Course content
By the end of this course, students will be able to:

- Explain concepts related to applied cryptography, including plaintext, ciphertext, symmetric cryptography, asymmetric cryptography, and digital signatures.
- Experience the implementation and network standards behind the security of different cryptographic algorithms.
- Analyze and implement common network vulnerabilities and attacks, defense mechanisms against network attacks, and cryptographic protection mechanisms.

Objectives (and/or specific learning outcomes)
Provide a solid understanding of the design and analysis of network security architectures, protocols, and services. Most of these protocols are based on cryptographic primitives and can be used as building blocks for more sophisticated networked systems. During the course, we will perform an in-depth coverage of today’s network security standards, their functionality and limitations e.g., SSL/TLS, Kerberos, IPsec, Radius, IEEE 802.1x, WPA, etc. Furthermore, the students will acquire a practical knowledge and experience in deploying, configuring, and analyzing current network security tools and protocols.

We will also discuss recent trends in network security attacks, and cyber-attacks in general, and analyze variety of attacks with in mind the legal, technology, and society impacts.

Pre-requisites and co-requisites
Course having this one as pre-requisite
INFO-Y122 | Security Analysis: from audits to red teaming | 5 crédits
Programmes proposing this course at the faculty of Sciences

MA-SECU | Master in cybersecurity | finalité Cryptalalysis and Forensics/unit 1 and finalité Corporate Strategies/unit 1