

Degree programme	Type	Course
Computer Engineering	OB	3
Computer Engineering	OP	4

Contact lecturer

Name : Jordi Herrera Joancomarti

Email : jordi.herrera@uab.cat

Teaching staff

Mercè Villanueva Gay

Carlos Garrigues Olivella

Sergi Sánchez Aragón

Group languages

You can consult this information at the [end](#) of the document.

Prerequisites

There are no prerequisites. However, it is recommended that students had previously taken the 'Information and Security' subject.

Objectives

The "Information and Security" course is part of "SUBJECT 29: INFORMATION TECHNOLOGY". The course deals with topics such as coding theory; advanced cryptographic protocols, blockchain technology and cryptocurrencies.

Learning outcomes

1. Apply cost evaluation, time management, resource management and planning techniques in information technology environments.
2. Work independently.
3. Know how to protect access and security in systems that treat information.
4. Identify the applicable standards for the development of information technologies.
5. Know and understand needs in the field of an organisation's ICT.
6. Evaluate and operate a system of distributed communication applications or services.
7. Know about information systems and apply them to meet the needs of organisations.
8. Incorporate distributed information treatment systems in an organisation in order to increase operative

- capacity.
- 9. Prevent and solve problems.
- 10. Develop scientific thought .

Contents

1. The role of the ICT

- ICT in the organization

2. Fundamentals

- Modular Arithmetic
- Polynomials over $GF(2)$

3. Information processing

- Cyclic codes
- CRC and LFSR

4. Advanced cryptography

- Public key cryptography
- Hash functions
- Cryptographic protocols

5. Applications

- Blockchain technology
- Cryptocurrencies: Bitcoins

Learning activities and methodology

Title	Hours	ECTS	Learning outcomes
Theory classes	26	1.04	1, 2, 3, 4, 5, 6, 7, 8, 10
Exercises and practices preparation	25	1	1, 2, 3, 5, 6
Tutoring and consults	17	0.68	1, 2, 3, 5, 7
Exercises classes	12	0.48	2, 3, 7, 9
Final test preparation	25	1	1, 2, 3, 5, 6
Personal work	25	1	1, 2, 3, 5, 6, 9, 10
Mandatory laboratory classes	12	0.48	1, 2, 3, 4, 5, 7, 10

Theory classes will be based on lectures, although students will be encouraged to actively participate in the resolution of examples, etc. During problem sessions, a list of exercises will be resolved. Students are encouraged to solve the problems on their own in advance. Students will be encouraged to present their own solutions in class.

During laboratory sessions, topics related to the theory classes will be studied in depth. E.g., the exposition of real cases, or the extension of certain subjects with techniques and algorithms alternative to those already seen. The Virtual Campus will be used for teachers and student communication (material, news, etc.).

Annotation: within the schedule set by the centre or degree programme, 15 minutes of one class will be reserved for students to evaluate their lecturers and their courses or modules through questionnaires.

Assessment

Continuous assessment activities

Title	Weight	Hours	ECTS	Learning outcomes
Problem solving	1	1	0.04	1, 2, 3, 4, 5, 6, 7, 8
Individual partial tests	6	3	0.12	1, 3, 4, 5, 6, 7, 8
Practical activities	3	2	0.08	3, 5, 7, 9, 10
Final test	6	2	0.08	1, 2, 3, 4, 5, 6, 7, 8

The dates for continuous assessment will be published on the Virtual Campus and in the course presentation slides. They may be subject to scheduling changes due to unforeseen circumstances. Any such changes will always be communicated through the UAB Virtual Campus, which is considered the standard platform for communication between teaching staff and students.

