Last update: 13-09-2017

34954 - CC - Codes and Cryptography

Coordinating unit: 200 - FME - School of Mathematics and Statistics

Teaching unit: 749 - MAT - Department of Mathematics

Academic year: 2017

Degree: MASTER'S DEGREE IN ADVANCED MATHEMATICS AND MATHEMATICAL ENGINEERING (Syllabus 2010). (Teaching unit Optional)

ECTS credits: 7,5 Teaching languages: English

Teaching staff

Coordinator: MARIA PAZ MORILLO BOSCH

Others: Primer quadrimestre:
SIMEON MICHAEL BALL - A
JAVIER HERRANZ SOTOCA - A
MARIA PAZ MORILLO BOSCH - 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. CALCULUS. Obtain (exact or approximate) solutions for these models with the available resources, including computational means.
3. CRITICAL ASSESSMENT. Discuss the validity, scope and relevance of these solutions; present results and defend conclusions.

Transversal:

4. 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.
5. 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.
6. 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.
7. 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.
8. 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.

Last update: 13-09-2017

34954 - CC - Codes and Cryptography

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

Total learning time: 187h 30m	Hours large group:	60h	32.00%
	Self study:	127h 30m	68.00%

Last update: 13-09-2017

34954 - CC - Codes and Cryptography

Content

Introduction

Learning time: 6h 15m
Theory classes: 2h
Self study : 4h 15m

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

Information and Entropy

Learning time: 18h 45m
Theory classes: 6h
Self study : 12h 45m

Description:
Uncertainty or information. Entropy. Mutual information

Source codes without memory

Learning time: 12h 30m
Theory classes: 4h
Self study : 8h 30m

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

Channel coding

Learning time: 18h 45m
Theory classes: 6h
Self study : 12h 45m

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

Block codes

Learning time: 18h 45m
Theory classes: 6h
Self study : 12h 45m

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

Last update: 13-09-2017

34954 - CC - Codes and Cryptography

Cyclic codes	Learning time: 18h 45m Theory classes: 6h Self study : 12h 45m

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.

Introduction to modern cryptography	Learning time: 15h 37m Theory classes: 5h Self study : 10h 37m

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

Symmetric key cryptography	Learning time: 15h 38m Theory classes: 5h Self study : 10h 38m

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

Public key encryption	Learning time: 15h 37m Theory classes: 5h Self study : 10h 37m

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

Digital signatures	Learning time: 15h 38m Theory classes: 5h Self study : 10h 38m

Description:
Security definitions. RSA and Schnorr signatures.

Last update: 13-09-2017

34954 - CC - Codes and Cryptography

Proofs of knowledge and other cryptographic protocols	Learning time: 15h 37m Theory classes: 5h Self study : 10h 37m
Description: Ring signatures. Distributed signatures. Identity and attribute based protocols.	

Multiparty computation	Learning time: 15h 38m Theory classes: 5h Self study : 10h 38m
Description: Secret sharing schemes. Unconditionally and computationally secure multiparty computation.	

Qualification 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.

Regulations for carrying out activities

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

Last update: 13-09-2017

34954 - CC - Codes and Cryptography

Bibliography

Basic:

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.

Xambó Descamps, Sebastián. Block error-correcting codes : a computational primer. Berlin: Springer, 2003. ISBN 3540003959.

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.

Complementary:

Johnson, Sarah J. Iterative error correction : turbo, low-density parity-check and repeat-accumulate codes. Cambridge: Cambridge University Press, 2010. ISBN 9780521871488.

Welsh, Dominic. Codes and cryptography. Oxford: Oxford university Press, 1988. ISBN 0198532881.

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.