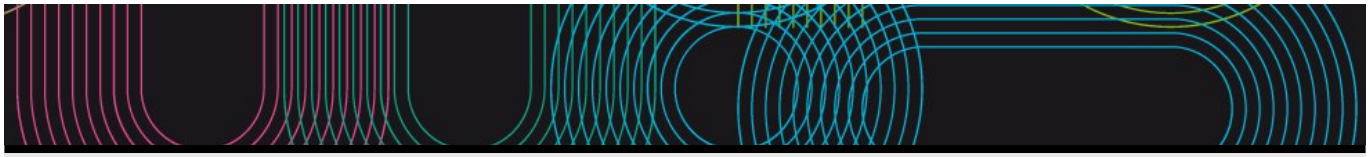
Universidade Vigo

Subject Guide 2018 / 2019



IDENTIFYING DATA				
Information Security				
Subject	Information Security			
Code	V05M175V01102			
Study programme	(*)Máster Universitario en Ciberseguridade			
Descriptors	ECTS Credits	Choose	Year	Quadmester
	6	Mandatory	1st	1st
Teaching language	English			
Department	External Telematics Engineering Signal Theory and Communications			
Coordinator	Fernández Veiga, Manuel			
Lecturers	Fernández Veiga, Manuel Gestal Pose, Marcos Pérez González, Fernando			
E-mail	mveiga@det.uvigo.es			
Web	http://faitic.uvigo.es			
General description	This course covers the fields of cryptography and cryptanalysis, generation of pseudorandom numbers and functions, message integrity, authenticated encryption, public key cryptography, privacy and anonymity in information systems, secure computations, steganography and watermarking.			

Competencies	
Code	
A2	Students will be able to apply their knowledge and their problem-solving ability in new or less familiar situations, within a broader context (or in multi-discipline contexts) related to their field of specialization.
A5	Students will apprehend the learning skills enabling them to study in a style that will be self-driven and autonomous to a large extent.
C1	To know, to understand and to apply the tools of cryptography and cryptanalysis, the tools of integrity, digital identity and the protocols for secure communications.
C4	To understand and to apply the methods and tools of cybersecurity to protect data and computers, communication networks, databases, computer programs and information services.
C10	Knowledge of the mathematical foundations of cryptography. Ability to understand their evolution and future developments.

Learning outcomes	
Expected results from this subject	Training and Learning Results
Understand the theoretical basis of encryption: Shannon ciphers, perfect security, semantic security, information-theoretic security	C1 C10
To know and be able to use stream ciphers	C1 C4 C10
To know and be able to apply block ciphering tools, pseudorandom functions and the DES and AES ciphering standards	C1 C4 C10
Knowledge about the construction, use and properties of hash functions, universal hashing and collision resistant hashing. Knowledge about message authentication codes. Case studies	C1 C4 C10
Knowledge about public key cryptography and PK cryptographic schemes: RSA, ElGamal, Diffie-Hellman. Knowledge about digital signatures. Semantic security of public key cryptography	C1 C4 C10

To know the basics of advanced cryptography: cryptography on elliptic curves. Lattice-based cryptography	A2 A5 C1 C4 C10
To know and be able to use identification protocols, key interchange protocols and interactive communication protocols	A5 C1 C4 C10
To understand and have the ability to apply the basic techniques for steganography, watermarking and digital forensics	A5 C1 C4 C10
To know, understand and be able to use techniques for data anonymization	A2 A5 C1 C4 C10
To know and understand the basic principles of distributed secure computation	A2 A5 C1 C4 C10

Contents

Topic	
1. Encryption	Shannon ciphers. Perfect security. Semantic security. Information-theoretic security: the wiretap channel
2. Stream ciphers	Pseudorandom generators. Composition of PRGs. Security. Attacks. Case studies
3. Block ciphers	Block ciphers. Security. DES & AES. Pseudorandom functions. Construction of PRFs and block ciphers
4. Message integrity	Authentication codes. Message integrity. Definition of security. Keyed MACs. PRFs and MAC. Hashing, hash functions. Universal hashing. Collision resistant hashing. Case studies
5. Authenticated encryption	Definition. Composition. Attacks, examples and case studies
6. Public key cryptography	Definition. Semantic security. One-way trapdoor functions. RSA, ElGamal, McEliece crypto systems. Diffie-Hellman key agreement. Digital signatures. Case studies
7. Advanced cryptography	Elliptic curve cryptography. Lattice-based cryptography. RLWE. Quantum-resistant cryptography. Homomorphic encryption
8. Identification protocols	Definitions. Passwords. Challenge-response. sigma-protocols. Okamoto and Schnorr protocols
9. Anonymization	Definitions. t-integrity and anonymity. Divergence. Analysis
10. Data hiding and steganography	Definitions. Spread-spectrum watermarking. Dirty paper coding. Digital forensics.
11. Secure computation	Computable functions. Fundamental limits. Two-way secure computation. Multiparty secure computation. Interactive communications. Homomorphic computations. Applications

