

Cryptography

1. **Course number and name:** 020CRYES4 Cryptography
2. **Credits and contact hours:** 4 ECTS credits, 2x1:15
3. **Name(s) of instructor(s) or course coordinator(s):** Elie Aouad
4. **Instructional materials:** Handouts posted on the Web

5. Specific course information

a. Catalog description:

Introduction on threats and attacks – services: authentication, integrity, confidentiality, non-repudiation – security mechanisms and technics: algorithms, smart cards, key management, certificates... – recommendations and law – security protocols: PKCS, PKI, X509, SSH, ISO9735, SSL, S/Mime – API – practical cases: e-banking, e-commerce, e-notary, health.

b. Prerequisites: None

c. Selected Elective for CCE students

6. Educational objectives for the course

a. Specific outcomes of instruction:

- Learn cryptographic theories, principles and technics used to establish secure protocols.
- Analyze and use cryptographic methods.
- Apply the theories through practical work and exercises.
- Research on the limits and applicability of the cryptographic technics by developing a mini-project.

b. PI addressed by the course:

PI	1.3	2.1	2.2	2.3	2.5	4.2	6.1	6.2	6.3	7.1
Covered	x	x	x	x	x	x	x	x	x	x
Assessed	x	x	x	x	x					

7. Topics and approximate lecture hours

- Encryption Algorithms: Symmetrical, Asymmetrical, Algorithms with Keys, Hash Functions, Authentication Codes (4 lectures)
- TP and managed work (2 lectures)
- Mechanisms (2 lectures)
- PKI (2 lectures)
- TP (2 lectures)
- Research on Algorithms (2 lectures)

- PKCS (2 lectures)
- TP (2 lectures)
- Security Devices/Smart Cards (2 lectures)
- TP (2 lectures)
- Digital Signature Law (1 lecture)
- Research on real applications (1 lecture)