Last update: 04-07-2019

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

Coordinating unit: 230 - ETSETB - Barcelona School of Telecommunications Engineering

Teaching unit: 749 - MAT - Department of Mathematics

Academic year: 2019

Degree: BACHELOR'S DEGREE IN ELECTRONIC ENGINEERING AND TELECOMMUNICATION (Syllabus 2018). (Teaching unit Optional)
BACHELOR'S DEGREE IN TELECOMMUNICATIONS TECHNOLOGIES AND SERVICES ENGINEERING (Syllabus 2015). (Teaching unit Optional)
BACHELOR'S DEGREE IN AUDIOVISUAL SYSTEMS ENGINEERING (Syllabus 2009). (Teaching unit Optional)
BACHELOR'S DEGREE IN ELECTRONIC SYSTEMS ENGINEERING (Syllabus 2009). (Teaching unit Optional)
BACHELOR'S DEGREE IN TELECOMMUNICATIONS SCIENCE AND TECHNOLOGY (Syllabus 2010). (Teaching unit Optional)
BACHELOR'S DEGREE IN TELECOMMUNICATIONS SYSTEMS ENGINEERING (Syllabus 2010). (Teaching unit Optional)
BACHELOR'S DEGREE IN NETWORK ENGINEERING (Syllabus 2010). (Teaching unit Optional)

ECTS credits: 2 Teaching languages: Catalan

Teaching staff

Coordinator: Sáez Moreno, Germán

Others: Fàbrega Canudas, Josep
Muñoz López, Francisco Javier
Sáez Moreno, Germán

Prior skills

Basic concepts and tools from linear algebra.

Requirements

IMPORTANT: if you have taken previously "Data transmission" subject, then this seminar don't should be taken (after the subject "Data transmission").

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. Specifically, we present some basic notions on binary linear error correcting codes and cryptographic protocols for secret sharing schemes.

Last update: 04-07-2019

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

Study load

Total learning time: 50h	Hours large group:	20h	40.00%
	Hours medium group:	0h	0.00%
	Hours small group:	0h	0.00%
	Guided activities:	0h	0.00%
	Self study:	30h	60.00%

Content

Introduction to modular arithmetic.

Learning time: 5h
Theory classes: 5h

Description:
Introduction to modular arithmetic. Vector space over the finite field of two elements.

Introduction to secret sharing schemes.

Learning time: 5h
Theory classes: 5h

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.

Introduction to error correcting codes.

Learning time: 5h
Theory classes: 5h

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.

Introduction to cryptography.

Learning time: 5h
Theory classes: 5h

Description:
Introduction to cryptography. History. Classical cryptographic methods. Public key cryptography. RSA. Signature and authentication.

Last update: 04-07-2019

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

Bibliography

Basic:

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