Universidad Zaragoza

Year : 2019/20

27045 - Applied and Computational Algebra

Syllabus Information

Academic Year: 2019/20
Subject: 27045 - Applied and Computational Algebra
Faculty / School: 100 -

Degree: 453 - Degree in Mathematics

ECTS: 6.0
Year: 4
Semester: Second semester
Subject Type: Optional
Module: ---

1.General information

1.1.Aims of the course

1.2.Context and importance of this course in the degree

1.3.Recommendations to take this course

2.Learning goals

2.1.Competences

2.2.Learning goals

2.3.Importance of learning goals

3.Assessment (1st and 2nd call)

3.1.Assessment tasks (description of tasks, marking system and assessment criteria)

4.Methodology, learning tasks, syllabus and resources

4.1.Methodological overview

The methodology followed in this course is oriented towards the achievement of the learning objectives. A wide range of teaching and learning tasks are implemented, such as lectures, practice sessions and computer laboratory sessions.

4.2.Learning tasks

This course is organized as follows:

- **Lectures / practice sessions**. (Two weekly sessions) The teacher will explain the theory contents. These explanations will have to be extended later by the student, with the use of notes and suitable bibliography. The tool Moodle and e-mail will be in use as a form of communication between teacher and student.
- **Computer laboratory sessions**. (Two hours every two weeks). Sage will be used. Resolution of exercises and the production of computer programs.

4.3.Syllabus

This course will address the following topics:

Section I. Cryptography

- **Topic 1**. Introduction to the cryptography.
- **Topic 2**. The Advanced Encryption Standard (AES).
- **Topic 3**. Public-Key Cryptography. The RSA Cryptosystem
- **Topic 4**. Public-Key Cryptosystems based on the Discrete Logarithm Problem.
- **Topic 5**. Elliptic Curve Cryptosystems.
- **Topic 6**. Electronic Signature. The Electronic Identity Card (DNIe).
- **Topic 7**. Hash Functions.

Section II. Error-Correcting Codes

- **Topic 8**. Error-Detector Codes.
- **Topic 9**. Linear Codes.
- **Topic 10**. Encoding and Decoding..
- **Topic 11**. Perfect Codes. The Hamming Codes.
- **Topic 12**. Multiple-Error Correcting Codes: BCH Codes.
- **Topic 13**. Error Burst Correcting Codes: The Reed-Solomon Codes.
- **Topic 14**. Error Correction in RS Codes.
- **Topic 15**. Applications of Error-Correcting Codes.

Section III. Computational Algebra

- **Topic 16**. Introduction to Gröbner.

4.4.Course planning and calendar

Timetable: Wednesday at 10:00-11:00 and Thursday 9:00-11:00.

Computer practices: Wednesday 16:00-18:00, using SAGE and PGP.

Further information concerning the timetable, classroom, office hours, assessment dates and other details regarding this course will be provided on the first day of class or please refer to the Faculty of Sciences website and Moodle.

4.5.Bibliography and recommended resources

- Hardy, Darel W.. Applied algebra : codes, ciphers, and discrete algorithms / Darel W. Hardy, Fred Richman, Carol L. Walker . - 2nd ed. Boca Raton : Chapman & Hall/CRC, cop. 2009
- Pastor Franco, José. Criptografía digital : fundamentos y aplicaciones / José Pastor Franco, Miguel Angel Sarasa López, José Luis Salazar Riaño . - 2a. ed. Zaragoza : Prensas Universitarias de Zaragoza, 2001
- Durán Díaz, Raúl. El criptosistema RSA / Raúl Durán Díaz, Luis Hernández Encinas, Jaime Muñoz Masqué Madrid : Ra-Ma, D.L. 2005
- Klima, Richard. E. [et al.]. Applications of abstract algebra. With Maple and MATLAB . 2nd. Ed. Taylor & Francis. 2006
- Joyner, David. Applied Abstract Algebra. Johns Hopkins. 2004
- Vaudenay, Serge. A Classical Introduction To Cryptography. reprint of 1st ed. 2006 Springer. 2010
- Paar, Christof. Understanding Cryptography. Springer. 2010
- Huppert, Bertram. Lineare Algebra. 2ª ed. Vieweg+teubner Verlag. 2010

http://biblos.unizar.es/br/br_citas.php?codigo=27045&year=2019