UCLouvain

lmat2450

2022

Cryptography

5.00 credits	30.0 h + 15.0 h	Q1

Teacher(s)	Pereira Olivier ;
Language :	English > French-friendly
Place of the course	Louvain-la-Neuve
Learning outcomes	
Evaluation methods	The evaluation is based on a written examination. Homeworks proposed during the semester may contribute to the final grade, for at most 20% of the grade, and provided that it is to the student's benefit.
Teaching methods	The class is organised around lectures and exercise sessions. Homeworks may also be proposed. A specific attention is placed on the links between the theoretical concepts introduced in the class and the practical applications of cryptography.
Content	We introduce the core concepts of modern cryptography, with a specific focus on the mathematical and algorithmic aspects. Historical problems and constructions will be discussed and serve as a basis for the introduction of the core security notions and cryptographic mechanisms that are in use to day, as well as for the development of methods for justifying the security of these mechanisms. The contents may include: • Information theoretic cryptography, perfect encryption. • Probabilistic algorithms, computational security, attacker models, elaboration of security proofs in cryptography. • Symmetric encryption: security definitions, basis constructions, block ciphers (AES, DES), cryptanalysis, operation modes. • Authentication codes, hash functions. • Asymmetric cryptography: Diffie-Hellman protocol, public key encryption (ElGamal, RSA, ...), signature (Schnorr, DSA/DSS, RSA hash-and-sign, ...), public key infrastructures. • Basic algorithmic number theory (modular arithmetic, primality testing, elliptic curves) • Protocols: challenge-response, identification, authentication, zero-knowledge • Standards and norms: discussion, practical concerns, The balance between the various parts can vary from one year to another.
Inline resources	Moodle website.
Bibliography	J. Katz et Y. Lindell, Introduction to Modern Cryptography, 2nd edition. (Chapman and Hall/CRC Press). More references are available on Moodle.
Faculty or entity in charge	MATH

Programmes containing this learning unit (UE)

Program title	Acronym	Credits	Prerequisite	Learning outcomes
Additionnal module in Mathematics	APPMATH	5		
Master [120] in Mathematics	MATH2M	5		
Master [120] in Electrical Engineering	ELEC2M	5		
Master [120] in Computer Science and Engineering	INFO2M	5		
Master [120] in Computer Science	SINF2M	5		
Master [120] in Mathematical Engineering	MAP2M	5		
Master [120] in Data Science Engineering	DATE2M	5		
Master [120] in Data Science: Information Technology	DATI2M	5		