UAB
Universitat Autònoma de Barcelona

Information and Security

2026/2027

Code: 104418
Credits: 6

Degree programme	Type	Course
Computational Mathematics and Data Analytics	OP	4

Contact lecturer

Name : Carlos Garrigues Olivella

Email : carlos.garrigues@uab.cat

Teaching staff

Jordi Herrera Joancomarti

Cristina Fernandez Cordoba

Cristina Perez Sola

Group languages

You can consult this information at the end of the document.

Prerequisites

There are no mandatory requirements. It is advisable however to have gained the knowledge of previous subjects related to algebra, information theory, probability, and programming.

Objectives

This subject will give an introduction to cryptography. The main goal i for students to learn the fundamental principles and tools used nowadays in cryptography.

Learning outcomes

- KM33 (Identify the basic results of information security and cryptography.) Identify the basic results of information security and cryptography.
- KM34 (Identify the parameters determining security in the functioning of a system.) Identify the parameters determining security in the functioning of a system.
- SM40 (Use numerical methods to solve problems in cryptography and security.) Use numerical methods to solve problems in cryptography and security.
- SM42 (Distinguish, among the different mathematical tools, those that are feasible for implementation from those that are not.) Distinguish, among the different mathematical tools, those that are feasible for implementation from those that are not.

Contents

2. Introduction to cryptography
4. Mathematical foundations of cryptography
6. Symmetric key cryptography
8. Hash functions
10. Public key cryptography
12. Public key infrastructures
14. Cryptographic protocols

Learning activities and methodology

Title	Hours	ECTS	Learning outcomes
Session preparation	15	0.6	
Personal work	30	1.2	
Tutoring	15	0.6	
Theory lectures	30	1.2	
Study / preparation of examination	22.5	0.9	
Problems sessions	15	0.6	
Seminars / labs	15	0.6	

The course is taught in two weekly sessions of 2 hours each. Each session will be held in a single classroom with computers or the possibility of plugging in student laptops. There is no clear distinction between theory, problems and laboratory sessions. These will alternate during the course as appropriate to the follow-up of the subject. In general, for each topic to be addressed, theoretical concepts will be introduced together with some applied activities such as problem solving or seminars. It is recommended for students to review the materials for each session prior to the respective class. Active participation in problem solving will be encouraged participating in its resolution, presentation and debate in the classroom. During the course some laboratory practices or work seminars will be carried out, where one or more problems will be posed that will require the design and implementation of a complete solution.

More specifically, during the course we will alternate:

- Theory sessions: master classes where the goal is to introduce the basic concepts that allow students to get an overview and a good base from which to develop the contents and skills of the subject. The interactivity and active participation of the students will be promoted.
- Problem sessions: sessions in which problems or exercises are proposed, mainly as practical activities and follow-ups tests. These exercises have to serve the student to achieve and practice the concepts and competencies related to the subject. The problems are realized in the general case individually.
- Labs / seminars: there will be a wider problem than the ones treated in problem sessions such as a project or laboratory practice. This will be done and evaluated in groups. The number of labs to perform will depend on its difficulty and length and may change in each course.

The Moodle classroom of the UAB Virtual Campus will be used throughout the course as the main means of communication between teachers and students. That includes the publication of materials, publication of partial notes, forum of discussion, delivery of works, ...

Annotation: within the schedule set by the centre or degree programme, 15 minutes of one class will be reserved for students to evaluate their lecturers and their courses or modules through questionnaires.

Assessment

Continuous assessment activities

Title	Weight	Hours	ECTS	Learning outcomes
Problems and exercisses	15	1.5	0.06	KM33, KM34, SM40, SM42
Partial examination	45	3	0.12	KM33, KM34, SM40, SM42
Labs / seminars	40	3	0.12	KM33, KM34, SM40, SM42

The evaluation of the subject consists of the following parts:

- Partial test: partial examination that will consist of theoretical questions and/or practical exercises. Minimum grade for each separate part is 5.
- Exercises and problems: problem solving and exercises during the sessions of problems. They can be practical or theoretical activities. It does not require a minimum grade.
- Labs / seminars: group resolution of three case studies.

The results of the lab activities/seminars must be submitted through the virtual campus, but these submissions will not have any grade associated with them.

- The evaluation of the labs will be carried out solely through paper-based exams taken on the dates of the midterm exams.
- Although the labs are solved in groups, the lab exams are carried out individually.
- These exams will assess the assimilation of both the theoretical and practical concepts associated with each activity.
- Each of the 3 labs must be passed separately with a minimum grade of 4.5.

