ANX-PR/CL/001-01

LEARNING GUIDE

SUBJECT

615000244 Information Security

DEGREE PROGRAMME

61IW – Degree in Software Engineering

ACADEMIC YEAR & SEMESTER

2022/23 - Semester 2

Index

Learning guide

1. Description

1.1. Subject details

Name of the subject	615000244- Information Security
No of credits	6 ECTS
Type	Mandatory
Academic year ot the programme	Second year
Semester of tuition	Semester 4
Tuition period	February - June
Tuition languages	English
Degree programme	61IW – Software Engineering Bachelor
Centre	61 - Escuela Tecnica Superior De Ingenieria De Sistemas Informaticos
Academic year	2022-23

2. Faculty

2.1. Faculty members with subject teaching role

Name and surname	Office/Room	Email	Tutoring hours *
Gianni Scarpa (Subject coordinator)	4304	g.scarpa@upm.es	To be confirmed.

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

3. Prior knowledge recommended to take the subject

3.1. Recommended (passed) subjects

- SecurityFundamentals
- Algebra
- Logic and Discrete Mathematics

3.2. Other recommended learning outcomes

4. Skills and learning outcomes *

4.1. Competences

- CC1 - Ability to design, develop, select, and evaluate computer applications and systems, ensuring their reliability, security, and quality, in accordance with ethical principles and current legislation and regulations.
- CT8 - Teamwork: Being able to work as a member of an interdisciplinary team with the aim of contributing to the development of projects with pragmatism and a sense of responsibility, taking into account the available resources.

4.2. .Learning outcomes

- RA86 - Develops Information Security Management Systems (ISMS) according to international standards and norms.
- RA334 - Analyzes and applies the RSA algorithm for data encryption and decryption.
- RA337 - Familiar with the Digital Signature Algorithm (DSA).
- RA200 - Understands authentication methods and mechanisms, as well as the utility of digital certificates.
- RA198 - Analyzes and applies the RSA algorithm for digital signatures.
- RA199 - Understands and calculates the NNC (Necessary Numeric Complexity) and CP (Computational Power) in the use of the RSA encryption algorithm and performs various attacks on the system.
- RA143 - Familiar with and applies mathematical methods and algorithms used in cryptographic implementations.
- RA118 - Able to work as a team member to contribute to project development with pragmatism and a sense of responsibility, assuming commitments and considering available resources. Able to generate trust and credibility among collaborators and committed to achieving the corporate vision through negotiation and motivation, rather than coercion and individualism.
- RA197 - Compares symmetric encryption systems with asymmetric encryption systems and is capable of applying the appropriate algorithms to each situation.
- RA85 - Understands and applies information protection schemes based on the application of techniques.

5. Brief description of the subject and syllabus

In this subject, the protection of information using asymmetric cryptography techniques, digital signatures, and digital certificates is studied. It also introduces the phases and implementation of an Information Security Management System (ISMS).

