	UE-SEC1: Cryptology	Semester 1
Contributes to	MICAS	

Coordinators:	Ghaya Rekaya-Ben Othman, Telecom Paris Michèle Wigger, Telecom Paris	
Volume:	30h	**3 ects**
Hours:	Lectures: 19.5h, Exercises: 9h	
Assessment:	1 Quizz and 1 Final Exam	
Language:	English	

Objectives:
The course provides an introduction to the most important concepts in cryptology such as: Shannon's cipher, block ciphers, pseudo random number generators, public-key cryptography, different types of attacks, secure hash functions, message authentication, and digital signatures.

Outcomes:
On completion of the course students should be able to:
- Know the most popular encryption systems and known attacks
- Know popular cryptographic concepts such as secure hashing, pseudo random number generators, message authentication, digital signatures

Prerequisite
- Algebra
- Introduction to Information Theory

Syllabus
- Historic ciphers, Shannon's cipher and perfect secrecy
- Block ciphers: Data encryption standard (DES), Triple DES, Advanced encryption standard (AES); Types of attacks
- Pseudo random number generators
- Topics in number theory and cryptographic hardness assumptions
- Public-key cryptography: Diffie-Hellman (DH), Rivest-Shamir-Adleman (RSA); Attacks
- Secure Hash Functions: Message digest algorithm (MD5), Secure hash algorithms (SHA); Attacks
- Message authentication
- Digital signatures

Bibliography:

- J. Katz and Y. Lindell, "Introduction to Modern Cryptography", 2007.
- M. Bellare and P. Rogaway, "Introduction to Modern Cryptography", 2005.