UVIC
UNIVERSITAT DE VIC
UNIVERSITAT CENTRAL
DE CATALUNYA

Study Abroad
INTERNATIONAL PROGRAMMES
UVIC | UMIC·UCC

Faculty: Science and Technology

Course: **Cryptography**

Program: Study Abroad in Engineering

Semester: 1 - Autumn

ECTS credits: 6

Duration: 45 hours

Language of instruction: English

Instructor: Iban Ricart

Course Description

This course builds on the fundamentals of modern cryptography. During the course, we will study the classic and modern techniques of cryptography. We will manage Python to try several techniques. We will learn the mathematics concepts that cryptography use. Finally, we will learn how computers use secure communication to share information.

Prerequisites

Basic knowledge about math and Python needed.

Attendance policy

Attendance is mandatory for all classes, including study visits. Any exams, tests, presentations, or other work missed due to student absences can only be rescheduled in cases of certified medical or family emergencies.

Learning outcomes

By the end of the course, students should be able to understand the main concepts related with cryptography, its principles and students should be able to implement basic code to encrypt and decrypt data.

Method of presentation

- Lectures and discussions: Lectures with appropriate visual support provide the theoretical content of the sessions. Class discussions facilitate the students' ability to connect reading and lectures, analyzing or applying concepts.
- Class participation: Students are expected to participate in group activities and in the discussions based on the course readings and cases proposed.
- Home exercises: Students are expected to solve several exercises during the semester.

Required work and assessment methods

- Cases, reading and exercises (65%). Preparation, development and discussions related to exercises will be highly valuable for the success of the course both at individual and group level.
- 2 Validation exams (35%). Individual tests.

Schedule. Content and Targeted Skills relations.

Unit One: Introduction to cryptography

Week 1. Course presentation. Introduction to cryptography. Classic cryptography theory. Math fundamentals.

Week 2. Introduction to Colab Environment and first applications. Classic cryptography

(Examples with Python). (E1. Introduction to cryptography with Python).

Unit Two: Symmetric cryptography

Week 3. Symmetric cryptography. Python exercises. (E1. Basic Symmetric cryptography with Python).

Week 4. Symmetric cryptography. Finishing the E2 activity. Maths and cryptography (First Steps). Mathematical theory of AES.

Week 5. Advanced Symmetric cryptography. (E3. Advanced Symmetric cryptography with Python)

Unit Three: Asymmetric cryptography

Week 6. Asymmetric cryptography. Python exercises. Mathematical theory of RSA and public keys.

Week 7. Asymmetric cryptography. (E4. Asymmetric cryptography project with Python).

Week 8. Asymmetric cryptography with Python. Revision of concepts.

Week 9. (T1. Test). Cryptography and symmetric and asymmetric techniques.

Unit Four: Secure connections

Week 10. Introduction to secure connections.

Week 11. Advanced concepts of secure connections. (E5. Activity. Secure connections).

Week 12. E5. Activity. Secure connections.

*Week 13. (*T2. Test). Secure connections and other cryptography concepts.

Week 14. E6. Final cryptography activity.

Week 15. E6. Final cryptography activity.

Activities weight. Ordinary evaluation

E1	E2	E3	E4	E5	E6	T1	T2
10	10	10	15	10	10	20	15

Retake exams and activities

The student must present the activities pending to delivery (E1 from E6). If the student passed the tests T1 and T2, it is not necessary to take the retake test. It is only mandatory to take the retake test if one or both tests were not passed.
The activities weight in the retake evaluation is the same as activities weight in the ordinary evaluation (see the percentages table), but the maximum grade is 5.