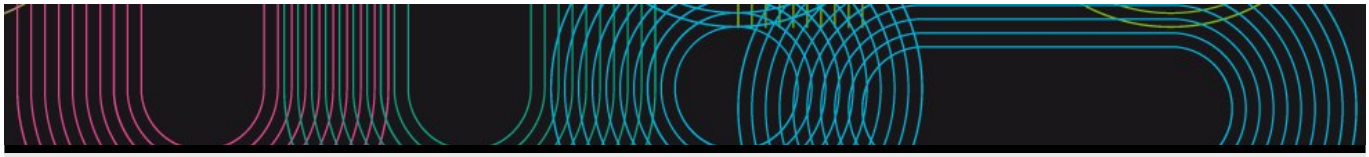

IDENTIFYING DATA				
(*)Seguridade Multimedia				
Subject	(*)Seguridade Multimedia			
Code	V05M145V01318			
Study programme	(*)Máster Universitario en Enxeñaría de Telecomunicación			
Descriptors	ECTS Credits	Choose	Year	Quadmester
	5	Optional	2nd	1st
Teaching language	English			
Department				
Coordinator	Pérez González, Fernando			
Lecturers	Pérez González, Fernando			
E-mail	fperez@gts.uvigo.es			
Web	http://faitic.uvigo.es			
General description	Multimedia security is an increasingly important topic as most of the information exchanged nowadays over the Internet is multimedia. Traditional data protection solutions like cryptography only solve the problem partially, because contents, once decrypted, are no longer protected. In addition, there is a rising concern over the integrity of multimedia contents: modern editing tools jeopardize our trust on video, images or audio. Fortunately, a number of research groups and companies have addressed these problems and ingenious solutions exist. This course presents advanced topics in multimedia security, with emphasis on cryptography, watermarking, forensics and signal processing in the encrypted domain. Teaching and exams are in English.			

Competencies	
Code	
B4	CG4 The capacity for mathematical modeling, calculation and simulation in technological centers and engineering companies, particularly in research, development and innovation tasks in all areas related to Telecommunication Engineering and associated multidisciplinary fields.
B8	CG8 The ability to apply acquired knowledge and to solve problems in new or unfamiliar environments within broader and multidiscipline contexts, being able to integrate knowledge.
C31	CE37/OP7 Ability to model, operate, manage, and deal with the full cycle and bagging of networks, services and applications considering the quality of service, direct and costs of operation, the plan of implementation, monitoring, security, scaling and maintenance, managing and ensuring the quality of the development process

Learning outcomes	
Expected results from this subject	Training and Learning Results
Handle the most advanced information protection methods.	B4 B8 C31
Understand the potential and limitations of the different methods.	B4 B8 C31
Handle the use of different algorithms in current multimedia communications environments.	B4 B8 C31
Understand technical material in an autonomous way.	B4 B8 C31

Contents	
Topic	
Introduction to cryptography.	Application to multimedia systems. Integration with source and channel coding. Block and stream ciphers. Hashing and MAC codes. Specific algorithms.
Conditional access systems.	Requirements. History and state of the art. Design of a conditional access system.
Secret sharing.	Simple secret sharing systems. Visual cryptography.
Data hiding and watermarking.	Basic concepts. Watermarking versus data hiding. Spread-spectrum watermarking. Quantization-based watermarking. Application to images and video.
Forensic signal processing.	Quantization detection and estimation. Filtering detection and identification. Resampling detection and estimation. Source ballistics.
Signal Processing in the Encrypted Domain.	Privacy metrics and notions. Homomorphic encryption. Garbled cicruits. Signal representation and cipher blowup. Applications.

Planning	Class hours	Hours outside the classroom	Total hours
Master Session	14	28	42
Laboratory practises	9	42	51
Reports / memories of practice	0	30	30
Long answer tests and development	2	0	2

*The information in the planning table is for guidance only and does not take into account the heterogeneity of the students.

Methodologies	Description
Master Session	The course is structured in several topics in multimedia security, including cryptography, watermarking, forensics and signal processing in the encrypted domain. Competences: CG4, CG8, CE31
Laboratory practises	Lab practices will cover different aspects of multiple-input data hiding, watermarking and forensics. This will allow students to practically implement and considerably expand some of the concepts seen in the lectures. Competences: CG4, CG8, CE31

Personalized attention	
Methodologies	**Description**
Master Session	Students will have the opportunity to meet in person with the instructor at some office hours that will be announced at the beginning of the course. The schedule will published in the course webpage.
Tests	**Description**
Reports / memories of practice	Students will have the opportunity to meet in person with the instructor at some office hours that will be announced at the beginning of the course. The schedule will published in the course webpage.

Assessment	Description	Qualification	Training and Learning Results

Reports / memories of practice	Reports of the practices and additional personal work that employ the techniques seen in the classroom. Quality of the reports and correctness of the results will be evaluated. Reports will be individual or collective, depending on the size of the unit that carried out the practices.	70	B4 B8	C31
Long answer tests and development	Final exam with short questions on the contents of the subject.	30	B4 B8	C31

Other comments on the Evaluation

A minimum score of 30% with respect to the maximum possible score in the final exam is required to pass the course.

In those cases in which the student decides not to carry out the continuous evaluation tasks, the final score will be solely based on the exam with questions of the subject. This applies as well to the second call.

Once the student turns in any of the deliverables, he/she will be considered to be following the continuous evaluation track. Any student that chooses the continuous evaluation track will get a final score, regardless of he/she takes the final exam.

Continuous evaluation tasks cannot be redone after their corresponding deadlines, and are only valid for the current year.

Sources of information

Cox, Miller, Bloom, Fridrich, Kalker, **Digital Watermarking and Steganography**, 2nd,

Troncoso-Pastoriza, Perez-Gonzalez, **Secure Signal Processing in the Cloud: enabling technologies for privacy-preserving multimedia cloud processing**, Signal Processing Magazine,

A.J. Menezes, **Handbook of Applied Cryptography**, 1996,

A. Piva, **An Overview of Image Forensics**, Signal Processing,

Recommendations

Subjects that it is recommended to have taken before

(*)Procesado Estatístico de Sinal/V05M145V01303