



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	English			
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
Problem and/or exercise solving	0	5	5
Objective questions exam	2	0	2
Report of practices, practicum and external practices	0	2	2

*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
Problem and/or exercise solving	Resolution of questions, problems and exercises throughout the course. Individual delivery in writing.	30	
Objective questions exam	Written exam. Resolution of questions, problems or exercises.	40	
Report of practices, practicum and external practices	Reports on the practices carried out individually or in pairs.	30	

Other comments on the Evaluation

Two alternative evaluation methods in the subject are left to the discretion of the students: continuous evaluation and global evaluation.

The continuous evaluation will consist of the completion of a final exam (40% of the grade), the development of practices and projects (30% of the grade) and the delivery throughout the course and within the established deadlines of resolved exercises (30%).

The single evaluation will consist of a final written exam (70% of the grade) and the development of practices and projects (30%).

The written tests of the global and continuous assessment modalities will not necessarily be the same.

Students will be able to opt for one or another modality of evaluation until the date of the written exam of the course.

Those who do not pass the subject in the ordinary call have a second extraordinary opportunity at the end of the course in which their knowledge will be reassessed with a written test.

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 Samaraweera, **Privacy-preserving Machine Learning**, 9781617298042, Manning Publications, 2023

Mark Craddock, Ed., **UN Handbook on Privacy-Preserving Computation Techniques**, 9781913805272, GCATI, 2020

Complementary Bibliography

Katharine Jarmul, **Practical Data Privacy**, 9781098129460, O'Reilly Media, 2023

Nishant Bhajaria, **Data Privacy**, 9781617298998, Manning Publications, 2022

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

Recommendations

