

Course guide

330120 - SSCI - Secret and Security in Information Coding

Last modified: 25/04/2024

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

Degree: BACHELOR'S DEGREE IN INDUSTRIAL ELECTRONICS AND AUTOMATIC CONTROL ENGINEERING (Syllabus 2009). (Optional subject).
BACHELOR'S DEGREE IN ICT SYSTEMS ENGINEERING (Syllabus 2010). (Optional subject).
BACHELOR'S DEGREE IN INDUSTRIAL ELECTRONICS AND AUTOMATIC CONTROL ENGINEERING (Syllabus 2016). (Optional subject).

Academic year: 2024 **ECTS Credits:** 6.0 **Languages:** Catalan, English

LECTURER

Coordinating lecturer: MONTSERRAT ALSINA AUBACH

Others: ENRIC VENTURA CAPELL

PRIOR SKILLS

The subject is suitable to complement studies in any industrial or ITIC degree, but it is especially indicated in those related to electronic or digital systems. It does not use advanced mathematics, it only requires knowledge of arithmetic and linear algebra, which will be reviewed and expanded in topic 2.

It is necessary to have a level of oral and written comprehension of English that does not negatively interfere with intercommunication in the classroom.

No technical knowledge of transmission systems is required.

DEGREE COMPETENCES TO WHICH THE SUBJECT CONTRIBUTES

Specific:

1. Ability to know, understand and use the coding of information to ensure security and secrecy in the transmission processes

Transversal:

2. 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.

TEACHING METHODOLOGY

LEARNING OBJECTIVES OF THE SUBJECT

STUDY LOAD

Type	Hours	Percentage
Hours large group	30,0	20.00
Self study	90,0	60.00
Hours small group	30,0	20.00

Total learning time: 150 h

CONTENTS

(ENG) Títol del contingut 1: INTRODUCCIÓ A LA TEORIA DE LA INFORMACIÓ

Full-or-part-time: 20h

Theory classes: 4h

Practical classes: 4h

Self study : 12h

(ENG) Títol del contingut 2: EINES D'ARITMÈTICA MODULAR

Full-or-part-time: 20h

Theory classes: 4h

Practical classes: 4h

Self study : 12h

(ENG) Títol del contingut 3: TEORIA DE CODIS

Full-or-part-time: 60h

Theory classes: 12h

Practical classes: 12h

Self study : 36h

(ENG) Títol del contingut 4: CRIPTOGRAFIA

Full-or-part-time: 50h

Theory classes: 10h

Practical classes: 10h

Self study : 30h

ACTIVITIES

(ENG) TÍTOL DE L'ACTIVITAT 1: PROVA D'AVALUACIÓ CONTÍNUA (CONTINGUTS 1-2)

Full-or-part-time: 6h

Theory classes: 1h 30m

Self study: 4h 30m

(ENG) TÍTOL DE L'ACTIVITAT 2: PROVA D'AVALUACIÓ CONTÍNUA (CONTINGUT 3)

Full-or-part-time: 6h

Theory classes: 1h 30m

Self study: 4h 30m



(ENG) TÍTOL DE L'ACTIVITAT 3: PROVA D'AVALUACIÓ CONTÍNUA (CONTINGUT 4)

Full-or-part-time: 6h
Theory classes: 1h 30m
Self study: 4h 30m

(ENG) TÍTOL DE L'ACTIVITAT 4: TREBALL DE RECERCA (CONTINGUT 1, 2, 3 I 4)

Full-or-part-time: 20h
Theory classes: 4h
Self study: 16h

(ENG) TÍTOL DE L'ACTIVITAT 5: PROVA FINAL (CONTINGUT 1, 2, 3 I 4)

Full-or-part-time: 15h
Theory classes: 3h
Self study: 12h

(ENG) TÍTOL DE L'ACTIVITAT 6: PROVA DE REEVALUACIÓ (CONTINGUT 1, 2, 3 I 4)

GRADING SYSTEM

BIBLIOGRAPHY

Basic:

- Brunat, J. M.; Ventura, Enric. Informació i codis [on line]. Barcelona: Edicions UPC, 2001 [Consultation: 17/11/2020]. Available on: <http://hdl.handle.net/2099.3/36184>. ISBN 8483015285.
- Herrera, Jordi; Domingo, Josep. Criptografia per als serveis telemàtics i el comerç electrònic [on line]. Barcelona: EDIUOC, 1999 [Consultation: 07/06/2024]. Available on: <https://ebookcentral-proquest-com.recursos.biblioteca.upc.edu/lib/upcatalunya-ebooks/detail.action?pq-origsite=primo&docID=7025923>. ISBN 8484290379.
- Rosen, Kenneth H. Discrete mathematics and its applications [on line]. Global ed. Boston: McGraw Hill, 2013 [Consultation: 06/09/2023]. Available on: https://www-ingebook-com.recursos.biblioteca.upc.edu/ib/NPcd/IB_BooksVis?cod_primaria=1000187&codigo_libro=11905. ISBN 9780071315012.

