UAB
Universitat Autònoma de Barcelona

Data Security and Privacy

Code: 106568
ECTS Credits: 6

2024/2025

Degree	Type	Year
2504392 Artificial Intelligence	OT	3
2504392 Artificial Intelligence	OT	4

Contact

Name: Cristina Perez Sola

Email: cristina.perez@uab.cat

Teachers

Guillermo Navarro Arribas

Teaching groups languages

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

Prerequisites

For a better follow-up of the course, it is recommended to have basic programming skills acquired in the previous "Programming Fundamentals" courses.

Objectives and Contextualisation

This course covers the fundamental principles of data security and privacy through cryptography, providing a comprehensive understanding of both classical and modern cryptographic methods, and how to apply them to protect data in different real-world scenarios.

Competences

Artificial Intelligence

- Analyse and solve problems effectively, generating innovative and creative proposals to achieve objectives.
- Know and efficiently use techniques and tools for representation, manipulation, analysis and management of large-scale data.

Learning Outcomes

1. Analyse and solve problems effectively, generating innovative and creative proposals to achieve objectives.
2. Understand how public key infrastructure works.
3. Understand how symmetric and asymmetric cryptography works.
4. Understand the main data privacy models, their limitations and how they are used in data publication and processing.
5. Understand the risks of internet communication.

Content

- Unit 1: Introduction to Cryptography and Mathematical Foundations
- Unit 2: Classical Cryptosystems
- Unit 3: Symmetric Key Cryptography
- Unit 4: Hash Functions
- Unit 5: Public Key Cryptography
- Unit 6: Public Key Infrastructure
- Unit 7: Security and Privacy in Machine Learning

Activities and Methodology

Title	Hours	ECTS	Learning Outcomes
Type: Directed			
Lab activities	12	0.48	1, 2, 3, 4, 5
Problem solving classes	12	0.48	1, 2, 3, 4, 5
Theory lectures	26	1.04	2, 3, 4
Type: Supervised			
Tutorship	14	0.56	1, 2, 3, 4, 5
Type: Autonomous			
Exam study	25	1	1, 2, 3, 4, 5
Personal work	25	1	1, 2, 3, 4, 5
Problems and lab activities work	25	1	1, 2, 3, 4, 5

The official communication channel between students and teachers is the UAB's Virtual Campus.

The theory classes will be based on lectures, although efforts will be made to encourage student participation in solving examples, etc. In problem-solving classes, a list of exercises will be followed for students to attempt on their own. Encouragement will be given for students to present their problem-solving approaches. Practical sessions will delve deeply into related topics: real-world scenarios, expansion of specific subjects with alternative techniques and algorithms to those already covered.

Throughout the course, the following activities will be carried out:

- Theory Lectures: Theory will be presented with various example exercises, and efforts will be made to encourage student participation in their resolution.
- Problem-solving classes: These are sessions with the entire group or small groups aimed at applying theory to problem-solving. Students will have a list of problems to solve. In some cases, instructors may request solutions to exercises before the seminar and discuss their resolution during these sessions. These sessions are intended to promote analytical and synthetic skills, critical reasoning, problem-solving, and teamwork.
- Practical sessions: These will explore topics related to those covered in theory in depth. Emphasis will be placed on real-world scenarios, expanding on specific topics with alternative techniques and algorithms.
- Project presentation sessions: During the course, students will undertake a group project on the final topic of the subject. In project presentation sessions, some students will present their work while others will listen and ask questions. The topics presented during project presentation sessions will also be evaluated in the subject exams.

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

Continous Assessment Activities

Title	Weighting	Hours	ECTS	Learning Outcomes
Exams	5	3	0.12	1, 2, 3, 4, 5
Exercise solving	1	4	0.16	1, 2, 3, 4, 5
Final project	1	2	0.08	1, 2, 3, 4, 5
Lab activities	3	2	0.08	1, 2, 3, 4, 5

The dates for continuous assessment activities will be published on the virtual campus and in the course presentation slides. These dates may be subject to rescheduling due to possible incidents. Any changes will always be communicated through the UAB virtual campus, as it is understood to be the usual platform for information exchange between faculty and students.

The course assessment, out of 10 points, will be carried out as follows:

- Exams (5 points): Two individual midterm exams for a total of 5 points (2.5 points each). As part of continuous assessment, these tests will be conducted during the class sessions. Each test will separately assess a part of the syllabus, and the final grade will be the arithmetic mean of the two tests. Each test will only be averaged if it is graded higher than 4 out of 10. If any of the tests do not score higher than 4, the midterm exams will be considered failed.
- Exercises (1 point): As part of continuous assessment, students will submit the solutions to activities or exercises proposed throughout the course.
- Lab activities (3 points): As part of continuous assessment, some lab activities must be completed in the Integrated Laboratory. Each lab activity will only be averaged if it is graded higher than 4 out of 10. If any of the lab acitivies does not score higher than 4, the lab activities will be considered failed. The average of the lab activities grades should be higher than 5 out of 10 in order to pass the course.
- Final project (1 point): A written report and an oral presentation and defense of the final project has to be done.

