Universitat Autònoma de Barcelona

2022/2023

Information and Security

Code: 102769
ECTS Credits: 6

Degree	Type	Year	Semester
2502441 Computer Engineering	OB	2	2

Contact

Name: Cristina Fernandez Cordoba
Email: cristina.fernandez@uab.cat

Use of Languages

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

Other comments on languages

Group 43 classes wil be given in English and all the other groups in Catalan.

Teachers

Victor García Font
Jordi Ventayol Marimón
Adrian Cabello Corpas
Victor Asensio Casas
Adrià Figuerola Torrell

Prerequisites

There are no prerequisites. However, students should be familiar with basic algorithms and programming. It is also recommended for students to have notions of linear algebra, mathematical analysis and probabilities.

Objectives and Contextualisation

The "Information and Security" course is part of SUBJECT 9: ALGORITHMIC AND INFORMATION. The course deals with topics such as: information measures; source and channel coding; cryptography; privacy, authenticity and accessibility; public key infrastructure (PKI), etc.

Competences

- Acquire thinking habits.
- Capacity to design, develop, select and evaluate computer applications and systems, ensuring reliability, security and quality, in accordance with ethical principles, and applicable standards and legislation.

- Have the capacity to conceive, draft, organise, plan, develop and sign projects in the field of computer engineering for the conception, development and exploitation of computer systems, services and applications.
- Have the right personal attitude.
- Know and apply the basic algorithmic procedures of computer technologies to design solutions for problems and to analyse the adequacy and complexity of the algorithms proposed.

Learning Outcomes

1. Demonstrate a high capacity for abstraction.
2. Design, develop, select and evaluate applications, ensuring their reliability and security.
3. Develop curiosity and creativity.
4. Identify the computational complexity of an algorithm in terms of memory resources and run time.
5. Identify the main attacks that a computer system can receive, as well as the possible protection and detection methods and the application of security policies to avoid damage to the system or minimise the repercussions.
6. Manage information by critically incorporating the innovations of one's professional field, and analysing future trends.

Content

1. Motivation. Introduction to communication problems (1 hour)
    1. Communication model. Elements.
    2. Noise, transmission errors.
    3. Spies: privacy and authenticity.
2. Basic concepts of information theory (4 hours)
    1. Information measurement.
    2. Shannon's memoryless discrete source.
    3. Entropy of a discrete random variable.
    4. Mutual information between two discrete random variables. Channel capacity.
3. Source coding (3 hours)
    1. Fixed and variable length codes, uniquely decodable codes, and instant codes.
    2. Shannon's first theorem. Existence of optimal codes.
    3. Construction of optimal codes: Huffman method.
4. Data compression (3 hours)
    1. Types of compression.
    2. Statistical methods and dictionary techniques.
5. Channel coding (3 hours)
    1. Important models of memoryless discrete channels.
    2. Decoding rules.

3. Shannon's second theorem.

6. Detector and error-correcting codes (4 hours)
    1. Coding. Block codes. Errors.
    2. Linear binary codes. Parameters.
    3. Generator and control matrices.
    4. Decoding.
    5. Some important codes.
7. Cryptography and security (8 hours)
    1. Basic concepts. Security and authenticity.
    2. Symmetric key cryptography.
    3. Public key cryptography.
    4. Digital certificates and public key infrastructures.

Methodology

Theoretical content will be taught through 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 also be encouraged to present their own solutions in class.

During laboratory sessions, topics related to the lectures will be studied in depth. These include the presentation of real cases, or the extension of certain subjects with techniques and algoriths alternative to those already seen. Campus Virtual will be used for communication between lecturers and students (material, updates, announcements, etc.).

