# Introduction to cryptography

**Lecturers**
Christophe PETIT (Coordinator) and Gilles VAN ASSCHE

**Course mnemonic**
INFO-F405

**ECTS credits**
5 credits

**Language(s) of instruction**
English

**Course period**
First term

**Campus**
Plaine

## Course content

Historical aspects of cryptology. Symmetric and asymmetric encryption, integrity, authentication, digital signatures and key management. Notions of confidentiality and authenticity. Inner workings and usage of cryptographic algorithms.

## Objectives (and/or specific learning outcomes)

Understanding of fundamental computer security concepts and of classical cryptographic tools, algorithms and protocols. Know the usage limits and interoperability constraints of these different mechanisms.

## Pre-requisits and co-requisits

### Course having this one as co-requisit

MEMO-H504 | Mémoire de fin d'études en Informatique | 20 crédits

## Teaching method and learning activities

Lectures and practical exercises.

### Contribution to the teaching profile

Acquire knowledge in cryptograhy and computer security, being able to act as an scientific expert in problems solving, assimilate new concepts, develop a rigorous approach of scientific reasoning, being able to communicate in an adapted way (depending of the audience), being able to develop new competencies while respecting ethical aspects of the corresponding scientific field.

### References, bibliography and recommended reading

- Paar et Pelzl, *Understanding Cryptography*, Springer, 2011 (ISBN 978-3642041006)
- Katz et Lindell, *Introduction to Modern Cryptography (third edition)*, CRC Press, 2021 (ISBN 978-0815354369)
- Alfred J. Menezes, Paul C. van Oorschot et Scott A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1997

### Course notes

Université virtuelle

## Other information

### Place(s) of teaching

Plaine

### Contact(s)

- Gilles Van Assche, gilles.van.assche@ulb.ac.be
- Abel Laval, Département d'Informatique - CP212 Campus Plaine - N/O building, 8th floor, abel.laval@ulb.be
- Christhope Petit, Département d'Informatique - CP212 Campus Plaine - N/O building, 8th floor, christophe.petit@ulb.be

## Evaluation method(s)

written examination

### Evaluation method(s) (additional information)

Attendance at exercise sessions is a necessary criterion for success.

### Determination of the mark (including the weighting of partial marks)

Exam at the end of the quadrimester

### Main language(s) of evaluation

English

## Programmes

### Programmes proposing this course at the faculty of Sciences

MA-INFO | Master in Computer science | finalité Professional/unit 1 and MA-SECU | Master in cybersecurity | finalité Cryptalalysis and Forensics/unit 1 and finalité Corporate Strategies/unit 1

## Programmes proposing this course at the Brussels School of Engineering

MA-IRIF | Master of science in Computer Science and Engineering | finalité Professional/unit 1