Complementary:

- Adámek, J. Foundations of coding: theory and applications of error-correcting codes, with an introduction to cryptography and information theory. Chichester: John Wiley & Sons, 1991. ISBN 0471621870.
- Hill, Raymond. A first course in coding theory. Oxford: Clarendon Press, 2009. ISBN 0198538030.
- Justesen, Jørn; Høholdt, Tom. A course in error-correcting codes [on line]. 2nd ed. Zürich: European Mathematical Society, 2017 [Consultation: 13/06/2024]. Available on: https://search-ebscobhost-com.recursos.biblioteca.upc.edu/login.aspx?direct=true&AuthType=ip,uid&db=nlebk&AN=1547213&site=ehost-live&ebv=EB&ppid=pp_a. ISBN 3037190019.
- Lin, Shu. Error control coding fundamentals and applications. 2nd ed. Englewood Cliffs: Pearson Prentice-Hall, 2004. ISBN 0130179736.
- McEliece, Robert J. The Theory of information and coding [on line]. Cambridge: Cambridge University Press, 2004 [Consultation: 30/09/2024]. Available on: <https://www-cambridge-org.recursos.biblioteca.upc.edu/core/books/theory-of-information-and-coding/3EF5291C0C1F716387B17284>

[7CFD35FC#](#). ISBN 0521831857.

- MacWilliams, Florence Jessie; Sloane, N. J. A. The theory of error correcting codes. Amsterdam: North-Holland, 2006. ISBN 0444851933.
- Pless, Vera. Introduction to the theory of error-correcting codes. 3rd ed. New York: John Wiley & Sons, 1998. ISBN 0471190470.
- Roman, Steven. Coding and information theory. New York: Springer-Verlag, 1992. ISBN 0387978127.
- Pretzel, Oliver. Error correcting codes and finite fields. Oxford: Clarendon Press, 1992. ISBN 0198596782.
- Xambó Descamps, Sebastián. Block error-correcting codes: a computational primer. Berlin: Springer, 2003. ISBN 3540003959.
- Stinson, D. R. Cryptography: theory and practice. 3rd ed. Boca Raton: CRC Press, 2006. ISBN 1584885084.
- Gonzalez, J.; Rio, A. Introducció a la matemàtica dels sistemes criptogràfics. Barcelona: SCM, 2000.
- Juher, David. Introducció a la criptografia. 2a ed. Girona: Servei de Publicacions de la Universitat de Girona, 2001. ISBN 8484580229.
- Juher, David. L'art de la comunicació secreta: el llenguatge de la criptografia. Barcelona: Llibres de l'Índex, 2004. ISBN 8495317710.
- Rifà Coma, Josep; Huguet Rotger, Llorenç. Comunicación digital: teoría matemática de la información, codificación algebraica, criptología. Barcelona: Masson, 1991. ISBN 8431105763.
- López García, Cándido; Fernández Veiga, Manuel. Teoría de la información y codificación [on line]. Vigo: Universidad de Vigo, 2002 [Consultation: 03/12/2021]. Available on: <http://www.investigacion.biblioteca.uvigo.es/xmlui/bitstream/handle/11093/188/mybook.pdf?sequence=1>. ISBN 8484082202.
- Munuera Gómez, Juan; Tena Ayuso, Juan. Codificación de la información. Valladolid: Universidad, Secretariado de Publicaciones e Intercambio Científico, 1997. ISBN 8477627649.
- Caballero Gil, Pino. Introducción a la criptografía. 2ª ed. Madrid: Ra-Ma, 2002. ISBN 8478975209.
- Córdoba, A. "Felipe II, el diablo y las matemáticas". Saber leer [on line]. enero 2003, no. 161, p. 10-11 [Consultation: 17/11/2020]. Available on: <http://matematicas.uam.es/~antonio.cordoba/miscelanea/ensayos/Felipe%20II.pdf>.
- Pastor, J.; Sarasa, M. A.; Salazar, J. L. Criptografía digital: fundamentos y aplicaciones. 2ª ed. Zaragoza: Publicaciones Universitarias Universidad de Zaragoza, 2001. ISBN 8477335583.
- Sgarro, Andrea. Códigos secretos. Madrid: Pirámide, 1990. ISBN 8436805259.
- Singh, Simon. Los códigos secretos: el arte y la ciencia de la criptografía, desde el antiguo Egipto a la era de internet. Barcelona: Círculo de Lectores, 2000. ISBN 8422685604.