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

- T01.04 - To develop systemic thinking: Throughout the course, we consider the different parts that intervene in a system of transmission of the information and we will see how they are related between them. The evaluation of this competence isincluded in the evaluation of the resolution of exercises and in the partial and final tests.
- T06.02 - To develop curiosity and creativity: Especially in the resolution of challenges that appear throughout the course, as for example in the resolution of problems. In this case, the curiosity and creativity areneeded to carry out the resolution.
- T06.04 - To manage information by critically incorporating the innovations of the professional field, and to analyze the trends of the future: In the realization of the practices it is necessary to use techniques that are being used today. In this part we consider what are future trends and how they are used in the resolution of the practices.

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			
Exercise-based classes	12	0.48	1, 2, 5, 4
Mandatory laboratory classes	12	0.48	1, 3, 2, 6, 5, 4
Theorical classes / lectures	26	1.04	1, 2, 5, 4
Type: Supervised			
Tutoring and consultations	17	0.68	1, 2, 5, 4
Type: Autonomous			
Other independent study	25	1	1, 2, 5, 4
Preparing exercises and practical assigments	25	1	1, 2, 5, 4
Preparing the final test	25	1	1, 2, 5, 4

Assessment

Continuous-assessment dates will be published on Campus Virtual and on the presentation slides, specific programming may change when necessary. Any such modification will always be communicated to students through Campus Virtual, which is the usual communication platform between lecturers and students.

Subject assessment (out of 10 points) will be carried out as follows:

- Two individual partial tests, 6 points (out of 10, 3 points each). As part of continuous assessment, the first test will take place during lectures;the second will take placeon the date specified bycoordination. The first partial test will be givenat the end of the first five chapters of the course; the second partial test will be givenonfinishing all the chapters of the course. At least 2.4 points (out of 6 points) must be obtained in order to pass the subject.
- Exercises resolution, 1.5 points (out of 10). As part of continuous assessment, activities must be carried out or exercises must be solved via online quizzes. In some cases, another assessment activity could be programmed and will be informed to the students through the Campus Virtual.
- Mandatory laboratory practices, 2.5 points (out of 10). As part of continuous assessment, certainlaboratory assignments must be fulfilled. In some cases, validation tests may be done to guarantee authorship and the acquisition of competences. At least 1 point (out of 2.5 points) must be obtained to pass the subject.
- Final exam, 6 points (out of 10). Those who have not passed the subject throughthe individual partial tests will have the option to takefinal exam as a re-assessment grade to compensatethe individual partial tests. There is thereforeno separete re-assessment for each partial test;thisexam covers material from the entirecourse. At least 2.4 (out of 6) points must be obtained in order to pass the subject.

Notwithstanding other disciplinary measures deemed appropriate, and in accordance with the academic regulations in force, assessment activities (laboratory practices, exercises ressolutions or exams) will receive a zero score whenever a student commits academic irregularities that may alter such assessment. Assessment activities graded in this way and by this procedure will not be re-assessable. If passing the assessment activity or activities in question is required to pass the subject, the awarding of a zero for disciplinary measures will also entail a direct fail for the subject, with no opportunity to re-assess this in the same academic year. Irregularities contemplated in this procedure include, among others:

- the total or partial copying of a practical exercise, report, or any other evaluation activity;
- allowing others to copy;
- presenting group work that has not been done entirely by the members of the group;
- presenting any materials prepared by a third party as one's own work, even if these materials are translations or adaptations, including work that is not original or exclusively that of the student;

To pass the course it is necessary that the markof each one of the parts exceeds the minimum required and that the overall grade is 5.0 or higher. If you do not pass the subject because some of the assessment activities do not reach 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-assessable" grade will be assigned to those students 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 the event of irregularities have been committed for any assessmentactivity(andtherefore re-assessmentwill not be possible). In order to pass the course with honors, the final grade must be a9.0 o higher. Because the number of students with this distinction cannot exceed 5% of the numberof students enrolled in the course, this distinction will be awardedtowhoever has the highest final grade. In case of a tie, partial-test results will be taken into consideration.

