

Informació i Seguretat

Codi: 102769
Crèdits: 6

Titulació	Tipus	Curs	Semestre
2502441 Enginyeria Informàtica	OB	2	2

Professor de contacte

Nom: Cristina Fernández Córdoba
Correu electrònic: Cristina.Fernandez@uab.cat

Utilització d'idiomes a l'assignatura

Llengua vehicular majoritària: català (cat)
Grup íntegre en anglès: No
Grup íntegre en català: Sí
Grup íntegre en espanyol: No

Equip docent

Josep Rifà Coma
Joan Serra Sagristà

Prerequisits

No hi ha prerequisits. En tot cas és aconsellable que l'estudiant domini les qüestions més bàsiques d'algorísmica i programació. També és convenient que l'estudiant tingui nocions d'àlgebra lineal, anàlisi matemàtica i probabilitats.

Objectius

L'assignatura "Informació i Seguretat" forma part de la **MATÈRIA 9 : ALGORÍSMICA I INFORMACIÓ**. Alguns dels temes dels quals s'ocupa són: mesurar la informació; codificació de la font i del canal; criptografia; privacitat, autenticitat i accessibilitat; infraestructura de clau pública (PKI), etc.

Competències

- Adquirir hàbits de pensament.
- Capacitat per concebre, redactar, organitzar, planificar, desenvolupar i signar projectes en l'àmbit de l'enginyeria informàtica que tinguin per objecte la concepció, el desenvolupament o l'explotació de sistemes, serveis i aplicacions informàtiques.
- Capacitat per dissenyar, desenvolupar, seleccionar i avaluar aplicacions i sistemes informàtics, assegurant-ne la fiabilitat, la seguretat i la qualitat, d'acord amb els principis ètics i la legislació i la normativa vigents.
- Conèixer i aplicar els procediments algorítmics bàsics de les tecnologies informàtiques per dissenyar solucions a problemes i per analitzar la idoneïtat i la complexitat dels algoritmes proposats.
- Tenir una actitud personal adequada.

Resultats d'aprenentatge

1. Desenvolupar el pensament sistèmic.
2. Desenvolupar la curiositat i la creativitat.
3. Dissenyar, desenvolupar, seleccionar i avaluar aplicacions, assegurant la seva fiabilitat i seguretat.
4. Gestionar la informació incorporant de manera crítica les innovacions del propi camp professional, i analitzar les tendències de futur.
5. Identificar els principals atacs que pot rebre un sistema informàtic, així com els possibles mètodes de protecció, detecció i aplicació de polítiques de seguretat que permetin evitar el dany al sistema o minimitzar la seva repercussió.
6. Identificar la complexitat computacional d'un algorisme en termes de recursos de memòria i temps d'execució.

Continguts

1. Motivació. Planteig dels problemes de la comunicació (1 hora)
 1. Esquema de comunicació. Elements.
 2. Soroll, errors de transmissió.
 3. Espies: privacitat i autenticitat.
2. Conceptes bàsics de teoria de la informació (4 hores)
 1. Mesura de la informació.
 2. Model de Shannon de font discreta sense memòria.
 3. Entropia d'una variable aleatòria discreta.
 4. Informació mútua entre dues v.a. discretes. Capacitat d'un canal.
3. Codificació de la font (3 hores)
 1. Codis de longitud fixa, variable, a descodificació única i instantanis.
 2. Primer teorema de Shannon. Existència de codis òptims.
 3. Construcció de codis òptims: mètode de Huffman.
4. Compressió de dades (3 hores)
 1. Tipus de compressió.
 2. Mètodes estadístics i tècniques de diccionari.
5. Codificació del canal (3 hores)
 1. Models importants de canals discrets sense memòria.
 2. Regles de descodificació.
 3. Segon teorema de Shannon.
6. Codis detectors i correctors d'errors (4 hores)
 1. Codificació. Codis bloc. Errors.
 2. Codis binaris lineals. Paràmetres.
 3. Matrius generadora i de control.

4. Descodificació.
5. Alguns codis importants.
7. Criptografia i seguretat (8 hores)
 1. Conceptes bàsics. Seguretat i autenticitat.
 2. Criptografia de clau simètrica.
 3. Criptografia de clau pública.
 4. Certificats digitals i infraestructures de clau pública.

Metodologia

Les classes de teoria es basaran en lliçons magistrals, si bé s'intentarà fomentar la participació de l'estudiant en la resolució d'exemples, etc. A les classes de problemes, se seguirà una llista d'exercicis que l'estudiant intentarà resoldre pel seu compte. Es fomentarà l'exposició de la resolució de problemes per part dels estudiants. En les sessions de pràctiques es tractaran en profunditat temes relacionats: plantejament de casos reals, ampliació de determinats temes amb tècniques i algorismes alternatius als ja vistos. Es farà servir el Campus Virtual com a mitjà de comunicació del professor cap als estudiant (material, notícies, etc.).

