IDENTIFYING DATA

Information Security

Subject	Information Security			
Code	V05M175V11108			
Study programme	Máster Universitario en Ciberseguridad			
Descriptors	ECTS Credits	Choose	Year	Quadmester
	5	Mandatory	1st	1st
Teaching language	English			
Department				
Coordinator	Fernández Veiga, Manuel			
Lecturers	Fernández Veiga, Manuel Gestal Pose, Marcos Pérez González, Fernando			
E-mail	mveiga@det.uvigo.es			
Web	http://moovi.gal			
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.			

Training and Learning Results

Code

Expected results from this subject

Expected results from this subject	Training and Learning Results

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. Quantumresistant 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 practical	18	36	54
Lecturing	17	51	68
Essay questions exam	2	0	2
Problem and/or exercise solving	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
Problem solving	Students are supposed to solve problems and exercises about the curse contents. Written homework, with review and grading.
Laboratory practical	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.
Lecturing	Lectures on the topics included in the course: definitions, concepts, main results, properties and applications.

Personalized assistance

Methodologies	Description
Problem solving	Individual office hours will be offered to answer the questions about problems and exercises assigned to the students. https://www.uvigo.gal/es/universidad/administracion-personal/pdi/manuel-fernandez-veiga
Laboratory practical	Individual assistance will be given to the students who request guidance on the programming assignments or computer lab practice. https://www.uvigo.gal/es/universidad/administracion-personal/pdi/manuel-fernandez-veiga
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. https://www.uvigo.gal/es/universidad/administracion-personal/pdi/manuel-fernandez-veiga

Assessment

	Description	Qualification	Training and Learning Results
Problem solving	4 homework problem sets, to be worked out individually. Written submission	30	
Laboratory practical	Design and development of programming assignments. Functional and performance tests will be run	30	
Essay questions exam	Written exam. Questions, problems or exercises about the contents covered in the course	40	

Other comments on the Evaluation

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

global assessment.

The continuous evaluation option consists in a final written exam (40% of the qualification), the completion of programming

assignments (30% of the qualification) and homework (30%). The global assessment option consists in a final written exam (40% of the

qualification) and in the completion of assignments (two, 30% of the qualification each one). 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 an extraordinary 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, 2021

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**, 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.