UAB
Universitat Autònoma de Barcelona

Fundamentals of Information Technology

Code: 102773
ECTS Credits: 6

2024/2025

Degree	Type	Year
2502441 Computer Engineering	OB	3
2502441 Computer Engineering	OT	4

Contact

Name: Cristina Perez Sola

Email: cristina.perez@uab.cat

Teachers

Maria Merce Villanueva Gay

(External) Carles Garrigues Olivella

Teaching groups languages

You can view this information at the end of this document.

Prerequisites

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

Objectives and Contextualisation

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.

Competences

Computer Engineering

- Acquire personal work habits.
- Acquire thinking habits.
- Capacity to design, develop, evaluate and ensure the accessibility, ergonomics, usability and security of computer systems, services and applications, as well as of the information that they manage.

- Have the capacity to select, deploy, integrate and manage information systems that satisfy the needs of an organisation, identifying the cost and quality criteria.
- Have the capacity to understand an organisation's environment and its needs in the field of information and communication technologies.
- Know and apply basic elements of economics, human resource management, project organisation and planning, as well as legislation, regulation and standardisation in the field of computer projects.

Learning Outcomes

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

Content

1. The role of the ICT
    1. ICT in the organitzation
2. Fundamentals
    1. Modular Arithmethic
    2. Polinomials over GF(2)
3. Information processing
    1. Ciclic codes
    2. CRC and LFSR
4. Advanced cryptography
    1. Public key cryptography
    2. Hash funcions
    3. Cryptographic protocols
5. Aplications
    1. Blockchain technology
    2. Cryptocurrencies: Bitcoins

Activities and Methodology

Title	Hours	ECTS	Learning Outcomes
Type: Directed			
Exercises classes	12	0.48	6, 9, 8, 10
Mandatory laboratory classes	12	0.48	1, 6, 7, 2, 4, 8, 10
Theory classes	26	1.04	1, 3, 6, 7, 2, 4, 5, 8, 10
Type: Supervised			

Tutoring and consults	17	0.68	1, 6, 7, 8, 10
Type: Autonomous			
Exercises and practices preparation	25	1	1, 3, 7, 8, 10
Final test preparation	25	1	1, 3, 7, 8, 10
Personal work	25	1	1, 3, 7, 2, 9, 8, 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.).

Transversal competences. These competences will be worked out and evaluated at various times throughout the course. Specifically:

- T01.03 - Develope scientific thought: It will work more intensively in the sessions of problemsof the subject where students will have to analyze the problems presented and see what theoretical solutions are the most appropriate and how they can be applied.
- T02.01 - Work independently: This competence is focused on individual activities, such as the delivery of problems that are carried out throughout the course or the individual proofs of the subject.
- T02.04 - Prevent and solve problems: This competence is worked more extensively in the practical sessions of the subject.

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

Continous Assessment Activities

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

The dates of continuous assessment will be published on the virtual campus and in the transparency of the presentation of the subject and may be subject to changes in programming due to adaptation to possible incidents. These changes will always be reported through the UAB virtual campus, as it is understood that this is the usual platform for the exchange of information between teachers and students.

The evaluation of the subject, on 10 points, will be done as follows:

- Theoretical part (7 points): In order to pass the subject, it is necessary to pass the theoretical part individually so that it can average, ie it is necessary to obtain at least 3.5 points in the total assessment of the theoretical part. The evaluation of the theoretical part of the course is divided into two
  Examns (6 points): Two individual partial tests for a total of 6 points (3 points each). As part of the ongoing assessment, these tests will be conducted during the theory sessions. Each test will evaluate a part of the syllabus separately and the final grade will be the arithmetic mean of the two tests. Each test will only be able to average if it is graded with a grade higher than 4 out of 10. In case one of the tests does not have a grade higher than 4, the partial tests will be considered suspended.
  Exercises (1 point): As part of the continuous assessment, the resolution of activities or exercises proposed throughout the course will be delivered.
- Practical activities (3 points): As part of the continuous assessment, some practical activities will have to be solved in the Integrated Laboratory. You must obtain at least 1.5 points in the assessment of the internship, out of the 3 on which the internship is assessed, in order to pass the subject.

Students who have failed the theory part of the subject will have the option of taking the final exam, where they will be examined in the whole syllabus of the course, regardless of the marks obtained in the partial exams.

Students who want to improve the mark obtained in the partial exams, can take the final exam to improve the mark. In this case, the fact of handing in the exam and having the teacher correct it will involve overwriting the grades of the previous exams.

