Guia docent
330120 - SSCI - Seguretat i Secret en la Codificació de la Informació

Última modificació: 04/05/2023

Unitat responsable: Escola Politècnica Superior d'Enginyeria de Manresa
Unitat que imparteix: 749 - MAT - Departament de Matemàtiques.

Titulació: GRAU EN ENGINYERIA ELECTRÒNICA INDUSTRIAL I AUTOMÀTICA (Pla 2009). (Assignatura optativa).
GRAU EN ENGINYERIA DE SISTEMES TIC (Pla 2010). (Assignatura optativa).

Curs: 2023 **Crèdits ECTS:** 6.0 **Idiomes:** Català, Anglès

PROFESSORAT

Professorat responsable: MONTSERRAT ALSINA AUBACH

Altres: ENRIC VENTURA CAPELL

CAPACITATS PRÈVIES

L'assignatura és adequada per complementar els estudis en qualsevol grau industrial o de ITIC, però està especialment indicada en aquells relacionats amb sistemes electrònics o digitals. No utilitza matemàtiques avançades, només requereix uns coneixements d'aritmètica i àlgebra lineal, que es revisaran i ampliaran en el tema 2.
Cal que es disposi d'un nivell de comprensió oral i escrita de l'anglès que no interfereixi negativament en la intercomunicació a l'aula.
No es requereixen coneixements tècnics de sistemes de transmissió.

COMPETÈNCIES DE LA TITULACIÓ A LES QUALS CONTRIBUEIX L'ASSIGNATURA

Específiques:
1. Capacitat per conèixer, entendre i utilitzar la codificació de la informació per garantir la seguretat i el secret en els processos de transmissió.

Transversals:
2. TERCERA LLENGUA: Conèixer una tercera llengua, que serà preferentment l'anglès, amb un nivell adequat de forma oral i per escrit i amb consonància amb les necessitats que tindran les titulades i els titulats en cada ensenyament.

METODOLOGIES DOCENTS

L'assignatura consta de quatre hores de classe presencial a l'aula on es combinen la teoria i els problemes amb activitats més aplicades (resolució d'exercicis, discussió de casos pràctics,...), convidant als estudiants a una participació activa.

S'utilitzarà l'anglès com a llengua vehicular a l'aula, integrant-la en la metodologia docent. Així: s'impartiran classes magistrals, classes de problemes en anglès, es consultaran recursos d'informació recomanats en anglès, i es redactaran entregables (exercicis, problemes, suport escrit de presentacions, etc) en anglès.

Existeix la possibilitat, però no l'obligació, de programar algoritmes. En aquest cas, l'alumnat podrà utilitzar el llenguatge de programació que li sigui més còmode.

OBJECTIUS D'APRENENTATGE DE L'ASSIGNATURA

En acabar l'assignatura l'alumnat ha de ser capaç de:

- Comprendre els principis actuals bàsics de la transmissió d'informació i la necessitat de la codificació.

- Utilitzar eines d'aritmètica modular.

- Enumerar i descriure els principals mètodes criptogràfics per protegir la informació i aconseguir confidencialitat, integritat, autenticitat i no repudiació.

- Enumerar i descriure els principals codis detectors i correctos d'errors.

- Elaborar programes que implementin alguns mètodes per codificar i descodificar.

Pel que fa a la competència genèrica en 3a llengua, en acabar l'assignatura a l'alumnat se li hauran donat recursos per a ser capaç de:

- Conéixer terminologia tècnico-científica relativa al contingut de l'assignatura en anglès.
- Llegir i comprendre textos en anglès i material audio relacionats amb el contingut de l'assignatura.
- Resoldre problemes i exercicis en anglès.
- Produir textos tècnics i explicar en anglès continguts relacionats amb l'assignatura.
- Utilitzar l'anglès en la intercomunicació a l'aula, en activitats escrites i/o orals.

