COM-401 **Cryptography and security**

Vaudenay Serge

Cursus	Sem.	Type
Computer and Communication Sciences		Opt.
Computer science minor	H	Opt.
Computer science	MA1, MA3	Obl.
Cyber security minor	H	Opt.
Cybersecurity	MA1, MA3	Obl.
Data Science	MA1, MA3	Opt.
Financial engineering	MA1, MA3	Opt.
Minor in Quantum Science and Engineering	H	Opt.
Quantum Science and Engineering	MA1, MA3	Opt.
SC master EPFL	MA1, MA3	Obl.

Language of teaching	English
Credits	8
Session	Winter
Semester	Fall
Exam	Written
Workload	240h
Weeks	14
Hours	**6 weekly**
Courses	4 weekly
Exercises	2 weekly
Number of positions	

Remark

This course is a "depth" for Cyber Security master program and Cyber Security minor.

Summary

This course introduces the basics of cryptography. We review several types of cryptographic primitives, when it is safe to use them and how to select the appropriate security parameters. We detail how they work and sketch how they can be implemented.

Content

1. **Ancient cryptography**: Vigenère, Enigma, Kerckhoffs principle, Vernam cipher, Shannon theory
2. **Diffie-Hellman cryptography**: algebra, Diffie-Hellman, ElGamal, DSA
3. **RSA cryptography**: number theory, primality, RSA, factoring
4. **Elliptic curve cryptography**: elliptic curves over a finite field, ECDH, ECIES, ECDSA, pairing
5. **Symmetric encryption**: block ciphers, stream ciphers, exhaustive search
6. **Integrity and authentication**: hashing, MAC, AES-CCM, AES-GCM, birthday paradox
7. **Public-key cryptography**: key lengths, Fujisaki-Okamoto, hybrid encryption, post-quantum cryptography
8. **Trust establishment**: password-based cryptography, secure communication, trust setups
9. **Case studies**: TLS, WiFI, bitcoin, EMV, Signal, mobile telephony, Bluetooth, biometric passport

Keywords

cryptography, encryption, secure communication

Learning Prerequisites

Required courses

MATH-310 Algebra
MATH-232 Probability and statistics for IC
CS-250 Algorithms I

Recommended courses

COM-301 Computer security and privacy

Important concepts to start the course

- Mathematical reasoning
- Probabilities
- Algebra, arithmetics
- Algorithmics

Learning Outcomes

By the end of the course, the student must be able to:

- Choose the appropriate cryptographic primitive in a security infrastructure
- Judge the strength of existing standards
- Assess / Evaluate the security based on key length
- Implement algorithms manipulating big numbers and use number theory
- Use algebra and probability theory to analyze cryptographic algorithms
- Identify the techniques to secure the communication and establish trust
- Choose the appropriate cryptographic primitive in a security infrastructure
- Judge the strength of existing standards
- Assess / Evaluate the security based on key length
- Implement algorithms manipulating big numbers and use number theory
- Use algebra and probability theory to analyze cryptographic algorithms
- Identify the techniques to secure the communication and establish trust

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

Supervision

Office hours	No
Assistant.e.s	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.

Ressources en bibliothèque

• Find the references at the Library

Websites

• https://lasec.epfl.ch/teaching.php

Moodle Link

• https://go.epfl.ch/COM-401

Videos

• https://mediaspace.epfl.ch/channel/COM-401+Cryptography+and+security

Prerequisite for

• Advanced cryptography (COM-501)
• Seminar on applied cryptography (COM-506)