

330120 - SSCI - Secret and Security in Information Coding

Coordinating unit: 330 - EPSEM - Manresa School of Engineering
 Teaching unit: 749 - MAT - Department of Mathematics
 Academic year: 2019
 Degree: BACHELOR'S DEGREE IN ICT SYSTEMS ENGINEERING (Syllabus 2010). (Teaching unit Optional)
 BACHELOR'S DEGREE IN INDUSTRIAL ELECTRONICS AND AUTOMATIC CONTROL ENGINEERING (Syllabus 2016). (Teaching unit Optional)
 BACHELOR'S DEGREE IN INDUSTRIAL ELECTRONICS AND AUTOMATIC CONTROL ENGINEERING (Syllabus 2009). (Teaching unit Optional)
 ECTS credits: 6 Teaching languages: English

Teaching staff

Coordinator: MONTSERRAT ALSINA AUBACH
 Others: ENRIC VENTURA CAPELL

Degree competences to which the subject contributes

Specific:

- (ENG) Capacitat per conèixer, entendre i utilitzar la codificació de la informació per a garantir la seguretat i el secret en els processos de transmissió.

Transversal:

- 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.

Learning objectives of the subject

Study load

Total learning time: 150h	Hours large group:	30h	20.00%
	Hours medium group:	0h	0.00%
	Hours small group:	30h	20.00%
	Guided activities:	0h	0.00%
	Self study:	90h	60.00%

330120 - SSCI - Secret and Security in Information Coding

Content

(ENG) Títol del contingut 1: INTRODUCCIÓ A LA TEORIA DE LA INFORMACIÓ	Learning time: 20h Theory classes: 4h Practical classes: 4h Self study : 12h
(ENG) Títol del contingut 2: EINES D'ARITMÈTICA MODULAR	Learning time: 20h Theory classes: 4h Practical classes: 4h Self study : 12h
(ENG) Títol del contingut 3: TEORIA DE CODIS	Learning time: 60h Theory classes: 12h Practical classes: 12h Self study : 36h
(ENG) Títol del contingut 4: CRIPTOGRAFIA	Learning time: 50h Theory classes: 10h Practical classes: 10h Self study : 30h

330120 - SSCI - Secret and Security in Information Coding

Planning of activities

(ENG) TÍTOL DE L'ACTIVITAT 1: PROVA D'AVALUACIÓ CONTÍNUA (CONTINGUTS 1-2)	Hours: 6h Theory classes: 1h 30m Self study: 4h 30m
(ENG) TÍTOL DE L'ACTIVITAT 2: PROVA D'AVALUACIÓ CONTÍNUA (CONTINGUT 3)	Hours: 6h Theory classes: 1h 30m Self study: 4h 30m
(ENG) TÍTOL DE L'ACTIVITAT 3: PROVA D'AVALUACIÓ CONTÍNUA (CONTINGUT 4)	Hours: 6h Theory classes: 1h 30m Self study: 4h 30m
(ENG) TÍTOL DE L'ACTIVITAT 4: TREBALL DE RECERCA (CONTINGUT 1, 2, 3 I 4)	Hours: 20h Theory classes: 4h Self study: 16h
(ENG) TÍTOL DE L'ACTIVITAT 5: PROVA FINAL (CONTINGUT 1, 2, 3 I 4)	Hours: 15h Theory classes: 3h Self study: 12h
(ENG) TÍTOL DE L'ACTIVITAT 6: PROVA DE REVALUACIÓ (CONTINGUT 1, 2, 3 I 4)	

330120 - SSCI - Secret and Security in Information Coding

Bibliography

Basic:

Brunat, J. M.; Ventura, Enric. Informació i codis [on line]. Barcelona: Edicions UPC, 2001 [Consultation: 25/01/2016]. Available on: <<http://hdl.handle.net/2099.3/36184>>. ISBN 8483015285.

Herrera, Jordi; Domingo, Josep. Criptografia per als serveis telemàtics i el comerç electrònic. Barcelona: EDIUOC, 1999. ISBN 8484290379.

Rosen, Kenneth H. Discrete mathematics and its applications. Global ed. Boston: McGraw Hill, 2013. 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. Zürich: European Mathematical Society, 2004. 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. Cambridge: Cambridge University Press, 2004. 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. Vigo: Universidad de Vigo, 2002. 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: 05/03/2014]. Available on: <<http://matematicas.uam.es/~antonio.cordoba/miscelanea/ensayos/Felipe%20II.pdf>>.

Pastor, J.; Sarasa, M. A.; Salazar, J. L. Criptografia 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.



330120 - SSCI - Secret and Security in Information Coding

Barcelona: Círculo de Lectores, 2000. ISBN 8422685604.