Course guide
34954 - CC - Codes and Cryptography

Last modified: 01/06/2023

Unit in charge:	School of Mathematics and Statistics
Teaching unit:	749 - MAT - Department of Mathematics.
Degree:	MASTER'S DEGREE IN ADVANCED MATHEMATICS AND MATHEMATICAL ENGINEERING (Syllabus 2010). (Optional subject).

Academic year: 2023 **ECTS Credits:** 7.5 **Languages:** English

LECTURER

Coordinating lecturer:	SIMEON MICHAEL BALL MARKS
Others:	Segon quadrimestre: SIMEON MICHAEL BALL MARKS - A JAVIER HERRANZ SOTOCA - A

PRIOR SKILLS

Basic probability, basic number theory and linear algebra

REQUIREMENTS

Undergraduate mathematics

DEGREE COMPETENCES TO WHICH THE SUBJECT CONTRIBUTES

Specific:
1. RESEARCH. Read and understand advanced mathematical papers. Use mathematical research techniques to produce and transmit new results.
2. MODELLING. Formulate, analyse and validate mathematical models of practical problems by using the appropriate mathematical tools.
3. CALCULUS. Obtain (exact or approximate) solutions for these models with the available resources, including computational means.
4. CRITICAL ASSESSMENT. Discuss the validity, scope and relevance of these solutions; present results and defend conclusions.

Transversal:
5. SELF-DIRECTED LEARNING. Detecting gaps in one's knowledge and overcoming them through critical self-appraisal. Choosing the best path for broadening one's knowledge.
6. EFFICIENT ORAL AND WRITTEN COMMUNICATION. Communicating verbally and in writing about learning outcomes, thought-building and decision-making. Taking part in debates about issues related to the own field of specialization.
7. THIRD LANGUAGE. Learning a third language, preferably English, to a degree of oral and written fluency that fits in with the future needs of the graduates of each course.
8. TEAMWORK. Being able to work as a team player, either as a member or as a leader. Contributing to projects pragmatically and responsibly, by reaching commitments in accordance to the resources that are available.
9. EFFECTIVE USE OF INFORMATION RESOURCES. Managing the acquisition, structure, analysis and display of information from the own field of specialization. Taking a critical stance with regard to the results obtained.

TEACHING METHODOLOGY

The course is divided in two parts: codes and cryptography. Each part consists of 26 h of ordinary classes, including theory and problem sessions.

LEARNING OBJECTIVES OF THE SUBJECT

This course aims to give a solid understanding of the uses of mathematics in Information technologies and modern communications. The course focuses on the reliable and efficient transmission and storage of the information. Both the mathematical foundations and the description of the most importants cryptographic protocols and coding systems are given in the course.

STUDY LOAD

Type	Hours	Percentage
Hours large group	60,0	32.00
Self study	127,5	68.00

Total learning time: 187.5 h

CONTENTS

Introduction

Description:
The problem of communication. Information theory, Coding theory and Cryptographic theory

Full-or-part-time: 6h 15m
Theory classes: 2h
Self study : 4h 15m

Information and Entropy

Description:
Uncertainty or information. Entropy. Mutual information

Full-or-part-time: 18h 45m
Theory classes: 6h
Self study : 12h 45m

Source codes without memory

Description:
Codes. Average length. Huffman codes. Extensions of a source. Theory of an noiseless communication. Notes of compression.

Full-or-part-time: 12h 30m
Theory classes: 4h
Self study : 8h 30m

Channel coding

Description:
Discrete channels without memory. Symmetric channels. Shannon's theorem.

Full-or-part-time: 18h 45m
Theory classes: 6h
Self study : 12h 45m

Block codes

Description:
Hamming's distance. Detection and correction of errors. Bounds. Linear codes.

Full-or-part-time: 18h 45m
Theory classes: 6h
Self study : 12h 45m

Cyclic codes

Description:
Cyclic codes. Generator and control matrices. Factorization of x^n-1. Roots of a cyclic code. BCH codes. Primitive Reed-Solomon codes. Meggit's decoder.

Full-or-part-time: 18h 45m
Theory classes: 6h
Self study : 12h 45m

Introduction to modern cryptography

Description:
The setting: secure storage and symmetric key encryption. Turing machines and complexity classes. Security definitions. Adversarial models. Reductionist security proofs.

Full-or-part-time: 15h 37m
Theory classes: 5h
Self study : 10h 37m

Symmetric key cryptography

Description:
Symmetric key encryption. Pseudorandom generators. Block ciphers. Message authentication codes.

Full-or-part-time: 15h 38m
Theory classes: 5h
Self study : 10h 38m

Public key encryption

Description:
Definitions and security notions. One way functions. Probabilistic encryption. Main constructions. Homomorphic encryption. Chosen ciphertext security.

Full-or-part-time: 15h 37m
Theory classes: 5h
Self study : 10h 37m

Digital signatures

Description:
Security definitions. RSA and Schnorr signatures.

Full-or-part-time: 15h 38m
Theory classes: 5h
Self study : 10h 38m

Proofs of knowledge and other cryptographic protocols

Description:
Ring signatures. Distributed signatures. Identity and attribute based protocols.

Full-or-part-time: 15h 37m
Theory classes: 5h
Self study : 10h 37m

Multiparty computation

Description:
Secret sharing schemes. Unconditionally and computationally secure multiparty computation.

Full-or-part-time: 15h 38m
Theory classes: 5h
Self study : 10h 38m

GRADING SYSTEM

Exam of coding part (50%) and exam of crypto part (50%). If the average is less than 5 out of 10, there is a chance to pass the subject in a final exam.

EXAMINATION RULES.

All the subjects are important. To pass the course it is required to fulfill all the items.

BIBLIOGRAPHY

Basic:
- Jones, Gareth A.; Jones, J. Mary. Information and coding theory. Springer, 2000. ISBN 9781447103615.
- Delfs, Hans; Knebl, Helmut. Introduction to cryptography : principles and applications. 2nd ed. Berlin: Springer, 2007. ISBN 9783540492436.
- Katz, Jonathan; Lindell, Yehuda. Introduction to modern cryptography : principles and protocols. Boca Raton: Chapman & Hall, 2008. ISBN 9781584885511.
- Ball, Simeon. A Course in algebraic error-correcting codes [on line]. Birkhauser, 2020 [Consultation: 07/07/2023]. Available on: https://ebookcentral-proquest-com.recursos.biblioteca.upc.edu/lib/upcatalunya-ebooks/detail.action?pq-origsite=primo&docID=6194949. ISBN 9783030411534.

Complementary:
- Huffman, W. Cary; Pless, Vera. Fundamentals of error-correcting codes. Cambridge: Cambridge University Press, 2003. ISBN 0521782805.
- Justesen, Jorn; Hoholdt, Tom. A Course in error-correcting codes. Zürich: European Mathematical Society, 2004. ISBN 3037190019.

- Welsh, Dominic. Codes and cryptography. Oxford: Oxford university Press, 1988. ISBN 0198532881.
- Xambó Descamps, Sebastián. Block error-correcting codes : a computational primer. Berlin: Springer, 2003. ISBN 3540003959.
- Goldreich, Oded. Foundations of cryptography : basic tools. New York: Cambridge University Press, 2001. ISBN 0521791723.
- Goldreich, Oded. Foundations of cryptography : basic applications. New York: Cambridge University Press, 2004. ISBN 9780521830843.