Data Privacy and Security

Code: 104369
ECTS Credits: 6

2025/2026

Degree	Type	Year
Data Engineering	OT	4

Contact

Name: Guillermo Navarro Arribas

Email: guillermo.navarro@uab.cat

Teachers

Julián Salas Piñón

Teaching groups languages

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

Prerequisites

In this subject, we will make use of knowledge acquired during the degree. There is no mandatory requirement, but it will be assumed that students have a Cryptography base (corresponding to the subject Cryptography and Security) and basic knowledge of statistics, graphs, programming, and computer networks.

Objectives and Contextualisation

The objectives of the subject are:

- Understand the issue of privacy in digital environments.
- Knowledge of tools that provide privacy to various levels.
- Understand the main models of data privacy.
- Understand and know mechanisms for data evaluation and protection.
- Get to know some advanced cryptographic mechanisms for privacy.
- Knowledge of mechanisms for private communication.

Competences

- Demonstrate sensitivity towards ethical, social and environmental topics.
- Students must develop the necessary learning skills to undertake further training with a high degree of autonomy.

- Work cooperatively in complex and uncertain environments and with limited resources in a multidisciplinary context, assuming and respecting the role of the different members of the group.

Learning Outcomes

1. Demonstrate sensitivity towards ethical, social and environmental topics.
2. Students must develop the necessary learning skills to undertake further training with a high degree of autonomy.
3. Work cooperatively in complex and uncertain environments and with limited resources in a multidisciplinary context, assuming and respecting the role of the different members of the group.

Content

- Introduction to privacy
- Data privacy
  - Models: k-anonymity, differential privacy
  - Methods of protection for data privacy
  - Privacy and machine learning
- Private communications
- Cryptographic protocols for privacy

Activities and Methodology

Title	Hours	ECTS	Learning Outcomes
Type: Directed			
Practical sessions	25	1	1, 3
Theoretical sessions	25	1	1, 3
Type: Supervised			
Tutorials	10	0.4	1, 3
Type: Autonomous			
Preparation of practical sessions	25	1	1, 3
Preparation of theoretical sessions	37.5	1.5	1, 3

The subject is taught in two-hour sessions. These sessions will be organized dynamically and will require the active participation of the students. Throughout the course there will be sessions of more theoretical typology and another of practical typology.

Theoretical sessions can be structured in various ways. In some cases, the teaching staff, prior to the session, will make available to the students material on the topic to be discussed. In accordance with this material, different types of sessions will be structured. For example, question and answer sessions where the students will formulate the doubts that have arisen from the previous work on the material provided. In these sessions, the teaching staff will also challenge the students to bring out the most relevant aspects of the material being worked on. There will also be sessions where the students, in groups, will present a more detailed study of

some of the topics covered in the subject. Depending on the specific topic to be dealt with, the theory session can also be structured as a master class.

The practical type sessions include the resolution of questions or exercises, such as the resolution of more technical tasks of a practical type.

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
Activities in lecture sessions	40	14	0.56	1, 3
Practical activities	50	12.5	0.5	1, 2, 3
Topic presentation and preparation	10	1	0.04	1, 2, 3

This course uses a continuous assessment model uniquely. Given its dynamism and the involvement that students are asked for in all class sessions (both those of a more theoretical nature and the more practical ones), teachers will have multiple elements to be able to evaluate students. Active participation in classes, resolution of exercises or activities in class, are examples of evidence for evaluation.

Beyond the evaluation based on the contributions in the classes, the students will also have to deliver different works, exercises or activities that will be proposed throughout the course on the virtual campus of the UAB, deliveries that will complement the evaluation evidence of students. The evaluation of the participation might also include individual exam-like exercises to be done in class.

On the other hand, the presentation of the subject that the students will carry out in the theoretical sessions of the subject will also form part of the evaluation evidence.

Final evaluation and grades: The final evaluation is calculated by weighting the evaluation activities as follows:

- Activities in class: 40%
- Practical work: 50%
- Preparation and presentation of theme: 10%

The practical work requires a minimum grade of 5. If this part is not passed, it may be recovered, although in this case the maximum grade for the recovered part will be 5.

The class activities also require a minimum grade of 5, In case of not passing the evaluation of class activities and presentation of the theme, they cannot be recovered.

