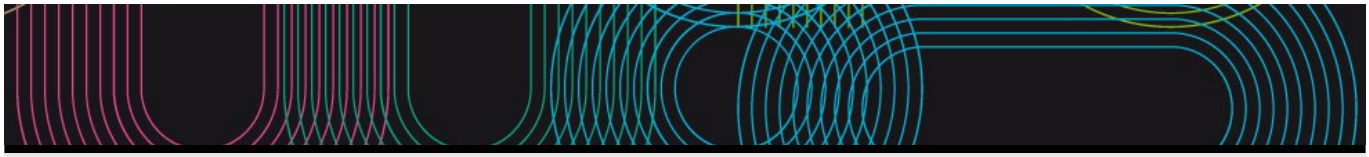

IDENTIFYING DATA				
Privacy and anonymity				
Subject	Privacy and anonymity			
Code	V05M175V11110			
Study programme	Máster Universitario en Ciberseguridad			
Descriptors	ECTS Credits	Choose	Year	Quadmester
	5	Mandatory	1st	1st
Teaching language	#EnglishFriendly Spanish			
Department				
Coordinator	Pérez González, Fernando			
Lecturers	Hernández Pereira, Elena María Pérez González, Fernando			
E-mail	fperez@gts.uvigo.es			
Web	http://http://moovi.gal			
General description	This subject presents the main techniques to provide privacy and anonymity in networks, systems and applications. It covers concepts and methods of differential privacy, privacy enhancing technologies (PET), geolocation privacy, machine learning privacy, and anonymity techniques. The implications of privacy by design, and ethical and legal aspects of privacy are also explored.			

Training and Learning Results	
Code	

Expected results from this subject	
Expected results from this subject	Training and Learning Results

Contents	
Topic	
Introduction. Attacks.	Introduction to privacy and anonymity. Inference attacks. Traffic analysis attacks. Online tracking.
Differential privacy.	Differential privacy. Differential privacy mechanisms. Composition theorems.
Privacy preserving and enhancing techniques.	Privacy-preserving primitives: information retrieval, set intersection. Privacy enhancement techniques with homomorphic encryption and secure multi-party computing. Bloom filters.
Anonymity.	Basic concepts. K-anonymity, l-diversity and t-proximity.
Applications in privacy and anonymity.	Geolocation privacy. Anonymous communications. Onion routing. Mixes. Anonymous authentication. Privacy in machine learning.

Planning	Class hours	Hours outside the classroom	Total hours
Laboratory practical	19	38	57
Lecturing	19	38	57
Problem solving	2	0	2
Objective questions exam	2	0	2
Report of practices, practicum and external practices	0	3	3
Report of practices, practicum and external practices	0	4	4
*The information in the planning table is for guidance only and does not take into account the heterogeneity of the students.			

Methodologies

	Description
Laboratory practical	Students will develop privacy and anonymity projects in the laboratory as applications of the techniques presented in the master classes. The practices or projects will be supervised by the teachers.
Lecturing	Systematic presentation of the course contents: concepts, results, algorithms, examples and use cases.
Problem solving	Solving problems in the classroom by teachers.

Personalized assistance

Methodologies	Description
Laboratory practical	Questions related to laboratory practices and the development of the project will be answered individually. Office hours will be established at the beginning of the course and will be published on the subject's website.
Lecturing	Individual attention will be given to students who require orientation for the study, additional explanation on the contents of the discipline, clarification or guidance on problem solving. Office hours will be established at the beginning of the course and will be published on the subject's website.
Problem solving	Queries about solving problems and exercises raised in class or worked independently will be addressed individually. Office hours will be established at the beginning of the course and will be published on the subject's website.

Assessment

	Description	Qualification	Training and Learning Results
Objective questions exam	Written exam. Resolution of questions, problems or exercises.	40	
Report of practices, practicum and external practices	Reports on the practices corresponding to the first half of the course carried out individually or in pairs.	30	
Report of practices, practicum and external practices	Reports on the practices corresponding to the first half of the course carried out individually or in pairs.	30	

Other comments on the Evaluation

It is necessary to achieve a minimum of 4.00 in the written exam to pass the subject.

In the practice reports, it will be necessary to indicate if generative AI tools were used and, if so, explicitly state which elements of the report were produced with them. In case of detection of plagiarism or unjustified use of these tools, the professors may grade the deliverable with 0 points.

The grade of the tests/reports will only be valid in the academic year in which they are obtained.

Sources of information

Basic Bibliography

C. Dwork, **The Algorithmic Foundations of Differential Privacy**, Now Publishers Inc., 2013

J. Morris Chang, Di Zhuang, and G. Dumindu Samaraweer, **Privacy-preserving Machine Learning**, Manning Publications, 2023

Mark Craddock, Ed., **UN Handbook on Privacy-Preserving Computation Techniques**, GCATI, 2020

Complementary Bibliography

Katharine Jarmul, **Practical Data Privacy**, O'Reily Media, 2023

Nishant Bhajaria, **Data Privacy**, Manning Publications, 2022

PALISADE, **PALISADE HOMOMORPHIC ENCRYPTION SOFTWARE LIBRARY**,

Ilaria Chillotti, **TFHE Deep Dive**, https://www.zama.ai/post/tfhe-deep-dive-part-1,

Daniele Micciancio, and Oded Regev, **Lattice-based cryptography**, https://cseweb.ucsd.edu/%7Edaniele/papers/PostQuantum.pdf, Springer, 2009

Recommendations