

IDENTIFICATION

Course code : SEC602
ECTS : 1

DURATION

Lectures : 6
Tutorial classes : 22
Labs : 0
Total : 28

Project :
Personnal work :

ASSESSMENT

At least two written continuous assessments, and a lab report.

TEACHING MATERIALS

Slides, directed and practical work sheets, online learning platforms (CryptoHack, Root-Me).

LANGUAGE

English

CONTACT

Joël GROUFFAUD
joel.grouffaud@univ-reunion.fr

Modifié le : 14 juillet 2026

UE : UE6-CYBER

COURSE : Cybersecurity : Cryptography and Applications

SCOPE OF THE COURSE

OBJECTIVES

This course aims to provide essential cryptography knowledge for any computer science engineer, enabling them to select appropriate security tools for software or hardware systems, considering technical constraints (real-time data, energy-autonomous devices, etc.) and ANSSI recommendations to account for known weaknesses in certain protocols.

COMPETENCE AND SKILLS

- Select cryptographic tools suited to a specification requirement
- List and implement network protocols for IoT
- Design, from concept to production deployment, a company's IT network while integrating QoS and security considerations
- Manually deploy and administer services

PROGRAM

- Introduction to cryptography : basic vocabulary, key concepts.
- Classical cryptography : mono- and polyalphabetic substitutions, transposition, cryptanalysis.
- Symmetric block cryptography (AES), stream cryptography (ChaCha20).
- Asymmetric cryptography : Diffie-Hellman, RSA, ElGamal, elliptic curves.
- Hash functions, applications for integrity and authenticity : signatures, HMAC.
- Certificates, key management infrastructures.
- Use in classic protocols : SSH, TLS.
- Application examples : blockchain, anonymization on the Internet (Tor).
- Cryptanalysis : studying weaknesses in cryptographic tools and protocols.
- Introduction to SMPC and homomorphic encryption capabilities.
- Post-quantum cryptography : the quantum threat, post-quantum algorithms.
- Steganography.

BIBLIOGRAPHY

Johannes Buchmann - Introduction to Cryptography - Sciences Sup Collection
- Dunod Editions

REQUIREMENTS

Modules "Discrete Mathematics for Computer Science" (S5) and "Cybersecurity Principles 1" (S6).