UAB
Universitat Autònoma de Barcelona

Information and Security

2026/2027

Code: 102769
Credits: 6

Degree programme	Type	Course
Computer Engineering	OB	2

Contact lecturer

Name : Cristina Fernandez Cordoba

Email : cristina.fernandez@uab.cat

Teaching staff

Ester Jara Lorente

Adrià Figuerola Torrell

Pau Quintas Torra

Julián Salas Piñón

Natàlia Blasco Andreo

Marc Caravaca Rodriguez

Group languages

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

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

The course deals with topics such as: information measures; source and channel coding; cryptography; privacy, authenticity and accessibility; public key infrastructure (PKI), etc.

Learning outcomes

- CM17 (Integrate cryptography, compression and coding methodologies into computer problem-solving.) Integrate cryptography, compression and coding methodologies into computer problem-solving.
- KM18 (Explain the concepts of cryptography, coding and data compression within the framework of information theory in problem-solving.) Explain the concepts of cryptography, coding and data compression within the framework of information theory in problem-solving.
- SM22 (Analyse IT services, applications and systems from the perspective of information theory.) Analyse IT services, applications and systems from the perspective of information theory.

Contents

1. Motivation. Introduction to communication problems (1 hour)

- Communication model. Elements.
- Noise, transmission errors.
- Spies: privacy and authenticity.

2. Basic concepts of information theory (4 hours)

- Information measurement.
- Shannon's memoryless discrete source.
- Entropy of a discrete random variable.
- Mutual information between two discrete random variables. Channel capacity.

3. Source coding (3 hours)

- Fixed and variable length codes, uniquely decodable codes, and instant codes.
- Shannon's first theorem. Existence of optimal codes.
- Construction of optimal codes: Huffman method.

4. Data compression (3 hours)

- Types of compression.
- Statistical methods and dictionary techniques.

5. Channel coding (3 hours)

- Important models of memoryless discrete channels.
- Decoding rules.
- Shannon's second theorem.

6. Detector and error-correcting codes (4 hours)

- Coding. Block codes. Errors.
- Linear binary codes. Parameters.
- Generator and control matrices.
- Decoding.
- Some important codes.

7. Cryptography and security (8 hours)

- Basic concepts. Security and authenticity.
- Symmetric key cryptography.
- Public key cryptography.
- Digital certificates and public key infrastructures.

Learning activities and methodology

Title	Hours	ECTS	Learning outcomes
Other independent study	25	1	CM17, SM22
Preparing exercises and practical assigments	25	1	CM17, SM22
Theorical classes / lectures	26	1.04	CM17, KM18, SM22
Exercise-based classes	12	0.48	CM17, KM18

Preparing the final test	25	1	CM17, KM18, SM22
Mandatory laboratory classes	12	0.48	SM22
Tutoring and consultations	17	0.68	KM18

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.).

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
Individual partial tests	6	3	0.12	CM17, KM18, SM22
Exercises resolution	1.5	1	0.04	CM17, SM22
Final test	6	2	0.08	CM17, KM18, SM22
Mandatory laboratory practices	2.5	2	0.08	SM22

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 place on the date specified by coordination. The first partial test will be given at the end of the first five chapters of the course; the second partial test will be given on finishing all the chapters of the course. At least 3 (out of 6) points in the average of the two midterms 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, laboratory assignments in groups must be fulfilled. The qualification of the lab sessions will be validated at class and, in case of hesitation, with a final exam. 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 through the individual partial tests, and have at least of 1 point out of 2.5 in laboratory practices, will have the option to take final exam as a re-assessment grade to compensate the individual partial tests. There is therefore no separete re-assessment for each partial test; this exam covers material from the entire course. At least 3(out of 6) points must be obtained in order to pass the subject.

Academic integrity:

Notwithstanding other disciplinary measures deemed appropriate, and in accordance with the academic regulations in force, assessment activities (laboratory practices, exercises resolutions 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;
- unauthorized used of AI (for example Copilot, ChatGPT, or equivalent);
- 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 mark of 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 file 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-assessment will not be possible).

In this course, the use of Artificial Intelligence (AI) technologies is not allowed at any stage. Any assignment that includes AI-generated content will be considered a breach of academic integrity and may result in a partial or full penalty on the activity's grade, or more severe sanctions in serious cases.

Course with honors:

In order to pass the course with honors, the final grade must be a 9.0 o higher. Because the number of students with this distinction cannot exceed 5% of the number of students enrolled in the course, this distinction will be awarded to whoever has the highest final grade. In case of a tie, partial-test results will be taken into consideration.

Exams and revision dates:

It is important to bear in mind that the allowed justifications to ask for a different date or time to perform an avaluation activity, and the procedure to do it are described in:
https://www.uab.cat/ca/enginyeria/doc/criteris-avaluacio-esola-enginyeria.pdf.

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.

Single assesment:

A single assesment is not considered in this course.

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

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. Herrera-Joancomartí, C. Pérez-Solà, La criptografia que et cal saber. 2023. Available at https://criptografia.cat.
- 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 SageMath.

- SageMath is a free open-source mathematics software system licensed under the GPL. It builds on top of many existing open-source packages: NumPy, SciPy, matplotlib, Sympy, Maxima, GAP, FLINT, R and many more. Access their combined power through a common, Python-based language or directly via interfaces or wrappers. Since version 9.0 released in January 2020, SageMath is using Python 3. (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/)

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	41	English	second semester	morning-mixed

(TE) Theory	43	Catalan/Spanish	second semester	morning-mixed
(TE) Theory	45	Catalan/Spanish	second semester	afternoon
(TE) Theory	47	Catalan/Spanish	second semester	morning-mixed
(PAUL) Classroom practices	411	English	second semester	morning-mixed
(PLAB) Practical laboratories	411	English	second semester	morning-mixed
(PAUL) Classroom practices	412	English	second semester	morning-mixed
(PLAB) Practical laboratories	412	English	second semester	morning-mixed
(PLAB) Practical laboratories	413	English	second semester	morning-mixed
(PLAB) Practical laboratories	414	Catalan/Spanish	second semester	morning-mixed
(PLAB) Practical laboratories	415	Catalan/Spanish	second semester	morning-mixed
(PLAB) Practical laboratories	416	Catalan/Spanish	second semester	morning-mixed
(PLAB) Practical laboratories	417	Catalan/Spanish	second semester	morning-mixed
(PLAB) Practical laboratories	418	Catalan/Spanish	second semester	morning-mixed
(PLAB) Practical laboratories	419	Catalan/Spanish	second semester	morning-mixed
(PLAB) Practical laboratories	420	Catalan/Spanish	second semester	morning-mixed
(PLAB) Practical laboratories	421	Catalan/Spanish	second semester	morning-mixed
(PLAB) Practical laboratories	422	Catalan/Spanish	second semester	morning-mixed
(PLAB) Practical laboratories	423	Catalan/Spanish	second semester	morning-mixed
(PLAB) Practical laboratories	424	Catalan/Spanish	second semester	morning-mixed
(PAUL) Classroom	431	Catalan/Spanish	second semester	morning-mixed

practices				
(PAUL) Classroom practices	432	Catalan/Spanish	second semester	morning-mixed
(PAUL) Classroom practices	451	Catalan/Spanish	second semester	afternoon
(PAUL) Classroom practices	452	Catalan/Spanish	second semester	afternoon
(PAUL) Classroom practices	471	Catalan/Spanish	second semester	morning-mixed