HORES TOTALS DE DEDICACIÓ DE L'ESTUDIANTAT

Tipus	Hores	Percentatge
Hores grup petit	30,0	20.00
Hores grup gran	30,0	20.00
Hores aprenentatge autònom	90,0	60.00

Dedicació total: 150 h

CONTINGUTS

Títol del contingut 1: INTRODUCCIÓ A LA TEORIA DE LA INFORMACIÓ

Descripció:
Problema del soroll i la privacitat en els canals de transmissió de la informació. Exemples i vocabulari bàsic.

Dedicació: 20h
Grup gran/Teoria: 4h
Grup mitjà/Pràctiques: 4h
Aprenentatge autònom: 12h

Títol del contingut 2: EINES D'ARITMÈTICA MODULAR

Descripció:
Definicions i conceptes bàsics. Resultats fonamentals d'utilitat en la teoria de codis i la criptografia.

Dedicació: 20h
Grup gran/Teoria: 4h
Grup mitjà/Pràctiques: 4h
Aprenentatge autònom: 12h

Títol del contingut 3: TEORIA DE CODIS

Descripció:
Introducció a la teoria de codis detectors i correctors. Codis de bloc i codis aritmètics. Codis lineals i codis perfectes. Codis de Hamming. Altres codis i aplicacions.

Dedicació: 60h
Grup gran/Teoria: 12h
Grup mitjà/Pràctiques: 12h
Aprenentatge autònom: 36h

Títol del contingut 4: CRIPTOGRAFIA

Descripció:
Principis bàsics de la criptografia i el criptoanàlisi. Criptosistemes de clau privada. Criptosistemes de clau pública.

Dedicació: 50h
Grup gran/Teoria: 10h
Grup mitjà/Pràctiques: 10h
Aprenentatge autònom: 30h

ACTIVITATS

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

Descripció:
Prova individual amb una part dels conceptes teòrics de l'assignatura, resolució d'exercicis i problemes relacionats amb els objectius de l'aprenentatge.

Objectius específics:
En acabar l'activitat, l'alumnat ha de ser capaç de:
Conèixer, comprendre i utilitzar el principis bàsics de la teoria de la informació i l'aritmètica modular.

Material:
Enunciats, taules i calculadora.

Lliurament:
La prova resolta es lliura al professor.
La seva qualificació es denota A1 i representa un 20% de la qualificació final de l'assignatura.

Dedicació: 6h
Grup gran/Teoria: 1h 30m
Aprenentatge autònom: 4h 30m

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

Descripció:
Prova individual amb una part dels conceptes teòrics de l'assignatura, resolució d'exercicis i problemes relacionats amb els objectius de l'aprenentatge.

Objectius específics:
En acabar l'activitat, l'alumnat ha de ser capaç de:
Conèixer i comprendre el funcionament dels codis detectors i correctors d'errors.

Material:
Enunciats, taules i calculadora.

Lliurament:
La prova resolta es lliura al professor.
La seva qualificació es denota A2 i representa un 20% de la qualificació final de l'assignatura.

Dedicació: 6h
Grup gran/Teoria: 1h 30m
Aprenentatge autònom: 4h 30m

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

Descripció:
Prova individual amb una part dels conceptes teòrics de l'assignatura, resolució d'exercicis i problemes relacionats amb els objectius de l'aprenentatge.

Objectius específics:
En acabar l'activitat, l'estudianta o estudiant ha de ser capaç de:
Conèixer i comprendre el funcionament dels criptosistemes per xifrar i desxifrar.

Material:
Enunciats, taules i calculadora.

Lliurament:
La prova resolta es lliura al professor.
La seva qualificació es denota A3 i representa un 20% de la qualificació final de l'assignatura.

Dedicació: 6h
Grup gran/Teoria: 1h 30m
Aprenentatge autònom: 4h 30m

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

Descripció:
Individualment o per parelles, fora de l'aula, caldrà realitzar un petit treball de recerca sobre un contingut relacionat amb l'assignatura. S'entregarà una memòria escrita i es farà una presentació oral del treball.

Objectius específics:
Recerca de la informació, comunicació oral, tercera llengua.