The course will be assessed out of 10 points as follows:

- Theory (7 points): To pass the course, students must obtain at least 3.5 out of the 7 points allocated to the theory component in order for it to be averaged with the practical component. The assessment of the theoretical part of the course consists of two components:
- Examinations (6 points): Two individual midterm examinations worth a total of 6 points (3 points each). As part of the continuous assessment, these examinations will be held during the theory sessions. Each examination will assess a different part of the syllabus, and the final examination mark will be the arithmetic mean of the two. Each examination will only be included in the average if a minimum score of 4 out of 10 is obtained. If either examination receives a score of 4 or below, the midterm examinations will be considered failed.
- Exercises (1 point): As part of the continuous assessment, activities and exercises will be carried out in class and/or online and submitted according to the instructions provided. These exercises are not eligible for reassessment.
- Mandatory laboratory sessions (3 points): As part of the continuous assessment, students must complete several laboratory assignments in the Integrated Laboratory. The laboratory assignments must be submitted on the dates specified in the Virtual Campus. However, they will be assessed exclusively through an examination held during the laboratory session immediately following the session in which each assignment was completed (for the last laboratory assignment, the assessment will take place on the day of the second midterm examination). These examinations will assess students' understanding of both the theoretical and practical concepts associated with each laboratory activity. Students must obtain at least 1.5 out of the 3 points allocated to the laboratory component in order to pass the course.

Students who fail the theoretical component of the course may sit the final examination, which will cover the entire course syllabus, regardless of the marks obtained in the midterm examinations. The grade obtained in this reassessment examination will replace the midterm examination grade when calculating the final course mark and will account for 60% of the final grade.

To pass the course, the combined score of the reassessment examination and the exercises must be greater than 5 out of 10.

Students wishing to improve the mark obtained in the midterm examinations may also sit the final examination. In this case, submitting the examination for grading automatically replaces the marks previously obtained in the midterm examinations.

Reassessment of the laboratory component will consist of a single examination covering the contents of all laboratory sessions. The maximum grade obtainable in this reassessment examination will be 7.5 out of 10.

Submitted exercises cannot be reassessed.

For each assessment activity, the place, date and time of the review session will be announced. During this session, students may review their assessment with the instructor and submit appeals regarding the grade. These appeals will be evaluated by the course instructors. Students who do not attend the scheduled review session will not be entitled to a later review.

This course does not offer the single assessment system.

Students who have previously taken the course and have already passed the laboratory component will retain their laboratory grade. However, they must inform the laboratory instructors at the beginning of the semester (when laboratory groups are organized). Under no circumstances will grades from theory examinations or submitted exercises from previous editions of the course be retained.

Without prejudice to any other disciplinary measures that may be deemed appropriate, and in accordance with current academic regulations, any irregularity committed by a student that may affect the assessment process will result in a grade of zero (0). Assessment activities graded in this way are not eligible for reassessment. If passing any such assessment activity is required to pass the course, the student will automatically fail the course, with no opportunity for reassessment during the same academic year. Such irregularities include, but are not limited to:

- Copying all or part of a laboratory assignment, report, or any other assessment activity.
- Allowing another student to copy.
- Submitting group work that has not been completed entirely by the members of the group.
- Unauthorized use of Artificial Intelligence tools (e.g., Copilot, ChatGPT, or similar systems) to solve exercises, laboratory assignments, or any other graded activity.
- Submitting as one's own work materials produced by a third party, including translations or adaptations, or, in general, work containing elements that are not original and exclusively created by the student.
- Having communication devices (such as mobile phones, smartwatches, etc.) accessible during individual theory or practical examinations.
- Talking to other students during individual theory or practical examinations.
- Copying or attempting to copy from other students during examinations.
- Using or attempting to use written material related to the subject during examinations when such material has not been explicitly authorized.

In future editions of the course, students who have committed academic misconduct in any assessment activity will not be granted credit for any assessment activities previously completed.

In summary, copying, allowing others to copy, plagiarism, or attempting any of these actions in any assessment activity will result in a FAIL grade. Such a fail cannot be compensated and no assessment components will be recognized in future editions of the course.

- Students who obtain the minimum overall score required to pass the course but fail to achieve the minimum required mark in one or more assessment activities will receive a final grade of 4.5. If the course is failed because of a zero awarded for academic dishonesty, the final course grade will be 3, making the course ineligible for compensation.
- Students who do not attend any individual assessment activity (the two midterm examinations and the final examination) will receive the final grade "Not Assessable" (NA). Attendance at any of these assessment activities will automatically result in a final grade other than NA.
- No assessment activity will be rescheduled unless there is a justified reason, the student has informed the instructors in advance, and explicit approval has been granted by the teaching staff. Otherwise, missed assessment activities cannot be made up. The Assessment Activity Rescheduling Request Protocol is available on the School of Engineering website and applies in the cases described in the School's assessment regulations and guidelines.
- Regarding Honours Distinction (Matrícula de Honor), it may be awarded to students who obtain a final

course grade of 9.0 or higher. Since the number of honours distinctions cannot exceed 5% of enrolled students, they will be awarded to those with the highest final grades. In the event of a tie, the quality of the solutions submitted in the various assessment activities completed throughout the course will be taken into account.