Syllabus

1.. Asymmetric or Public Key Cryptography

1.1. Introduction

1.2. Advantages and disadvantages of asymmetric encryption compared to symmetric encryption

1.3. Diffie-Hellman Key Exchange

1.4. Extended Euclidean Algorithm for inverse calculation

1.5. Fast Exponentiation Algorithm for encryption

2. Principles of the RSA algorithm

2.1. Principles

2.2. Parameters and key generation

2.3. Encryption and decryption

2.4. Block ciphering of text

3. Characteristics of keys and cipher elements in RSA

3.1. Paired private keys

3.2. Paired public keys

3.3. Non-encryptable numbers

4. Attacks on RSA

4.1. Factorization-based attack on the modulus n

4.2. Cyclic encryption attack with the public key

4.3. Birthday paradox attack

4.4. Side-channel attacks

5. Elliptic Curves

5.1. Definition of continuous and discrete elliptic curves

5.2. Cryptography based on elliptic curves

5.3. Diffie-Hellman Key Exchange with elliptic curves

6. Hash Functions

6.1. Characteristics and properties of hash functions

6.2. MD5, SHA-1, and SHA-2 hash functions

6.3. Introduction to SHA-3

6.4. Birthday paradox attack on hash functions

7. Digital Signature Algorithms

7.1. RSA Digital Signature

7.2. DSA Standard Signature

8. Authentication Systems and Digital Certificates

8.1. Authentication mechanisms and methods

8.2. Introduction to digital certificates

8.3. Concept of a Certification Authority

8.4. Algorithms and characteristics of an X.509 digital certificate

9. Information Security Management System (ISMS)

9.1. Introduction to security policies and plans

9.2. Implementation of an ISMS

9.3. Phases of an ISMS

6. Schedule

6.1. Subject schedule*

Week	Classroom activities	Laboratory activities	Distant / On-line	Assessment activities
1	**Theoretical lesson** Lecture			
2	**Theoretical lesson** Lecture			
3		**Practical lesson** Duration: 02:00		Progressive Evaluation of Block I of the syllabus. EX: Written Exam Technique Continuous evaluation Face to face Duration: 00:30
4	**Theoretical lesson** Lecture			
5	**Theoretical lesson** Lecture			
6		**Practical lesson** Duration: 02:00		Progressive Evaluation of Block II of the syllabus. EX: Written Exam Technique Continuous evaluation Face to face Duration: 00:30
7	**Theoretical lesson** Lecture			
8	**Theoretical lesson** Lecture			

Week	Classroom activities	Laboratory activities	Distant / On-line	Assessment activities
9		**Practical lesson** Duration: 02:00		Progressive Evaluation of Block III of the syllabus. EX: Written Exam Technique Continuous evaluation Face to face Duration: 00:30
10	**Theoretical lesson** Lecture			
11	**Theoretical lesson** Lecture			
12		**Practical lesson** Duration: 02:00		Progressive Evaluation of Block IV of the syllabus. EX: Written Exam Technique Continuous evaluation Face to face Duration: 00:30
13	**Theoretical lesson** Lecture			Activities of the transversal competence: TG: Technique of Group Work Continuous evaluation with only a final test Non-presential Duration: 00:00
14	**Theoretical lesson** Lecture			
15		**Practical lesson** Duration: 02:00		
16				Progressive Evaluation of Block V of the syllabus: EX: Technique of Written Exam Continuous evaluation with only a final test In-person Duration: 00:30 Recovery Exam for Block I of the syllabus: EX: Technique of Written Exam Evaluation based only on the final test In-person Duration: 00:30 Recovery Exam for Block II of the syllabus: EX: Technique of Written Exam Evaluation based only on the final test In-person Duration: 00:30 Recovery Exam for Block III of the syllabus: EX: Technique of Written Exam Evaluation based only on the final test In-person Duration: 00:30 Recovery Exam for Block IV of the syllabus: EX: Technique of Written Exam Evaluation based only on the final test In-person Duration: 00:30

7. Activities and assessment criteria

7.1. Assessment activities

7.1.1. Assessment for progressive attendance

Week	Description	Modality	Type	Duration	Weight	Minimum grade	Evaluated skills
3	: Progressive Evaluation of Block I of the syllabus. :	Written exam	Face to face	00:30	18%	4/10	CC1
6	Progressive Evaluation of Block II of the syllabus.	Written exam	Face to face	00:30	18%	4/10	CC1
9	Progressive Evaluation of Block III of the syllabus.	Written exam	Face to face	00:30	18%	4/10	CC1
12	Progressive Evaluation of Block IV of the syllabus.	Written exam	Face to face	00:30	18%	4/10	CC1
13	Activities of the Transversal Competence.	Teamwork	Non-presential	00:00	10%	0 / 10	CT8
17	Progressive Evaluation of Block V of the syllabus.	Written exam	Face to face	00:30	18%	4/10	CC1

7.1.2. Global examination

Week	Description	Modality	Type	Duration	Weight	Minimum grade	Evaluated skills
13	: Progressive Evaluation of Block I of the syllabus. :	Written exam	Face to face	00:30	18%	4/10	CC1
17	Progressive Evaluation of Block II of the syllabus.	Written exam	Face to face	00:30	18%	4/10	CC1
17	Progressive Evaluation of Block III of the syllabus.	Written exam	Face to face	00:30	18%	4/10	CC1
17	Progressive Evaluation of Block IV of the syllabus.	Written exam	Face to face	00:30	18%	4/10	CC1
17	Activities of the Transversal Competence.	Teamwork	Non-presential	00:00	10%	0 / 10	CT8
17	Progressive Evaluation of Block V of the syllabus.	Written exam	Face to face	00:30	18%	4/10	CC1

7.1.3. Referred (re-sit) examination

Description	Modality	Type	Duration	Weight	Minimum grade	Evaluated skills
"Final exam" covering the entire content of the subject, "only final test.	Written exam	Face to face	02:30	90%	0/ 10	

7.2. Assessment criteria

1. ASSESSMENT CRITERIA

According to the regulations governing the assessment of learning in official undergraduate and master's degree programs at Universidad Politécnica de Madrid, approved by the Governing Council in its session on May 26, 2022, the evaluation system that contributes to promoting student learning and the achievement of learning outcomes and the acquisition of corresponding competencies is the distributed or progressive evaluation system.