It is important to bear in mind that no assessment activities will be permited for any student at a different date or time to that established, unless for justified causes duly advised before the activity and with the lecturer's previous consent. In all other cases, if an activity has not been carried out, this cannot be re-assessed.

In the case of on-line quizzes, a review may be requested after the date of closure of the quiz. For all other assessment activities, a place, date and time of review will be indicated allowing students to review the activity with the lecturer. In this context, students may discuss the activity grade awarded by the lecturers responsible for the subject. If students do not take part in thisreview, no further opportunity will be made available.

To consult the academic regulations approved by the Governing Council of the UAB, please follow this link: http://webs2002.uab.es/afers_academics/info_ac/0041.htm

Assessment Activities

Title	Weighting	Hours	ECTS	Learning Outcomes
Exercises resolution	1.5	1	0.04	1, 2, 5, 4
Final test	6	2	0.08	1, 2, 6, 5, 4
Individual partial tests	6	3	0.12	1, 2, 4
Mandatory laboratory practices	2.5	2	0.08	1, 3, 2, 6, 5, 4

Bibliography

Basic bibliography

- L. Huguet i J. Rifà. Comunicación Digital. Ed. Masson, 1991.
- D. Salomon: Data compression - The Complete Reference, 4th Edition. Springer 2007.
- R.B. Ash. Information Theory. John Wiley and Sons Inc, 1965.
- G. Alvarez. Teoría matemática de la información. Ediciones ICE, 1981.
- T.C. Bell, J.G. Cleary i I.H. Witten. Text Compression. Prentice Hall, 1990.
- J. Domingo i Ferrer and J. Herrera i Joancomartí, Criptografia per als Serveis Telemàtics i el Comerç Electrònic, Col·lecció Manuals no. 31, Barcelona: Editorial UOC, 1999. ISBN 84-8429-007-7.
- A. Menezes, P. van Oorschot and S.Vanstone.: Handbook of Applied Cryptography, CRC Press. (1996). Available at http://www.cacr.math.uwaterloo.ca/hac .

Complementary bibliography

- C.E. Shannon, "A mathematical theory of communications," Bell Syst. Tech. J., 27, 379-423, 1948.
- B. McMillan, "The basic theorems of Information Theory," Ann. Math. Stat., 24, 196-219, 1953.
- A.I. Khinchin. Mathematical foundations of Information Theory. Dover Publications, Inc., 1957.
- R. W. Hamming. Coding and Information Theory. Prentice Hall, Inc., 1980.
- M. Mansuripur. Introduction to Information Theory. Prentice Hall, Inc., 1987.

- G.J. Chaitin. Algorithmic Information Theory. Cambridge University Press., 1987.
- An Introduction to Computer Security: The NIST Handbook. Special Publication 800-12. NIST(1995). http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf
- D. E. Robling Denning. Cryptography and Data Security. Addison-Wesley Publishing Company (1988).
- B. Schneier. Applied Criptography, John Wiley and Sons, Inc. 1996.
- G.S. Simmons. Contemporary Criptology. The Science of Information Integrity, IEEEPress (1991).
- R. Anderson. Security Engineering: A Guide to Building Dependable Distributed System,Wiley (2001).
- C.P. Pfleeger. Security in Computing. , Prentice Hall (1997).
- V. Shoup. A computational Introduction tonumber theory and Algebra. http://shoup.net/ntb/

Software

The practical activities will be perform by using a docker environment, a Jupyter Notebook container and SageMa

SageMath is a free open-source mathematics software system licensed under the GPL. It builds on top of many

https://www.sagemath.org/)

Jupyter Notebook i a project directed by the comunity with the goal of develop "free software, open standards, and web services for interactive computing across all programming languages". (https://jupyter.org/)

Docker is an open source project that provides containers which isolate software from its environment and ensure that it works uniformly despite differences for instance between development and staging. (https://www.docker.com/resources/what-container/)