ch/teaching.php

# **Moodle Link**

• https://go.epfl.ch/COM-501

# Videos

• https://mediaspace.epfl.ch/channel/COM-501+Advanced+Cryptography