Material:
Bibliografia i internet.

Lliurament:
Comunicació oral a classe amb suport multimèdia.
La seva qualificació es denota A4 i representa un 40% de la qualificació final de l'assignatura.

Dedicació: 20h
Grup gran/Teoria: 4h
Aprenentatge autònom: 16h

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

Descripció:
Prova individual que mostri l'assoliment global dels conceptes de l'assignatura.

Objectius específics:
Avaluar l'assoliment general dels objectius dels continguts 1, 2 3 i 4.

Lliurament:
La prova o treball es lliura al professor.
La seva qualificació es denota A5 i representa un 60% de la qualificació final de l'assignatura.

Dedicació: 15h
Grup gran/Teoria: 3h
Aprenentatge autònom: 12h

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

Descripció:
Prova individual que mostri l'assoliment global dels conceptes de l'assignatura.
Només la poden realitzar els alumnes que hagin obtingut la qualificació de 'suspens' en el període ordinari d'avaluació. No la poden realitzar aquell alumnes que tinguin un 'no presentat' o hagin aprovat l'assignatura en el període ordinari d'avaluació.

Objectius específics:
Reavaluar l'assoliment general dels objectius dels continguts 1, 2, 3 i 4.

Lliurament:
La prova o treball es lliura al professor.
La seva qualificació es denota A6 i es té en compte en el procés de reavaluació.

SISTEMA DE QUALIFICACIÓ

Activitat 1 : A1= 20% de la nota de l'assignatura
Activitat 2 : A2= 20% de la nota de l'assignatura
Activitat 3 : A3= 20% de la nota de l'assignatura
Activitat 4 : A4= 40% de la nota de l'assignatura
Activitat 5 : A5= 60% de la nota de l'assignatura
Si un alumne no realitza alguna de les activitats, la seva qualificació en aquesta activitat serà 0.

L'alumat té opció a millorar la qualificació de les activitats (Activitat 1 ,2 i 3) realitzant l'activitat 5.

La nota final serà: NF= Max (0.2 A1 + 0.2 A2 + 0.2 A3 , 0.6A5) + 0.4 A4

L'avaluació del nivell assolit de la competència genèrica en tercera llengua s'efecturarà seguint el criteri dels tres nivells que indiquen les graelles de mesura, A (ben assolit), B (assolit), C (no assolit), en consonància amb els criteris d'avaluació que s'aprovin a l'EPSEM.

Procés de reavaluació:

L' alumnat que hagi obtingut la qualificació de 'suspens' en el període ordinari d'avaluació pot accedir al procés de reavaluació, realitzant l'activitat 6. No poden accedir-hi aquells alumnes que tinguin un 'no presentat' o hagin aprovat l'assignatura en el període ordinari d'avaluació.

La nota final reavaluada de l'assignatura no pot superar el 5 i es calcula:

NFR= mínim { 5 , 0.4 A4 + 0.6 A6}

BIBLIOGRAFIA

Bàsica:
- Rosen, Kenneth H. Discrete mathematics and its applications [en línia]. Global ed. Boston: McGraw Hill, 2013 [Consulta: 06/09/2023]. Disponible a: https://www-ingebook-com.recursos.biblioteca.upc.edu/ib/NPcd/IB_BooksVis?cod_primaria=1000187&codigo_libro=11905. ISBN 9780071315012.
- Brunat, J. M.; Ventura, Enric. Informació i codis [en línia]. Barcelona: Edicions UPC, 2001 [Consulta: 17/11/2020]. Disponible a: 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.

Complementària:
- 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 [en línia]. Vigo: Universidad de Vigo, 2002 [Consulta: 03/12/2021]. Disponible a: http://www.investigo.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 [en línia]. enero 2003, no. 161, p. 10-11 [Consulta: 17/11/2020]. Disponible a: 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 criptografia, desde el antiguo Egipto a la era de internet. Barcelona: Círculo de Lectores, 2000. ISBN 8422685604.