The delivery of the exercises and the realization of the practices will not be possible to recover them.

For each assessment activity, a place, date and time of review will be indicated in which the student will be able to review the activity with the teacher. In this context, claims may be made on the grade of the activity, which will be evaluated by the teacher responsible for the subject. If the student does not appear for this review, this activity will not be reviewed later.

Those students who have previously taken the course and who have passed the internship will be retained in the internship grade. It is important, however, that you contact the internship teacher of the subject at the beginning of the course (when the internship groups are held) to inform him of this fact. In no case will the marks of the theory exams or those of the deliveries of the problems that are carried out throughout the course be maintained.

Without prejudice to other disciplinary measures deemed appropriate, and in accordance with current academic regulations, irregularities committed by a student that may lead to a variation in the grade will be graded with a zero (0). Assessment activities qualified in this way and by this procedure will not be recoverable. If it is necessary to pass any of these assessment activities to pass the subject, this subject will be suspended directly, without the opportunity to retake it in the same course. These irregularities include, but are not limited to:

- the total or partial copy of a practice, report, or any other assessment activity;
- let copy;
- present group work not done entirely by group members;
- present as own materials prepared by a third party, even if they are translations or adaptations, and in general works with non-original and exclusive elements of the student;
- have communication devices (such as mobile phones, smart watches, etc.) accessible during individual theoretical-practical assessment tests (exams);
- talk with classmates during individual theoretical-practical assessment tests (exams);
- copying or attempting to copy from other students during the theoretical-practical assessment tests (exams);

- use or attempt to use writings related to the subject during the performance of the theoretical-practical assessment tests (exams), when these have not been explicitly allowed.

In future editions of this subject, the student who has committed irregularities in an evaluation act will not be validated any of the evaluation activities carried out.

To sum up: copying, let copy or plagiarizing (or attempting to) in any of the assessment activities is equivalent to a SUSPENSION, not compensable and without validations of parts of the subject in later courses.

Students who achieve the minimum number of points to pass the course, but have not reached the minimum grade in any of the assessment activities, will be assessed with a final grade of 4.5. In the event that the subject has not been passed due to the grade of zero of an activity due to copying, the final mark of the subject will be a 3, which will not compensate for this subject.

Finally, those students who do not take any of the individual tests (partial tests and the final exam) will obtain the qualification of "Non-Evaluable". Participation in any of these assessment activities will result in a different grade of "Non-Assessable".

No assessment activity will be carried out on any student at a time other than that established unless there is a just cause, the activity has been notified in advance and the teacher has given his / her consent. In any other case, if a student has not attended an activity, it cannot be recovered.

Bibliography

- Josep M. Basart, Josep Rifà and Mercè Villanueva: Fonaments de matemàtica discreta. Materials de la UAB. (1999).
- Josep Rifà and Llorenç Huguet: Comunicación Digital. Masson Ed. (1991).
- Victor Shoup: A computational Introduction to number theory and Algebra. (2008). http://shoup.net/ntb/
- Cristina Pérez Solà and Jordi Herrera Joancomartí, La criptografia que et cal saber. (2023) Disponible on-line: https://criptografia.cat/
- Nigel P. Smart: Cryptography Made Simple. Springer. (2016)
- Christof Paar and Jan Pelzl: Understanding Cryptography: A Textbook for Students and Practitioners. Springer. (2010).
- Ross Anderson: Security Engineering: A Guide to Building Dependable Distributed System, Wiley (2001).
- Charles P. Pfleeger: Security in Computing. Prentice Hall (1997).
- Andreas M. Antonopoulos: Mastering Bitcoin. Programming the Open Blockchain. O'Reilly Media (2017) 3rd Edition. https://github.com/aantonop/bitcoinbook

Software

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

Language list

Name	Group	Language	Semester	Turn
(PAUL) Classroom practices	451	Catalan	first semester	morning-mixed

(PAUL) Classroom practices	452	Catalan	first semester	morning-mixed
(PLAB) Practical laboratories	451	Catalan	first semester	morning-mixed
(PLAB) Practical laboratories	452	Catalan	first semester	morning-mixed
(PLAB) Practical laboratories	453	Catalan	first semester	afternoon
(PLAB) Practical laboratories	454	Catalan	first semester	afternoon
(PLAB) Practical laboratories	455	Catalan	first semester	morning-mixed
(TE) Theory	450	Catalan	first semester	morning-mixed