The subject consists of six distinct parts:
- Transversal Competence: Mandatory participation activity for students, which cannot be recovered.
- Thematic Blocks I - V: Evaluation activity for students, which can be recovered (evaluated during the teaching period).

However, under certain circumstances, as indicated in the following sections, students will be able to recover part of the subject (Thematic Blocks I - V) through the global evaluation system.

2. CRITERIA FOR GRADING.

2.1. ORDINARY ASSESSMENT PERIOD.

2.1.1 DISTRIBUTED OR PROGRESSIVE EVALUATION.
The assessment instruments to be used in the evaluation of student learning process in the progressive evaluation are detailed below:
Evaluation Technique: TG: Group Work Technique (Transversal Competence. Mandatory activity for students to be completed on time. Not recoverable)
Description: Carrying out activities related to the "Teamwork" competence.
Weight: 10%
Date: Week 13 of the teaching period
Evaluated Learning Outcomes: The student is capable of working as a member of a team with the aim of contributing to the development of projects with pragmatism and a sense of responsibility, taking into account the available resources. The student demonstrates the ability to generate trust and credibility among a group of collaborators, as well as commitment to achieving the corporate vision through negotiations and motivations, rather than in a coercive and individualistic manner.

Evaluation Technique: EX: Written Exam Technique
Description: Thematic Block I Exam (Passing grade is >= 4)
Weight: 18%
Date: Week 3
Evaluated Learning Outcomes: Compares symmetric encryption systems with asymmetric encryption systems and is capable of applying the appropriate algorithms to each situation. Knows and applies information protection schemes based on the application of cryptographic techniques. Knows and applies mathematical methods and algorithms that will be used in cryptographic implementations.

Thematic topics covered in Block I: Topic 1
Evaluation Technique: EX: Written Exam Technique
Description: Thematic Block II Exam (Passing grade is >= 4)
Weight: 18%
Date: Week 6

Evaluated Learning Outcomes: Analyzes and applies the RSA algorithm for data encryption and decryption. Knows and calculates NNC (Non-Cipherable Numbers) and CP (Coprime Numbers) in the use of the RSA encryption algorithm.
Thematic topics covered in Block II: Topics 2 and 3.

Evaluation Technique: EX: Written Exam Technique
Description: Thematic Block III Exam (Passing grade is >= 4)
Weight: 18%
Date: Week 9
Evaluated Learning Outcomes: Knows and performs different attacks on the RSA system. Understands the definition of Elliptic Curves and their applications in cryptography.
Thematic topics covered in Block III: Topics 4 and 5.

Evaluation Technique: EX: Written Exam Technique
Description: Thematic Block IV Exam (Passing grade is >= 4)
Weight: 18%
Date: Week 12
Evaluated Learning Outcomes: Analyzes and applies the RSA algorithm for digital signatures. Knows the DSA digital signature. Understands and analyzes the functioning of MD5 and SHA-1 hash functions, applying the algorithms. Knows authentication methods and mechanisms, as well as the utility of digital certificates.
Thematic topics covered in Block IV: Topics 6, 7, and 8.

Evaluation Technique: EX: Written Exam Technique
Description: Thematic Block V Exam.
Peso: 18%
Fecha: Date specified by the Subdirectorate of Academic Affairs and Postgraduate Studies. (Week 17)
Evaluated Learning Outcomes: Develops Information Security Management Systems (ISMS) according to international standards and norms.
Thematic topics covered in Block V: Topic 9.

To pass the subject, a grade equal to or higher than 5 must be obtained once the previous activities have been evaluated. To pass the transversal competence, all proposed activities for it must be completed and a grade of "APTO" obtained. The numerical grade to be added to the subject grade will be determined by the evaluation criteria established in the course syllabus.

Por the evaluation of one or several of the proposed activities.
2.1.2. GLOBAL EVALUATION
Students who have not obtained a grade higher than 4 in the evaluation of some of the thematic blocks I to IV will have the possibility to be examined in the same subject through a written exam, in addition to being examined in Block V. The grade obtained in the evaluation of the transversal competence will be added to the exam grade.

