UCLouvain

ldacs1310

2026

Introduction to Applied Cryptography

5.00 credits	30.0 h + 30.0 h	Q1

Teacher(s)	Peters Thomas ;Standaert François-Xavier ;
Language :	English > French-friendly
Place of the course	Louvain-la-Neuve
Prerequisites	· Discrete mathematics (as in LEPL1108 or LINFO1114) · Notions of probability (as in LBIR1212 or LEPL1108) · Computer programming (Python) and computational complexity (as in LEPL1401 or LINFO1101 and in LEPL1402) · Linear algebra (as in LEPL1101 or LINFO1112)
Main themes	The course will cover various introductory topics in cryptography and computational elements for its practical use: concepts of symmetric cryptography (pseudo-random functions, block ciphers, and Boolean functions), concepts of public-key cryptography (digital signatures, asymmetric encryption, and computation in simple fields and cyclic groups), and concepts of key exchange protocols as found in standards. Several common applications will also be discussed.
Learning outcomes	**At the end of this learning unit, the student is able to :** At the end of this course unit, students will be able to: · Understand the functionalities offered by the various cryptographic primitives used in authentication protocols and for building secure communication channels. · Understand how the security of cryptographic mechanisms is established. · Understand the impact of choosing different types of cryptographic mechanisms in terms of security and performance (in terms of time and energy). This course will contribute to the following learning outcomes frameworks for the Bachelor of Science in Computer Science program: S1.L1, S1.L3, S1.L8, S1.G1, S2.1, S2.2, S2.3, S2.4, S4.4, S5.2, S5.4, S5.5.
Evaluation methods	Students are assessed through a written examination.
Teaching methods	The course consists of lectures complemented by practical exercise sessions. Additional assignments may be proposed during the semester.
Content	The course covers the fundamental concepts of applied cryptography. - Security: perfect or computational, asymptotic or concrete. - Fundamentals of symmetric cryptography: pseudorandom generators/functions, secret-key encryption (block ciphers and modes of operation), message authentication codes, and hash functions. - Fundamentals of asymmetric cryptography: public-key encryption and digital signature schemes. - Authenticated encryption and its applications. - Standard algorithms: development processes and practical considerations. - Overview of post-quantum cryptography. The balance between these different topics may vary from year to year.
Bibliography	See on Moodle .
Faculty or entity in charge	DACS