

COM-401

Cryptography and security

Vaudenay Serge

| Cursus | Sem. | Type |
|-------------------------------------|----------|------|
| Communication systems minor | H | Opt. |
| Computer and Communication Sciences | | Obl. |
| 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. |
| SC master EPFL | MA1, MA3 | Obl. |

| | |
|----------------------------|-----------------|
| Language of teaching | English |
| Credits | 7 |
| Session | Winter |
| Semester | Fall |
| Exam | Written |
| Workload | 210h |
| Weeks | 14 |
| Hours | 6 weekly |
| Courses | 4 weekly |
| Exercises | 2 weekly |
| Number of positions | |

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, Vernam cipher, Shannon theory
2. **Diffie-Hellman cryptography:** algebra, Diffie-Hellman, ElGamal
3. **RSA cryptography:** number theory, RSA, factoring
4. **Elliptic curve cryptography:** elliptic curves over a finite field, ECDH, ECIES
5. **Symmetric encryption:** block ciphers, stream ciphers, exhaustive search
6. **Integrity and authentication:** hashing, MAC, birthday paradox
7. **Applications to symmetric cryptography:** mobile telephony, Bluetooth, WiFi
8. **Public-key cryptography:** cryptosystem, digital signature
9. **Trust establishment:** secure communication, trust setups
10. **Case studies:** Bluetooth, TLS, SSH, PGP, biometric passport

Keywords

cryptography, encryption, secure communication

Learning Prerequisites**Required courses**

- Algebra (MATH-310)
- Probability and statistics (MATH-310)
- Algorithms (CS-250)

Recommended courses

- Network security (COM-301)

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

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

- 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

- [Communication security / Vaudenay](#)
- [A computational introduction to number theory and algebra / Shoup](#)

Websites

- <http://lasec.epfl.ch/teaching.shtml>

Prerequisite for

- Advanced cryptography (COM-401)
- Algorithms in public-key cryptography (COM-408)