Students who achieve the minimum number of points to pass the subject, but have not reached the minimum grade in any of the evaluation activities, will be evaluated with a final grade of 4.5.In theevent that the subject has not been passed due to a zero grade for an activity due to copying, the final grade for the subject will be a 3, a fact that will not allow this subject to be compensated (see section on ethical commitment).

Those students who do not hand in any of the proposed activities will obtain the qualification of "Not Assessable". Participation in any of these evaluation activities will mean receiving a different qualification of

"Not Assessable".

Honors: Awarding an honors grade (MH) is the decision of the faculty responsible for the subject. The UAB regulations indicate that the MH may only be awarded to students who have obtained a final grade equal to or greater than 9.00. Up to 5% MH of the total number of students enrolled can be awarded.

Repeating students: No type of validation of the evaluable activities is contemplated for repeating students. This measure could be relaxed depending on the course and specific activity. If this were the case, the conditions and mechanisms for this will be announced at the beginning of the course.

Activities calendar: The dates of continuous evaluation and delivery of work will be published on the virtual campus and may be subject to changes in the programming for reasons of adaptation to possible incidents. These possible changes will always be reported on the virtual campus and in class, since these are the channels for exchanging information between teachers and students.

Grade review procedure: For each assessment activity, a review place, date and time will be indicated in which students will be able to review the activity with the teaching staff. In this context, claims may be made about the grade for the activity, which will be evaluated by the teaching staffresponsible for the subject. If the student does not show up for this review, this activity will notbe reviewed later.

Ethical commitment:

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 grade variation in an evaluable activity will be graded zero (0). The evaluation activities qualified in this way and by this procedure will not be recoverable. If it is necessary to pass any of these evaluation activities to pass the subject, this subject will be directly suspended, with no 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;
- let copy;
- present a group work not carried out entirely by the members of the group (applied to all members, not only to those who have not worked);
- unauthorized use of AI (eg Copilot, ChatGPT or equivalent) to solve exercises, practices and/or any other evaluable activity;
- Submit as your own materials prepared by a third party, even if they are translations or adaptations, and generally works with non-original and exclusive elements of the student;
- have communication devices (such as mobile phones, smart watches, camera pens, etc.) accessible during individual theoretical-practical assessment tests (exams);
- talk with classmates during individual theoretical-practical evaluation tests (exams);
- copy or try to copy from other students during the theoretical and practical evaluation tests (exams);
- Use or attempt to use writings related to the subject during the theoretical-practical evaluation tests (exams), when these have not been explicitly allowed.

The numerical mark of the file will be the lower value between 3.0 and the weighted average of the marks in case the student has committed irregularities in an actof evaluation (and, therefore, it will not be possible to pass by compensation). In future editions of this course, students who have committed irregularities in an evaluation act will not have any of the evaluation activities carried out validated.

In summary: copying, allowing copying or plagiarism (or the attempt to) in any of the evaluation activities is equivalent to a FAIL, non-compensable and without validation of parts of the subject in subsequent courses.

Single assessment: This subject does not contemplate the single assessment system.

Bibliography

Given the dynamism of the subject, many bibliographic references and material will be provided during the course. Here are some more generic references:

- Vicenç Torra (2022) Guide to data privacy : models, technologies, solutions. Springer.
- Cynthia Dwork, Aaron Roth (2014) The Algorithmic Foundations of Differential Privacy. Foundations and Trends in Theoretical Computer Science (vol. 9, núm. 3-4, págs. 211-407).
- Solon Barocas, Moritz Hardt, Arvind Narayanan (2009) Fairness and Machine Learning. https://fairmlbook.org/
- Anthony D. Joseph, Blaine Nelson, Benjamin I. P. Rubinstein, J. D. Tygar (2019) Adversarial Machine Learning. Cambridge University Press.
- Christof Paar, Pelzl Jan. (2010) Understanding Cryptography: A Textbook for Students and Practitioners. Springer Berlin Heidelberg, 2010.

Software

Given the multidisciplinary nature of this subject, we will use different tools and programming languages depending on the specific activity to be carried out, both for the labs and for the activities and exercises.

Groups and Languages

Please note that this information is provisional until 30 November 2025. You can check it through this link. To consult the language you will need to enter the CODE of the subject.

Name	Group	Language	Semester	Turn
(PAUL) Classroom practices	81	Catalan/Spanish	first semester	morning-mixed