ANX-PR/CL/001-01

LEARNING GUIDE

SUBJECT

103000810 - Design And Analysis Of Security Protocols

DEGREE PROGRAMME

10AR - Master Interuniversitario En Métodos Formales En Ingeniería Informática

ACADEMIC YEAR & SEMESTER

2023/24 - Semester 1

Index

Learning guide

1. Description

1.1. Subject details

Name of the subject	103000810 - Design And Analysis Of Security Protocols
No of credits	6 ECTS
Type	Optional
Academic year ot the programme	First year
Semester of tuition	Semester 1
Tuition period	September-January
Tuition languages	English
Degree programme	10AR - Master Interuniversitario en Métodos Formales en Ingeniería Informática
Centre	10 - Escuela Tecnica Superior De Ingenieros Informaticos
Academic year	2023-24

2. Faculty

2.1. Faculty members with subject teaching role

Name and surname	Office/Room	Email	Tutoring hours *
Manuel Carro Liñares (Subject coordinator)		manuel.carro@upm.es	F - 13:00 - 19:00 Please contact the instructor before making an appointment.
Guillermo Roman Diez		guillermo.roman@upm.es	M - 12:00 - 15:00 W - 08:00 - 08:15 Please contact the instructor for an appointment

* The tutoring schedule is indicative and subject to possible changes. Please check tutoring times with the faculty member in charge.

2.3. External faculty

Name and surname	Email	Institution
Pedro Moreno	pedro.moreno@imdea.org	IMDEA Software Institute
Dario Fiore	Dario.Fiore@imdea.org	IMDEA Software Institute
Ignacio Cascudo	ignacio.cascudo@imdea.org	IMDEA Software Institute

3. Skills and learning outcomes *

3.1. Skills to be learned

CB06 - Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y/o aplicación de ideas, a menudo en un contexto de investigación

CE06 - Capacidad para utilizar modelos de cómputo alternativos a los convencionales, tales como la computación cuántica, los sistemas de reescritura, las máquinas abstractas, la programación con restricciones o los algoritmos bio-inspirados.

CE07 - Capacidad para aplicar técnicas matemáticas a problemas informáticos relevantes, tales como el diseño de protocolos criptográficos seguros, la construcción de modelos formales del software, o el diseño de sistemas que aprenden automáticamente durante su ejecución.

CG05 - Capacidad para la aplicación de los conocimientos adquiridos para resolver problemas en entornos nuevos o poco conocidos dentro de contextos amplios y multidisciplinares, siendo capaces de integrar dichos conocimientos.

CT03 - Capacidad de razonamiento crítico como vía para mejorar la generación y desarrollo de ideas en un contexto profesional o de investigación.

CT04 - Capacidad para la búsqueda, análisis y síntesis de información.

3.2. Learning outcomes

RA21 - Ability to select the cryptographic method best suited for an application

RA23 - Ability to evaluate communication protocols

RA22 - Ability to design encryption communication protocols

RA24 - Ability to implement security protocols and services

RA16 - Knowledge of cryptography fundamentals

RA17 - Acquaintance with multi-party computation and its range of applications

RA18 - Blockchain technologies

* The Learning Guides should reflect the Skills and Learning Outcomes in the same way as indicated in the Degree Verification Memory. For this reason, they have not been translated into English and appear in Spanish.

4. Brief description of the subject and syllabus

4.1. Brief description of the subject

The goal of this course is to introduce basic notions of cryptographic protocols under a formal perspective, which makes emphasis on precise security definitions and rigorous proofs of security based on well delimited assumptions. We will explain the difference between symmetric and public key cryptography, their use cases, and present some of the best known and used encryption and authentication schemes. Finally, we will introduce some more advanced cryptographic protocols related to secure computing, such as zero knowledge proofs and secure multiparty computation, and their application to real world scenarios such as blockchain technologies.

4.2. Syllabus

1. Perfect security and computational security
    1.1. Notion of encryption, one-time pad
    1.2. Notions of security
    1.3. One-way functions and one way trapdoor functions, mathematical examples
    1.4. IND-CPA security
2. Pseudorandomness and symmetric-key cryptography:
    2.1. Hardcore predicates for one-way functions
    2.2. Pseudorandom generators and pseudorandom functions
    2.3. Message authentication codes
    2.4. Symmetric key encryption
    2.5. Modes of operation
3. Public key cryptography:
    3.1. Key Exchange
    3.2. Public key encryption
    3.3. El Gamal encryption
    3.4. RSA encryption
    3.5. Digital signatures
4. Advanced protocols
    4.1. Zero knowledge proofs
    4.2. Secret sharing
    4.3. Secure multiparty computation
5. Applications in real world scenarios
    5.1. Blockchain technologies

5. Schedule

5.1. Subject schedule*

Week	Classroom activities	Laboratory activities	Distant / On-line	Assessment activities
1	**Perfect security and computational security** Duration: 02:00 Lecture **Perfect Security and Computational Security** Duration: 01:00 Problem-solving class			
2	**Perfect security and computational security** Duration: 02:00 Lecture **Perfect Security and Computational Security** Duration: 01:00 Problem-solving class			
3	**Pseudorandomness and symmetric-key cryptography** Duration: 02:00 Lecture **Pseudorandomness and symmetric-key cryptography** Duration: 01:00 Problem-solving class			
4	**Pseudorandomness and symmetric-key cryptography** Duration: 02:00 Lecture **Pseudorandomness and symmetric-key cryptography** Duration: 01:00 Problem-solving class			**Individual homework: Practical problems on perfect security and computational security; and pseudorandomness and symmetric-key cryptography** Individual work Continuous assessment Not Presential Duration: 04:00
5	**Pseudorandomness and symmetric-key cryptography** Duration: 02:00 Lecture **Pseudorandomness and symmetric-key cryptography** Duration: 01:00 Problem-solving class			

