Course guide
230300 - COMSECRET - Linear Algebra, Linear Codes and Secret-Sharing Schemes

Last modified: 24/05/2024

Unit in charge: Barcelona School of Telecommunications Engineering
Teaching unit: 749 - MAT - Department of Mathematics.

Degree: BACHELOR'S DEGREE IN TELECOMMUNICATIONS TECHNOLOGIES AND SERVICES ENGINEERING (Syllabus 2015). (Optional subject).
BACHELOR'S DEGREE IN ELECTRONIC ENGINEERING AND TELECOMMUNICATION (Syllabus 2018). (Optional subject).

Academic year: 2024 **ECTS Credits:** 2.0 **Languages:** Catalan

LECTURER

Coordinating lecturer: GERMAN SAEZ MORENO

Others: Primer quadrimestre:
JOSE FABREGA CANUDAS - 10
FRANCISCO JAVIER MUÑOZ LOPEZ - 10
GERMAN SAEZ MORENO - 10

PRIOR SKILLS

Basic concepts and tools from linear algebra.

TEACHING METHODOLOGY

Class hours combine both theoretical and practical sessions. A practical laboratory session is also included.

LEARNING OBJECTIVES OF THE SUBJECT

The aim of the seminar is to provide, by using methods from elementary linear algebra, a brief introduction to some objects and techniques of telecommunications engineering which are central in the design of secure and reliable communications systems, arriving to the approach to edge research problems in these fields. Specifically, we present some basic notions on binary linear error correcting codes and cryptographic protocols for secret sharing schemes as well as an introduction to public key cryptography.

STUDY LOAD

Type	Hours	Percentage
Hours large group	20,0	40.00
Self study	30,0	60.00

Total learning time: 50 h

CONTENTS

Introduction to modular arithmetic.

Description:
Introduction to modular arithmetic putting emphasis in the arithmetic not contained in other courses. Vector space over the finite field of two elements and other finite fields.

Full-or-part-time: 5h
Theory classes: 5h

Introduction to secret sharing schemes.

Description:
Introduction to secret sharing schemes. Linear vectorial schemes over the finite field of two elements. Secret distribution and reconstruction process. Security of the scheme. Authorized subsets of participants. Study of some open problem.

Full-or-part-time: 5h
Theory classes: 5h

Introduction to error correcting codes.

Description:
Introduction to error correcting codes. Linear codes on vector spaces over the finite field of two elements. Generator and control matrices. Encoding and decoding. Hamming distance. Detection and correction of errors.

Full-or-part-time: 5h
Theory classes: 5h

Introduction to cryptography.

Description:
Introduction to cryptography. History. Classical cryptographic methods. Public key cryptography. RSA. Signature and authentication. Final lab work combining the three introduced techniques.

Full-or-part-time: 5h
Theory classes: 5h

GRADING SYSTEM

BIBLIOGRAPHY

Basic:
- Biggs, N.L. Matemática discreta. Barcelona: Vicens-Vives, 1994. ISBN 8431633115.