Universitat Autònoma de Barcelona

2020/2021

Fundamentals of Information Technology

Code: 102773
ECTS Credits: 6

Degree	Type	Year	Semester
2502441 Computer Engineering	OB	3	1
2502441 Computer Engineering	OT	4	1

The proposed teaching and assessment methodology that appear in the guide may be subject to changes as a result of the restrictions to face-to-face class attendance imposed by the health authorities.

Contact

Name: Jordi Herrera Joancomarti
Email: Jordi.Herrera@uab.cat

Use of Languages

Principal working language: catalan (cat)
Some groups entirely in English: No
Some groups entirely in Catalan: Yes
Some groups entirely in Spanish: No

Teachers

Josep Rifà Coma
Victor García Font

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 organisations 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 organisations 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

Methodology

Due to the situation derived from the COVID-19, the teaching of this subject for this course will be done in virtual format, both the theory sessions as well as the problems and practical sessions.

Before each theory session, the teacher will post a series of readings and materials on the virtual campus that the students must work on previously in the session. The theory session will consist of a synchronous online videoconference where the teacher will make a brief summary of the proposed readings and answer the questions that the students raise about the topic they have worked on. The teacher will also be able to propose questions to the students to repeat the most important questions of the subject of study so that they are clearer.
The problem sessions will be based on a list of exercises that the student will try to solve on their own. Before the problem session, the students will send the doubts of the proposed exercises to the teacher. This will make a video solving the doubts raised by the students and he will hang in the classroom on the date of the problem session.

In the practical sessions some of the topics covered in the theory sessions and problems will be covered in depth so that the students learn the difficulties that arise in the practical implementation of the systems that are worked on in the subject. The practices of this subject will follow an online and asynchronous work methodology. Each of the practices will be published at the beginning of the week and students in groups of two will have 5 days to solve it. The internship teacher will assist the students and answer their questions by email within 24 hours.

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.

Activities

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

Assessment

Continuous assessment dates will be published on the virtual campus and on the presentation slides, and the programming may change because of adaptation to possible incidents. Any modification will always be informed in the Campus Virtual, which is the usual exchange of information platform between teachers and students.

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

- Theory (7 points): Two individual partial tests (3,5 points each). As part of the continuous assessment, the first test will be done in theory classes hours, and the second will be done on the date specified for the coordination. Each test will evaluate a part of the course separately and the final mark will be the arithmetic mean of the two tests. Each test will only be able to do average in case it is qualified with a note greater than 4.
- Mandatory laboratory practices (3 ponits): As part of the continuous assessment, they will have to be done some laboratory assignments. At least 1 point (of 2.5 points) must be obtained pass the subject

In case the stundent does not pass any of the partial tests, they can be recovered as follows:

- Students who have fail the theory part will have the option of take a final exam, where they will be examined by the part of the subject that is suspended or from both parts, in the case of having both parts suspended. Students who want to improve the mark obtained in the partial exams can also take the final exam to improve their mark.

Failing either mandatory practices or exercices proposed during the course will not be able to be recovered.

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 theteacher. In this context, claims can be made about the activity grade, which will be graded by the teachers responsible for the subject. If the student does not take part of this review, this activity will not be reviewed later.

Those students who have already previously followed the subject and who have passed the mandatory laboratory practives will be able to kept the practices' mark. It is important, however, that they contact the teacher of the subject at the beginning of the course (when the practice groups are carried out) to inform him of this fact. Such behaviour is only intendend for mandatory laboratory practices, so marks from theory and/or exercicies will not be keep from previous courses.

Notwithstanding other disciplinary measures deemed appropriate, and in accordance with the academic regulations in force, the irregularities committed by a student who can lead to a variation of the qualification will be qualified with zero (0). The assessment activities qualified in this way and by this procedure will not be recoverable. If you need to pass any of these assessment activities to pass the subject, this subject will be failed directly, without opportunity to recover it in the same course These irregularities include, among others:

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

To pass the course it is necessary that the mark of each one of the parts exceeds the minimum required and that the final mark exceeds 5 points. If you do not pass the subject because some of the assessment activities do not reaches the minimum mark required, the mark in the Transcript of Records (ToR) will be the lowest value between 4.5 and the average weighted notes. With the exceptions that the "non-evaluable" qualification will be assigned to those who do not participate in any of the assessment activities, and that the mark in the ToR will be the lowest value between 3.0 and the weighted average of the marks, in case that irregularities have been committed in an assesment act (and therefore compensation will not be possible). In order to get an honors, the final grade must be equal or higher to 9 points. Because the number of honors can not exceed 5% of the number of students enrolled, it is given to whoever has the highest final marks. In case of a tie, it will be taken into account the resolutions of the partial tests.

It is important to keep in mind that there will be no assesment activity for any student at a different time of the established unless there is a justified cause, it has been advised before the activity and the teaching staff has given their consent. In any other case, if the student has not attended an activity, this can not be recovered.

You can check the academic regulations of the UAB approved by the Governing Council of the UAB: http://webs2002.uab.es/afers_academics/info_ac/0041.htm

Assessment Activities

Title	Weighting	Hours	ECTS	Learning Outcomes
Exercises resolution	7	4	0.16	1, 3, 6, 7, 4, 5, 8
Final test	7	2	0.08	1, 3, 6, 7, 4, 5, 8, 10
Individual partial tests	6	2	0.08	6, 7, 2, 9, 8

Bibliography

- J.M. Basart, J. Rifà i M. Villanueva: Fonaments de matemàtica discreta. Materials de la UAB. (1999).
- J. Rifà i L. Huguet: Comunicación Digital. Masson Ed. (1991).
- V. Shoup: A computational Introduction to number theory and Algebra. (2008). http://shoup.net/ntb/
- J. Domingo i J. Herrera, Criptografia per als Serveis Telemàtics i el Comerç Electrònic, Col·lecció Manuals no. 31, Barcelona: Editorial UOC, (1999). ISBN 84-8429-007-7.
- N. P. Smart: Cryptography Made Simple. Springer. (2016)
- C. Paar, J. Pelzl: Understanding Cryptography: A Textbook for Students and Practitioners. Springer. (2010).
- R. Anderson: Security Engineering: A Guide to Building Dependable Distributed System, Wiley (2001).
- C.P. Pfleeger: Security in Computing. Prentice Hall (1997).
- A. M. Antonopoulos: Mastering Bitcoins. Unlocking digital cryptocurrencies. O'Reilly Media (2017) 2nd Edition. https://github.com/aantonop/bitcoinbook