UCL Université catholique de Louvain

LMAT2450

2010-2011

Cryptography

5.0 credits	30.0 h	1q

Teacher(s) :	Pereira Olivier ;
Language :	Anglais
Place of the course	Louvain-la-Neuve
Main themes :	The course will be devoted to the study of cryptography, this corresponding algorithms, various examples and possible protocols, with each time a mathematically oriented approach. Historical aspects will also be considered.1. Information theory ; public and secret keys.2. Probabilistic algorithms and proofs in cryptography.3. Some cryptographic algorithms, like DES, RSA, El-Gamal, Diffle-Hellman, complexity analysis.4. Active and passive attitudes, false signatures.5. The zero-knowledge theory.6. Elliptic curves in cryptography.7. Norms, standards, precautions.8. Examples of cryptographic protocols.9. A detailed example of a formal proof in cryptography.10. Theoretical aspects.
Aims :	We introduce the fundamental concepts of modern cryptography, with a special attention given to the mathematical and algorithmic aspects. Historical problems and constructions are discussed, and will serve as a basis for the construction and discussion of today's most widely used algorithms. The following aspects are discussed: 1. Elements of information theory, perfect encryption 2. Probabilistic algorithms, computational security, attacker models, construction and use of proofs in cryptography 3. Symmetric encryption: security notions, basic constructions, DES, AES, cryptanalysis, operation modes 4. Authentication codes, hash functions 5. Asymmetric cryptography: Diffie-Hellman protocol, public-key encryption (RSA, El Gamal, ...), signature (RSA, hash-and-sign paradigm, DSS, ...), public key infrastructures 6. Elements of algorithmic number theory (primality testing, factoring, discrete logarithm extraction, ...), elliptic curve cryptography 7. Protocols: challenge-response, identification, authentication, zero-knowledge, GQ protocol 8. Main cryptographic standards, how they are built, and how to use them. The relative importance accorded to these aspects can vary from year to year. *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".*
Other infos :	Prerequisites: Basic notions in linear algebra and modular arithmetic (bachelor level). Lectures in French, with all written materials in English Evaluation: Oral examination. References: The book by Jonathan Katz et Yehuda Lindell: Introduction to Modern Cryptography (Chapman & Hall/CRC Press, 2007) can be used as support for most of the topics covered in this class. Other useful references: - N. Koblitz: A course in number theory and cryptography, Springer-Verlag, Graduate Texts in Mathematics, 1994 (2nd edition) - W. Mao: Modern Cryptography - Theory and Practice, Prentice Hall PTR, 2003 - A. Menezes, P. Van Oorschot, S. Vanstone: Handbook of applied cryptography (CRC press, 1996) (freely available from) - S. Stinson: Cryptography, theory and practice, CRC Press, 2005 (3rd edition)
Cycle and year of study :	> Master [120] in Mathematics > Master [60] in Mathematics > Master [120] in Mathematical Engineering > Master [120] in Computer Science and Engineering > Master [120] in Computer Science > Master [120] in Electrical Engineering > Master [120] in Electro-mechanical Engineering

Faculty or entity in charge:	MATH