- In this course, the use of Artificial Intelligence (AI) technologies is permitted only for learning support tasks, such as literature or information searches, proofreading, or personal study. The use of AI technologies to complete graded assignments (i.e., laboratory assignments, submitted exercises, or examinations) is strictly prohibited. Any submission containing AI-generated content will be considered a breach of academic integrity and may result in partial or full penalties in the corresponding assessment, or more severe disciplinary sanctions in serious cases.

Bibliography

- Josep M. Basart, Josep Rifà i Mercè Villanueva: Fonaments de matemàtica discreta. Materials de la UAB. (1999). Biblioteca UAB: https://bibcercador.uab.cat/permalink/34CSUC_UAB/1eqfv2p/alma991004816599706709
- Josep Rifà i Llorenç Huguet: Comunicació Digital. Masson Ed. (1991). Biblioteca UAB: https://bibcercador.uab.cat/permalink/34CSUC_UAB/1eqfv2p/alma991002495519706709
- Victor Shoup: A computational Introduction to number theory and Algebra. (2008). <http://shoup.net/ntb/>. Biblioteca UAB: https://bibcercador.uab.cat/permalink/34CSUC_UAB/avjcib/alma991010755053206709
- Cristina Pérez Solà i Jordi Herrera Joancomartí, La criptografia que et cal saber. (2023) Disponible on-line: <https://criptografia.cat/>
- Nigel P. Smart: Cryptography Made Simple. Springer. (2016). <https://doi.org/10.1007/978-3-319-21936-3>. Biblioteca UAB: https://bibcercador.uab.cat/permalink/34CSUC_UAB/1eqfv2p/alma991006792939706709
- Christof Paar i Jan Pelzl: Understanding Cryptography: A Textbook for Students and Practitioners. Springer. (2010). <https://doi.org/10.1007/978-3-642-04101-3>. Biblioteca UAB: https://bibcercador.uab.cat/permalink/34CSUC_UAB/1eqfv2p/alma991010489805006709
- Ross Anderson: Security Engineering: A Guide to Building Dependable Distributed System, Wiley (2001). Biblioteca UAB: https://bibcercador.uab.cat/permalink/34CSUC_UAB/1c3utr0/cdi_proquest_ebookcentral_EBC6412239
- Charles P. Pfleeger: Security in Computing. Prentice Hall (1997). Biblioteca UAB: https://bibcercador.uab.cat/permalink/34CSUC_UAB/avjcib/alma991005937479706709
- Andreas M. Antonopoulos: Mastering Bitcoin. Programming the Open Blockchain. O'Reilly Media (2017) 3rd Edition. <https://github.com/aantonop/bitcoinbook> . Biblioteca UAB: https://bibcercador.uab.cat/permalink/34CSUC_UAB/1eqfv2p/alma991010936637306709

Software

The practical activities of the subject will be developed using Python.

Course groups and languages

The information provided is provisional until November 30. After this date, you will be able to consult the language of each group through this [link](#). To access the information, you will need to enter the course CODE

Type of teaching	Group	Language	Semester	Shift
(TE) Theory	450	Catalan	first semester	morning-mixed
(PAUL) Classroom practices	451	Catalan	first semester	morning-mixed
(PLAB) Practical laboratories	451	Catalan	first semester	morning-mixed
(PAUL) Classroom practices	452	Catalan	first semester	morning-mixed

(PLAB) Practical laboratories	452	Catalan	first semester	morning-mixed
(PAUL) Classroom practices	453	Catalan	first semester	morning-mixed
(PLAB) Practical laboratories	453	Catalan	first semester	morning-mixed
(PLAB) Practical laboratories	454	Catalan	first semester	morning-mixed
(PLAB) Practical laboratories	455	Catalan	first semester	morning-mixed