UCLouvain

lmat2450

2020

Cryptography

Due to the COVID-19 crisis, the information below is subject to change, in particular that concerning the teaching mode (presential, distance or in a comodal or hybrid format).

5 credits	30.0 h + 15.0 h	Q1

Teacher(s)	Pereira Olivier ;
Language :	English
Place of the course	Louvain-la-Neuve
Aims	*The contribution of this Teaching Unit to the development and command of the skills and learning outcomes of the programme(s) can be accessed at the end of this sheet, in the section entitled "Programmes/courses offering this Teaching Unit".*
Evaluation methods	**Due to the COVID-19 crisis, the information in this section is particularly likely to change.** The evaluation is based on a written examination. Homeworks proposed during the semester may contribute to the final grade. Answers can be provided in English or in French.
Teaching methods	**Due to the COVID-19 crisis, the information in this section is particularly likely to change.** 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	Aims
Master [120] en sciences mathématiques	MATH2M	5		
Master [120] : ingénieur civil en informatique	INFO2M	5		
Master [120] en sciences informatiques	SINF2M	5		
Master [120] : ingénieur civil électricien	ELEC2M	5		
Approfondissement en sciences mathématiques	LMATH100P	5		
Master [120] : ingénieur civil en mathématiques appliquées	MAP2M	5		
Master [120] : ingénieur civil en science des données	DATE2M	5		
Master [120] en science des données, orientation technologies de l'information	DATI2M	5		