To pass the subject, the evaluation of each part (theory and labs) must reach the minimum required grade. In addition, the final grade calculated with the weights indicated above must reach 5 out of 10 points.

If this course is not passed because one of the assessment activities does not reach the required minimum grade, the numerical grade on the official transcript will be the lower value between 4.5 and the weighted average of the grades.

The "non-assessed" qualification will be awarded to students who do not participate in any of the assessment activities.

The qualification of "with honors" will be awarded to students with a mark equal to or greater than 9 by order of the best final grade.

The case of some small variation in the weighting of each part of the subject can occur. If this were the case, it would be communicated at the beginning of the course.

Recovery of marks from the continuous assessment:

A final test will be carried out that will allow the recovery of partial tests separately.

The possibility to retake any failed lab exams will also be offered. These retake exams will be held together with the final retake exam for the course.

The part of problems and / or activities that do not require a minimum mark can not be recovered.

Keeping partial marks for repeating students:

Repeating students will not keep the partial marks from previous years in the current course. However, this fact can be reconsidered at the beginning of the course depending on the availability of resources and specific content of the

assessed parts.

Dates for assessment activities:

The dates for test, assessments, work and practices deliveries will be published on the virtual campus and may be subject to change. All this changes will be always informed in the virtual campus, which is understood as the usual mechanism for exchanging information between teachers and students.

Likewise, the assessment mechanism, text, methodology or general operation of the course, that have not been specified in this guide will be detailed in advance.

For each assessment activity, a place, date and time of revision will be indicated in which the student will be able to review the activity with the teacher. In this context, claims can be made about the activity mark, which will be evaluated by the responsible teacher for the subject. If the student does not submit to this review, this activity will not be reviewed later.

Ethical Commitment:

Notwithstanding other disciplinary measures deemed appropriate, and in accordance with the academic regulations inforce, the irregularities committed by a student who can lead to a variation of the qualification will be qualified with zero (0). The assessment activities qualified in this way and by this procedure will not be recoverable. If you need to pass any of these assessment activities to pass the subject, this subject will be failed directly, without opportunity to recover it in the same course These irregularities include, among others:

- the total or partial copy of a practice, report, or any other evaluation activity;
- to let copy;
- present a group work not done entirely by the members of the group;
- present as own materials prepared by a third party, even if they are translations or adaptations, and generally works withnon-original and exclusive elements of the student;
- to have communication devices (such as mobile phones, smartphones, smartwatches, etc.) accessible during theoretical-practical assessment tests.

In these cases the final mark of the subject will be the lowest value between 3.0 and the weighted average of the marks (and therefore it will not be possible to pass the course by compensation).

Use of Artificial Intelligence (AI) Technologies

This course enforces a policy that restricts the use of Artificial Intelligence (AI) technologies. AI tools are permitted only for support tasks such as literature searches, information gathering, text correction, translation, or consulting documentation on functions and software libraries. The use of AI to generate complete solutions, write entire functions, or produce substantial portions of code is strictly prohibited. Students must clearly indicate any content generated with the help of AI and specify the tools or components used. Failure to transparently declare the use of AI in assessed work will be considered a breach of academic integrity and may result in partial or total loss of marks for the activity, or more serious disciplinary actions in severe cases.

Single assessment:

The subject does not offer the possibility of a single assessment.

Bibliography

- Herrera Joancomartí, Jordi; Pérez Solà, Cristina. La criptografia que et cal saber. (2023) Disponible on-line: https://criptografia.cat/
- Paar, C., Pelzl, J., Understanding Cryptography: A Textbook for Students and Practitioners. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010. https://doi.org/10.1007/978-3-642-04101-3. Biblioteca UAB: https://bibcercador.uab.cat/permalink/34CSUC_UAB/1eqfv2p/alma991010489805006709
- Smart, N. P., Cryptography Made Simple. Springer International Publishing, 2016. https://doi.org/10.1007/978-3-319-21936-3. Biblioteca UAB: https://bibcercador.uab.cat/permalink/34CSUC_UAB/1eqfv2p/alma991006792939706709

Software

Various software will be used during the course depending on the specific activity being carried out. We will use Python as the main programming language for solving exercises and labs, and the use of Linux system tools such as OpenSSL for some specific activity.

Course groups and languages

The information provided is provisional until November 30. After this date, you will be able to consult the language of each group through this link. To access the information, you will need to enter the course CODE