Universitat Autònoma de Barcelona

2023/2024

Data Transmission and Criptography

Code: 44734
ECTS Credits: 6

Degree	Type	Year	Semester
4318303 Reseach and Innovation in Computer Based Science and Engineering	OT	0	2

Contact

Name: Guillermo Navarro Arribas

Email: guillermo.navarro@uab.cat

Teaching groups languages

You can check it through this link. To consult the language you will need to enter the CODE of the subject. Please note that this information is provisional until 30 November 2023.

Prerequisites

There are no formal prerequisites. Graduate-level knowledge on topics related to data transmission are assumed.

Objectives and Contextualisation

The objective of this course is to study and delve into different data transmission search topics. To do this, the course focuses on providing an introduction to research in three main blocks:

- coding theory,
- data compression and
- security.

Students will learn advanced concepts of these topics and will be introduced to current research.

Learning Outcomes

- CA06 (Competence) Graduates will be able to design reliable, efficient and secure data transmission and storage systems, using error-correcting codes, compression and security techniques.
- CA06 (Competence) Graduates will be able to design reliable, efficient and secure data transmission and storage systems, using error-correcting codes, compression and security techniques.
- CA07 (Competence) Graduates will know how to plan and develop research projects in the field of information processing.
- CA07 (Competence) Graduates will know how to plan and develop research projects in the field of information processing.

- KA16 (Knowledge) Graduates will be able to describe different error correction systems applied to post-quantum cryptography and based on LDPC codes.
- KA17 (Knowledge) Graduates will be able to describe different compression methods used for IoT, social networking, telepresence, point cloud and medical imaging data.
- KA18 (Knowledge) Graduates will be able to describe different cryptographic methods based on elliptic curves and used in blockchain technology, as well as methods that guarantee data privacy.
- SA21 (Skill) Apply different encryption methods for error correction in the field of post-quantum cryptography and Big Data transmissions.
- SA22 (Skill) Apply different compression algorithms to different types of data.
- SA23 (Skill) Apply different cryptographic mechanisms, based on elliptic curves and blockchain technology, as well as data privacy.

Content

The main contents of the course are divided into the three main blocks of the subject:

- Coding theory: Error correction codes applied to post-quantum cryptography and LDPC codes used, e.g. on digital television.
- Data Compression: Compression for different types of data, such as the Internet of Things, social media, telepresence, medical imaging, and machine learning-based techniques.
- Security and privacy: elliptic curve cryptography, blockchain technology and its application to cryptocurrencies, data privacy.

Depending on the background and interests of the students, they will have the opportunity to delve more or less into certain topics.

Methodology

The methodology of this course is designed to expose students to some of the relevant research topics in the areas of coding theory, data compression and security. It will be based on the concept of "learning by doing", and will be adapted to the number of students who enroll in the course. There will generally be a combination of theoretical and practical sessions, including lectures, student assignments, presentations and collaborative work.

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			
Preparation of written assignments	25	1	CA06, CA07, KA16, KA17, KA18, SA21, SA22, SA23, CA06
Study for tests and presentations	15	0.6	CA06, CA07, KA16, KA17, KA18, SA21, SA22, SA23, CA06
Teacher directed sessions	45	1.8	CA06, CA07, KA16, KA17, KA18, SA21, SA22, SA23, CA06
Type: Supervised			

In-class activites	15	0.6	CA06, CA07, KA16, KA17, KA18, SA21, SA22, SA23, CA06
Type: Autonomous			
Homework and class preparation	35	1.4	CA06, CA07, KA16, KA17, KA18, SA21, SA22, SA23, CA06
Preparation of synthesis tests	15	0.6	CA06, CA07, KA16, KA17, KA18, SA21, SA22, SA23, CA06

Assessment

We want to adopt an assessment methodology that is flexible enough to adapt to the specific work done in class, which means that it can vary slightly from one course to another. The evaluation will be based on 2 different types of activities:

- Assignments: different assignments will be proposed to students during the course. These may include individual and group work and may have a theoretical or practical orientation. Examples can be: exercises, study and presentation of a topic related to the subject, practices, ...
- Test: Summative tests will be used as an individual assessment activity. These tests can be replaced by other assessment activities if, for example, the number of students is low.

The assessment activities will be explained in detail at the beginning of the course.

Assessment Activities

Title	Weighting	Hours	ECTS	Learning Outcomes
Assignments	70%	0	0	CA06, CA07, KA16, KA17, KA18, SA21, SA22, SA23
Synthesis test	30%	0	0	CA06, CA07, KA16, KA17, KA18, SA21, SA22, SA23

Bibliography

Will be provided at the beginning of the course. Given the dynamic nature of the topics to be presented, the specific bibliography will change each course to adapt it to the current state-of-the-art research in this area. It will usually include relevant papers.

Software

Will be provided at the beginning of the course.