Universitat Autònoma de Barcelona

2021/2022

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

Victor García Font

Mercè Villanueva Gay

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

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.

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 (6 points): Two individual partial tests (3 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.
- Exercises (1 point): As part of the continuous assessment, activities must be carried out or exercises must be solved and presented for evaluation.
- 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.

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

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

Software

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