6	**Pseudorandomness and symmetric-key cryptography** Duration: 02:00 Lecture **Pseudorandomness and symmetric-key cryptography** Duration: 01:00 Problem-solving class			
7	**Public key cryptography** Duration: 02:00 Lecture **Public key cryptography** Duration: 01:00 Problem-solving class			
8	**Public key cryptography** Duration: 02:00 Lecture **Public key cryptography** Duration: 01:00 Problem-solving class			
9	**Public key cryptography** Duration: 02:00 Lecture **Public key cryptography** Duration: 01:00 Problem-solving class			**Individual homework: Practical problems on public key cryptography** Individual work Continuous assessment Not Presential Duration: 04:00
10	**Public key cryptography** Duration: 02:00 Lecture **Public key cryptography** Duration: 01:00 Problem-solving class			
11	**Advanced protocols** Duration: 02:00 Lecture **Advanced protocols** Duration: 01:00 Problem-solving class			
12	**Advanced protocols** Duration: 02:00 Lecture **Advanced protocols** Duration: 01:00 Problem-solving class			
13	**Advanced protocols** Duration: 02:00 Lecture **Advanced protocols** Duration: 01:00 Problem-solving class			

14	**Advanced protocols** Duration: 02:00 Lecture **Advanced protocols** Duration: 01:00 Problem-solving class			**Individual homework: Practical problems on advanced protocols** Individual work Continuous assessment Not Presential Duration: 04:00
15	**Applications in real world scenarios** Duration: 02:00 Lecture **Applications in real world scenarios** Duration: 01:00 Problem-solving class			
16				
17				**Global exam** Written test Continuous assessment Presential Duration: 02:00 **Comprehensive exam** Written test Final examination Presential Duration: 02:00

Depending on the programme study plan, total values will be calculated according to the ECTS credit unit as 26/27 hours of student face-to-face contact and independent study time.

* The schedule is based on an a priori planning of the subject; it might be modified during the academic year, especially considering the COVID19 evolution.

6. Activities and assessment criteria

6.1. Assessment activities

6.1.1. Assessment

Week	Description	Modality	Type	Duration	Weight	Minimum grade	Evaluated skills
4	Individual homework: Practical problems on perfect security and computational security; and pseudorandomness and symmetric-key cryptography	Individual work	No Presential	04:00	13.3%	2 / 10	CB06 CG05 CT03 CT04 CE06 CE07
9	Individual homework: Practical problems on public key cryptography	Individual work	No Presential	04:00	13.3%	2 / 10	CB06 CG05 CT03 CT04 CE06 CE07
14	Individual homework: Practical problems on advanced protocols	Individual work	No Presential	04:00	13.3%	2 / 10	CB06 CG05 CT03 CT04 CE06 CE07
17	Global exam	Written test	Face-to-face	02:00	60.1%	5 / 10	CB06 CG05 CT03 CT04 CE06 CE07

6.1.2. Global examination

Week	Description	Modality	Type	Duration	Weight	Minimum grade	Evaluated skills
17	Comprehensive exam	Written test	Face-to-face	02:00	100%	5 / 10	CB06 CG05 CT03 CT04 CE06 CE07

6.1.3. Referred (re-sit) examination

Description	Modality	Type	Duration	Weight	Minimum grade	Evaluated skills
Global exam	Written test	Face-to-face	02:00	100%	5 / 10	CB06 CG05 CT03 CT04 CE06 CE07

6.2. Assessment criteria

- The assessment method will be weighted as follows: assignments to be developed during the course period at home or in class will constitute 40% of the final grade. The in-class final exam will constitute 60% of the final grade.
- Copying from any source (either textbooks, the Internet, another student, or any other source) with or without the permission of the author of the source, as well as other types of academic fraud, can lead to a 'fail' grade in the course and / or being reported to the academic authorities, who will decide whether to take additional authoritative measures. In particular, in case of non-ethical or fraudulent behavior, the Law 3/2022 of February 24th will be applied, as well as the corresponding UPM regulations. Article 12 and 14 of Law 3/2022 states that a serious fault may mean, among other outcomes, failing the corresponding sitting.
- There are no learning blocks whose earned grades can be carried over to future academic courses.
- Failure to deliver the homework at the time and in the form stated by the instructor(s) may result in a failure for that exercise.

7. Teaching resources

7.1. Teaching resources for the subject

Name	Type	Notes
Goldwasser, S; Bellare, M (1996) Lecture Notes on Cryptography	Bibliography	
Boneh, D; Shoup, V (2020) A Graduate Course in Applied Cryptography	Web resource	
Katz, J; Lindell, Y (2008) Introduction to Modern Cryptography	Bibliography	
Barak, B (2021)An Intensive Introduction to Cryptography	Web resource	
Rosulek, M (2021)The Joy of Cryptography	Web resource	