Evaluation technique: TG: Group Work Technique (Transversal Competence. Mandatory activity for students in a timely manner. Not recoverable)
Description: Carrying out activities related to the "Teamwork" competence.
Weight: 10%
Date: Week 13 of the teaching period
Evaluated learning outcomes: Ability to work as a team member in order to contribute to the development of projects with pragmatism and a sense of responsibility, assuming commitments and considering available resources. Ability to generate trust and credibility in a group of collaborators, as well as commitment to the corporate vision through negotiations and motivations, avoiding a coercive and individualistic approach.

Evaluation technique: EX: Written Exam Technique
Description: Block I Thematic Exam (Recovery)
Weight: 18%
Date: Date indicated by the Subdirectorate of Academic Organization and Postgraduate Studies.
Evaluated learning outcomes: Compares symmetric and asymmetric encryption systems and is able to apply the appropriate algorithms to each situation. Knows and applies information protection schemes based on cryptographic techniques. Knows and applies mathematical methods and algorithms used in cryptographic implementations.

Topics belonging to Block I: Topic 1
Evaluation technique: EX: Written Exam Technique
Description: Block II Thematic Exam (Recovery)
Weight: 18%
Date: Date indicated by the Subdirectorate of Academic Organization and Postgraduate Studies.
Evaluated learning outcomes: Analyzes and applies the RSA algorithm for data encryption and decryption. Knows and calculates the NNC and CP in the use of the RSA encryption algorithm.

Topics belonging to Block II: Topics 2 and 3
Evaluation technique: EX: Written Exam Technique
Description: Block III Thematic Exam (Recovery)
Weight: 18%
Date: Date indicated by the Subdirectorate of Academic Organization and Postgraduate Studies.
Evaluated learning outcomes: Knows and performs different attacks on the RSA system. Knows the definition of Elliptic Curves and their applications in cryptography.
Topics belonging to Block III: Topics 4 and 5
Evaluation technique: EX: Written Exam Technique
Description: Block IV Thematic Exam (Recovery)
Weight: 18%
Date: Date indicated by the Subdirectorate of Academic Organization and Postgraduate Studies.
Evaluated learning outcomes: Analyzes and applies the RSA algorithm for digital signatures. Knows the DSA digital signature. Understands and analyzes the operation of MD5 and SHA-1 hash functions, applying the algorithms. Knows authentication methods and mechanisms, as well as the utility of digital certificates.
Topics belonging to Block IV: Topics 6, 7, and 8

Assessment technique: EX: Written Examination Technique
Description: Examination Subject Block V.
Weight: 18% Weight: 18% Weight: 18% Weight: 18% Weight: 18% Weight: 18% Weight: 18
Date: Date indicated by the Subdirección de Ordenación Académica y de Postgrado.
Assessed learning outcomes: Develops ISMS information security management systems according to international standards and norms,
according to international standards and norms.
Topics that belong to Block V: Topic 9.
In order to pass the subject a grade equal or higher than 5 is required once the previous activities have been evaluated.
previous activities.

2.2. EXTRAORDINARY EXAM.

All students who have not passed the subject in the ordinary exam will have the possibility of take a final written exam with 9 points. The mark obtained in the evaluation of the transversal competency in the evaluation of the transversal competence in the teaching period will be added to the mark obtained in the exam.
Assessment technique: GC: Group Work Technique (Transversal Competence). Compulsory activity for the students in due time and form. Not recoverable)
Description: Performance of activities related to the competence "Teamwork".

Weight: 10% Weight: 10% Weight: 10% Weight: 10% Weight: 10% Weight: 10% Weight: 10% Weight: 10%
Date: Week 13 of the teaching period
Assessed learning outcomes: Is able to work as a member of a team in order to contribute to the development of projects with pragmatism and a sense of responsibility.
contribute to the development of projects with pragmatism and a sense of responsibility, making commitments and taking into account the resources available. Is able to work in a way that builds trust and credibility in a group of collaborators, in addition to
in a group of collaborators, in addition to the commitment to the achievement of the corporate vision through negotiations and motivations, and not in a coercive and individualistic way.

Evaluative technique: EX: Written Examination type technique.
Description: Evaluation of topics from 1 to 9
Weight: 90%.
Date: Date provided by Sub. Academic Ord.
Assessed learning outcomes: Compares symmetric and asymmetric cipher systems and is able to apply the appropriate algorithms to each situation.