Students who have failed the theory part of the course will have the option to take the final exam, which will cover the entire syllabus of the course, regardless of the scores obtained in the midterm exams. The grade of this recovery exam will be considered as the exam score for the final coursegrade calculation, accounting for 50% of the final course grade. To pass the course, the score of the recovery exam must be higher than 5 out of 10. Students who wish to improve their grades from the midterm exams can take the final exam for grade improvement. In this case, submitting the exam and having it graded by the instructor will overwrite the previous exam scores.

The submission of exercises, lab activities and the final project cannot be recovered.

For each assessment activity, a location, date, and time for review will be indicated, during which students can review the activity with the instructor. In this context, claims about the activity's grade can be made, which will be evaluated by the course instructor. If a student does not attend this review, the activity will not be reviewed later.

This course does not include a single assessment system.

Students who have previously taken the course and passed the lab activities will be able to retain their lab grades. However, it is important that they contact the lab instructors at the beginning of the course (when forming practical groups) to inform them of this. Under no circumstances will the theory exam scores, problem submissions nor the final project from previous courses be retained.

Without prejudice to other disciplinary measures deemed appropriate, and in accordance with current academic regulations, irregularities committed by a student that may lead to a variation in the grade will be graded with a zero (0). Assessment activities graded in this way and through this procedure will not be recoverable. If passing any of these assessment activities is necessary to pass the course, the course will be directly failed, without an opportunity to recover it in the same academic year. These irregularities include, among others:

- Total or partial copying of a practical, report, or any other assessment activity;
- Allowing others to copy;
- Presenting a group work not entirely done by the group members;
- Unauthorized use of AI (e.g., Copilot, ChatGPT, or equivalents) to solve exercises, practicals, and/or any other assessable activity;
- Presenting as one's own materials created by a third party, even if they are translations or adaptations, and in general, works with non-original and exclusive elements of the student;
- Having communication devices (such as mobile phones, smartwatches, etc.) accessible during individual theoretical-practical assessment tests (exams);
- Talking to classmates during individual theoretical-practical assessment tests (exams);
- Copying or attempting to copy from other students during theoretical-practical assessment tests (exams);
- Using or attempting to use writings related to the subject during theoretical-practical assessment tests (exams), when these have not been explicitly allowed.

In future editions of this course, students who have committed irregularities in an assessment act will not have any of their assessment activities validated. In summary: copying, allowing to copy, or plagiarism (or attempting any of these) in any of the assessment activities results in an immediate fail, non-compensable, and without validation of parts of the course in subsequent years.

Students who achieve the minimum number of points to pass the course but do not reach the minimum grade in any of the assessment activities will be graded with a final mark of 4.5. If the course is not passed due to a zero grade in an activity because of copying, the final course grade will be 3, which will not allow for the course to be compensated.

Finally, students who do not attend any individual tests (midterm exams and the final exam) will receive a grade of "Not Assessable." Participation in any of these assessment activities will result in a grade other than "Not Assessable."

No assessment activity will be conducted at a different time from the establishedscheduleunless there is a justified cause, prior notification before the activity, and consent from the instructor. In any other case, if a student does not attend an activity, it cannot be recovered.

Regarding honors grades, these may be awarded to students who have passed the course with a final grade of 9 or higher. Since the number of honors grades cannot exceed 5% of the enrolled students, they will be awarded to those with the highest grades. In case of a tie, the solutions proposed in each of the assessment activities carried out throughout the course will be considered.

Bibliography

- Cristina Pérez-Solà and Jordi Herrera Joancomartí. *La criptografia que et cal saber*. (2023) Available on-line: https://criptografia.cat/
- Christof Paar and Jan Pelzl. *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://cataleg.uab.cat/iii/encore/record/C__Rb1956470
- Nigel P. Smart. *Cryptography Made Simple*. Springer International Publishing, 2016. https://doi.org/10.1007/978-3-319-21936-3. Biblioteca UAB: https://cataleg.uab.cat/iii/encore/record/C__Rb1980662

Software

The lab activities of the course will be developed using Python.

Language list

Name	Group	Language	Semester	Turn
(PAUL) Classroom practices	1	English	first semester	afternoon
(TE) Theory	1	English	first semester	afternoon