Universitat Autònoma de Barcelona

2022/2023

Data Privacy and Security

Code: 104369
ECTS Credits: 6

Degree	Type	Year	Semester
2503758 Data Engineering	OT	4	1

Contact

Name: Guillermo Navarro Arribas
Email: guillermo.navarro@uab.cat

Use of Languages

Principal working language: catalan (cat)
Some groups entirely in English: No
Some groups entirely in Catalan: No
Some groups entirely in Spanish: No

Teachers

Cristina Perez Sola

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, or programming.

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.
- 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. 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

Methodology

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

Theoretical sessions can be structured in various ways. In a few cases the teacher, prior to the session, will make available to students material on the topic to be addressed. Based on this material, they will be structured
two different types of sessions. On the one hand, question sessions and answers where students will formulate the doubts that have arisen from the previous work on the material provided. In these sessions, the faculty will also challenge students to bring out more aspects relevant to the material being worked on. On the other hand, there will be sessions where students, in groups of two, will present some more detailed study of some themes treated in the subject. Depending on the specific topic, the theory session can also be structured as a master class.

Practical sessions include solving questions or exercises as the resolution of more technical work type practical.

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.

Activities

Title	Hours	ECTS	Learning Outcomes
Type: Directed			
Practical sessions	25	1	1, 2
Theoretical sessions	25	1	1, 2
Type: Supervised			
Tutorials	10	0.4	1, 2
Type: Autonomous			
Preparation of practical sessions	25	1	1, 2
Preparation of theoretical sessions	37.5	1.5	1, 2

Assessment

This subject uses a unique continuous assessment model. Given the dynamism of it and the involvement that is required of students in all class sessions (both theoretical and practical) teachers will have multiple elements

to be able to assess the students. Active participation in classes asking questions to the teacher and answering questions from other students or teacher questions will assume is an example of evidence for evaluation. It is for this reason that class attendance for this subject is mandatory.

Beyond assessment based on in-class contributions, the students will also have to hand in different more practical assignments to go proposing throughout the course in the virtual campus of the UAB, deliveries that they will complement the student's evidence of assessment.

On the other hand, the presentation of the topic that the students will do in the sessions Theorists of the subject will also be part of the evaluation evidence.

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

- Class participation: 20%
- Practical work: 50%
- Topic preparation and presentation: 30%

Both the practical work and the presentation of the topic require a grade minimum of 5. In case of not exceeding any of these parts, it will be possible to recover, although in this case, the maximum mark of the recovered part will be a 5.

In case of not passing the evaluation of the participation in class, this will not be will be able to recover.

If you do not pass the subject due to the fact that some evaluation activities do not reach the minimum grade required, the numerical final mark will be the lowest value between 4.5 and the weighted average of the marks.

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 awardedto students with a mark equal to or greater than 9 by order of the best final grade.

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 always be 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.

Other important aspects of the evaluation: Notwithstanding other disciplinary measures deemed appropriate, and in accordance with the academic regulations in force, 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 the 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 activity;
- to let copy;
- present a group work not done entirely by the group members (applied to all members, not just those who have not worked);
- to present as own, materials prepared by a third party, even if they are translations or adaptations, and in general works with non-original elements and student exclusives;
- to have communication devices (such as mobile phones, smart watches, camera pens, etc.) accessible during assessment tests;
- talk to classmates during assessment tests;
- copy or attempt to copy from other students during assessment tests;
- use or try to use writings related to the subject during the realization

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).

Assessment Activities

Title	Weighting	Hours	ECTS	Learning Outcomes
Participation in lecture sessions	20	14	0.56	1, 2
Practical activities	50	12.5	0.5	1, 2
Topic presentation and preparation	30	1	0.04	1, 2

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 (2017) Data Privacy: Foundations, New Developments and the Big Data Challenge. 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/
- Yevgeniy Vorobeychik, Murat Kantarcioglu. (2018) Adversarial Machine Learning. Synthesis Lectures on Artificial Intelligence and Machine Learning #38. Morgan & Claypool.
- Molnar, Christoph (2020). Interpretable Machine Learning: A Guide for Making Black Box Models Explainable.
- 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.