The student is able to apply the appropriate algorithms to each situation. Knows and applies information protection schemes based on the application of cryptographic techniques.
Knows and applies information protection schemes based on the application of cryptographic techniques. Knows and applies mathematical methods and algorithms mathematical methods and algorithms to be used in cryptographic implementations. Analyses and applies the RSA algorithm for encryption and decryption of data. Knows and calculates NNCs and CPs in the use of the RSA encryption algorithm.
Knows and performs different attacks on the RSA system. Knows the definition of Elliptic Curves and their applications in cryptography.
Analyses and applies the RSA algorithm for digital signature. Knows the DSA digital signature. Knows and Analyses the functioning of MD5 and SHA-1 hash functions, applying the algorithms. Knows forms and authentication mechanisms as well as the usefulness of digital certificates. Develops information security management Develops ISMS information security management systems, according to international standards and norms.

7.3. Teaching resources for the subject

Name	Type	Notes
Moodle UPM	Web resource	The whole pack of documentation and examples used in class by the teacher. It is documentation elaborated by the teacher
Security Fundamentals Volume II	Bibliography	Main book.
Security Fundamentals Volume I	Bibliography	Main book
Information Security. Networking, computing and information systems. Areitio, Javier. Paraninfo, 2008	Bibliography	Complementary book
Digital Cryptography. Pastor, José; Sarasa, Miguel Angel. Collection Textos Docentes; Prensas University Presses of Zaragoza	Bibliography	Complementary book.
Cryptography and Network Security. Stallings, William. Pearson, 2020	Bibliography	Complementary book.

8. Other information

Dealing with fraudulent behaviour (Article 13)
Examinations shall be conducted on a personal level. If cheating is detected in an assessment test, a mark of zero will be awarded to the student(s) involved (the rule applies equally to those who copy and those who leave copies, it is the student's responsibility to protect their own information) in the final grade of the corresponding exam session (ordinary or extraordinary).
In addition, depending on the seriousness of the case, the subject's Tribunal may decide to hold special and equivalent exam to assess the learning outcomes of the subject in the following official exam session. If academic fraud is detected during the course of the examination,the test may be interrupted immediately for the student(s) involved, and the lecturer must communicate the reason for the interruption to the student(s).
The lecturer must communicate the reason for the interruption. The Subject Tribunal may bring the facts to the attention of the Director of the Department, who in turn may bring them to the attention of the Rector so that a case can be disciplinary proceedings may be opened, if appropriate.

Publication of the solutions (Article 19. Point 9)
In all assessment tests, unless the type of test does not allow it, the solutions to the questions of the test shall be made public within two working days of the end of the test by all the candidates.
The solutions to the questions will be made public within two working days of the end of the test for all the students who have to take the test, on the Moodle platform of the subject, and must remain published for seven working days or until the end of the date scheduled for the revision.

Students who are unable to take an assessment test on the scheduled date (Article 21)
When a student, prior to an assessment test, knows of a justified cause that prevents him/her from attending the exams on the scheduled date, or is unable to attend an assessment test on the scheduled date of the exams made public at the time, or is unable to attend a scheduled assessment test due to a supervening cause, he/she may request to be examined on a date other than the scheduled date. To do so, you should consult article 21 of the regulations governing the assessment of learning in official bachelor's and master's degrees at the Polytechnic University of Madrid, approved by the Governing Council in its session of 26 May 2022, to check that the cause is justified and submit an application together with the justification:

- In the case of exams outside the official exam period, by e-mail addressed to the subject coordinator, by means of an e-mail addressed to the subject coordinator, who will propose, in agreement with the lecturer in charge, an alternative way of assessing the learning outcomes corresponding to that assessment test.
- In the case of an assessment test during the official examination period of the ordinary or extraordinary or extraordinary exam period that allows the request to be recorded, by means of an e-mail addressed to the Head of Studies, who will communicate to the coordination of the subject the possibility of carrying out another evaluation test.

Bringing forward the extraordinary call (Article 12.4)
Although it is unlikely for this subject, we remind you that, exceptionally, a student can may request to bring forward to the January call the July extraordinary call of the second semester subjects that he/she has pending, provided that semester subjects that are pending, as long as the following requirements are met:

- - That the student is enrolled for all the credits pending in order to complete his/her studies.
- - That, to complete their degree studies, they have a maximum of two subjects left from the 2nd semester, or one subject from the 1st semester and another from the 2nd semester (in addition to the TFG or TFM, if applicable, if not yet defended), in which he/she has been in which you have been enrolled at least once in a previous academic year.