Planning

	Class hours	Hours outside the classroom	Total hours
Problem solving	0	24	24
Laboratory practices	18	36	54
Lecturing	17	51	68
Essay questions exam	2	0	2
Problem solving	1	0	1
Project	1	0	1

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

Methodologies

	Description

Problem solving	Students are supposed to solve problems and exercises about the curse contents. Written homework, with review and grading. This methodology develops the competences CB2, CB4, CB5, CE1, CE44, CE10 and CT5.
Laboratory practices	Students are expected to work in the computer laboratory doing small programs on ciphering, and a programming assignment on ciphering, authentication, anonymity or digital forensics. The programming assignment will be supervised by the instructors. This methodology develops the competences CB2, CB4, CB5, CE1, CE44, CE10 and CT4.
Lecturing	Lectures on the topics included in the course: definitions, concepts, main results, properties and applications. This methodology develops the competences CB2, CB4, CB5, CE1, CE44, CE10 and CT5.

Personalized attention

Methodologies	Description
Lecturing	Individual office hours will be offered to the students who need guidance in the study, or further explanations on the course contents, clarification on the solutions to problems, etc.
Problem solving	Individual office hours will be offered to answer the questions about problems and exercises assigned to the students
Laboratory practices	Individual assistance will be given to the students who request guidance on the programming assignments or computer lab practice

Assessment

	Description	Qualification	Training and Learning Results	
Essay questions exam	Written exam. Questions, problems or exercises about the contents covered in the course	50	A2 A5	C1 C4 C10
Problem solving	2-3 homework problem sets, to be worked out individually. Written submission	20	A2 A5	C1 C4 C10
Project	Design and development of a programming assignment. Functional and performance tests will be run	30	A2 A5	C1 C4 C10

Other comments on the Evaluation

The student must choose between two alternative, mutually exclusive assessment method: continuous assessment or eventual assessment.

The continuous evaluation option consists in a final written exam (50% of the qualification), the completion of programming assignments (30% of the qualification) and homework (20%). These assignments will be due the last working day preceding the start of the examination period. The eventual assessment option consists in a final written exam (60% of the qualification) and in the completion of assignments (40% of the qualification). The assignments will be due the last working day preceding the start of the examination period. The examinations of the continuous and the eventual assessment options may not be equal.

The students can declare their preferred assessment type until the date of the written examination.

The students who fail the course will be given a second opportunity at the end of the academic year to do so. Their academic achievements will be re-evaluated, both with a written exam (theoretical knowledge) and a review of their engineering project looking for improvement or changes. The weights are the same they were committed to, according to their choice.

Any assigned grade will only be valid during the academic year where it is awarded.

Sources of information

Basic Bibliography

D. Boneh, V. Shoup, **A graduate course in applied cryptography**, http://toc.cryptobook.us, 2018

Complementary Bibliography

O. Goldreich, **Foundation of cryptography, vol. I**, Cambridge University Press, 2007

O. Goldreich, **Foundation of cryptography, vol. ii**, Cambridge University Press, 2009

J. Katz, Y. Lindell, **Introduction to modern cryptography**, 2, CRC Press, 2015

A. Menezes, P. van Oorschot, S. Vanstone., **Handbook of applied cryptography**, CRC Press, 2001
C. Dwork, A. Roth, **The algorithmic foundations of differential privacy**, NOW Publishers, 2014
W. Mazurczyk, S. Wenzel, S. Zander, A. Houmansadr, K. Szczypiorski, **Information hiding in communications networks: Fundamentals, mechanisms, applications, and countermeasures**, Wiley, 2016
I. Cox, M. Miller, J. Bloom, J. Fridrich, T. Kolker, **Digital watermarking and steganography**, 2, Morgan Kaufmann, 2008
A. El-Gamal, Y. Kim, **Network Information Theory**, Cambridge University Press, 2011

Recommendations

Other comments

The course is given in English. Ability for mathematical reasoning is highly recommended.