








Teacher(s)	Pereira Olivier ;Peters Thomas (compensates Pereira Olivier) ;
Language :	English > French-friendly
Place of the course	Louvain-la-Neuve
Prerequisites	It is recommended that students have a basic understanding of algebra as covered in LMAT1131 or LEPL1101 and of probability as covered in LMAT1271 or LEPL1108.
Main themes	The fundamental concepts of modern cryptography will be introduced, with particular attention to mathematical and algorithmic aspects. Historical problems and constructions will be discussed, which will serve as a basis for the presentation of the security concepts and algorithms most commonly used today, as well as for the justification of their security.
Learning outcomes	<p>At the end of this learning unit, the student is able to :</p> <p>Contribution of the course to the learning outcomes of the Master's programme in mathematics.</p> <p>At the end of this activity, the student will have progressed in his/her ability to :</p> <ul style="list-style-type: none"> - Know and understand a basic foundation of mathematics. In particular, he/she will have developed the ability to : <ul style="list-style-type: none"> -- Recognise the fundamental concepts of important current mathematical theories. - Demonstrate abstraction, reasoning and critical thinking skills. In particular, he/she will have developed the ability to : <ul style="list-style-type: none"> -- Identify unifying aspects of different situations and experiences. -- Reason within the framework of the axiomatic method. -- Construct and write a demonstration in an autonomous, clear and rigorous way. <p>Learning outcomes specific to the course.</p> <p>At the end of this activity, the student will be able to :</p> <ol style="list-style-type: none"> 1 - Describe, in a rigorous way, the function and security properties of the main primitives used in cryptography. - Construct attacks or proofs of the security of algorithms. - Recognise and articulate the main cryptographic techniques used to secure information. - Determine the existence of algorithms offering certain security guarantees in different contexts, notably on the basis of impossibility results. <p>Assessment of students' achievements :</p> <p>The evaluation is based on a written exam. Students are given the opportunity during the examination to present their solutions to the proposed questions orally.</p> <p>The knowledge and understanding of the concepts, examples and main algorithms introduced during the course are tested, as well as the ability to evaluate the security of cryptographic algorithms, either constructively (writing security proofs) or destructively (describing attacks). The student can choose the language of the exam (English or French).</p>
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	<p>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:</p> <ul style="list-style-type: none"> • 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.

	<ul style="list-style-type: none"> • 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, <p>The balance between the various parts can vary from one year to another.</p>
Inline resources	Moodle website.
Bibliography	J. Katz et Y. Lindell, Introduction to Modern Cryptography, 3rd 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		