Competències transversals. Seran treballades i avaluades en diversos moments al llarg del curs. Concretament:

- **T01.04 - Desenvolupar el pensament sistèmic:** Al llarg de tot el curs, considerem les diferents parts que intervenen en un sistema de transmissió de la informació i veurem com estan relacionades entre elles. L'avaluació d'aquesta competència està inclosa en l'avaluació de la resolució d'exercicis i en les proves parcials i final.
- **T06.02 - Desenvolupar la curiositat i la creativitat:** Especialment en la resolució de reptes que es poden presentar al llarg del curs com a la resolució de problemes es pretén desenvolupar la curiositat i és necessària la creativitat per portar a terme la resolució.
- **T06.04 - Gestionar la informació incorporant de manera crítica les innovacions del propi camp professional, i analitzar les tendències de futur:** En la realització de les pràctiques és necessari fer ús de tècniques que s'estan fent servir avui dia. En aquesta part valorem quines són les tendències de futur i com es fan servir en la resolució de les pràctiques.

Activitats formatives

Títol	Hores	ECTS	Resultats d'aprenentatge
Tipus: Dirigides			
Classes de problemes	12	0,48	1, 3, 5, 6
Classes de teoria	26	1,04	1, 3, 5, 6
Pràctiques obligatòries	12	0,48	1, 2, 3, 4, 5, 6
Tipus: Supervisades			
Tutories i consultes	17	0,68	1, 3, 5, 6
Tipus: Autònomes			
Preparació de problemes i pràctiques	25	1	1, 3, 5, 6
Preparació examen final	25	1	1, 3, 5, 6

Avaluació

Les dates d'avaluació continuada es publicaran al campus virtual i a les transparències de presentació de l'assignatura i poden estar subjectes a canvis de programació per motius d'adaptació a possibles incidències. Sempre s'informarà al campus virtual sobre aquests canvis ja que s'entén que aquesta és la plataforma habitual d'intercanvi d'informació entre professors i estudiants.

L'avaluació de l'assignatura, sobre 10 punts, es farà de la forma següent:

- Dues **proves parcials individuals, 6 punts** (3 punts cadascuna). Com a part de l'avaluació continuada la primera prova es farà en hores de teoria i la segona en la data especificada per la coordinació. La primera prova parcial es realitzarà en finalitzar els primers cinc capítols del curs, i la segona prova parcial en finalitzar tots els capítols del curs. Aquestes proves individuals consistiran majoritàriament en exercicis a l'estil dels que s'han anat fent durant el curs; una part menor consistirà en qüestions més teòriques. Cal obtenir almenys 2.4 punts (dels 6 punts) per poder superar l'assignatura.
- **Resolució d'exercicis, 1.5 punts**. Com a part de l'avaluació continuada, s'hauran de realitzar activitats o resoldre exercicis.
- **Pràctiques obligatòries, 2.5 punts**. Com a part de l'avaluació continuada, s'hauran de resoldre algunes pràctiques en el Laboratori Integrat. Cal obtenir almenys 1 punt (dels 2.5 punts) per poder superar l'assignatura.
- **Examen final, 6 punts**. Aquells estudiants que no hagin superat l'assignatura arran de les proves parcials individuals tindran l'opció de presentar-se a l'examen final per recuperar tota la matèria de l'assignatura. Per tant, no hi ha recuperació dels parcials per separat sinó que l'examen és de tot el curs. Aquesta prova individual consistirà majoritàriament en exercicis a l'estil dels que s'han anat fent durant el curs; una part menor consistirà en qüestions més teòriques. Cal obtenir almenys 2.4 punts per poder superar l'assignatura.

En les proves parcials, l'examen final, la resolució d'exercicis i les pràctiques es valoraran els coneixements adquirits de la matèria així com el pensament lògic i sistemàtic en la resolució d'exercicis fent servir aquests coneixements.

En el cas d'estudiants repetidors, es podrà validar la nota de les pràctiques del curs anterior, sempre que aquesta sigui superior o igual a 1.25 (sobre 2.5).

Sense perjudici d'altres mesures disciplinàries que s'estimin oportunes, i d'acord amb la normativa acadèmica vigent, les irregularitats comeses per un estudiant que puguin conduir a una variació de la qualificació es qualificaran amb un zero (0). Les activitats d'avaluació qualificades d'aquesta forma i per aquest procediment no seran recuperables. Si és necessari superar qualsevol d'aquestes activitats d'avaluació per aprovar l'assignatura, aquesta assignatura quedarà suspesa directament, sense oportunitat de recuperar-la en el mateix curs. Aquestes irregularitats inclouen, entre d'altres:

- la còpia total o parcial d'una pràctica, informe, o qualsevol altra activitat d'avaluació;
- deixar copiar;
- presentar un treball de grup no fet íntegrament pels membres del grup;
- presentar com a propis materials elaborats per un tercer, encara que siguin traduccions o adaptacions, i en general treballs amb elements no originals i exclusius de l'estudiant;
- tenir dispositius de comunicació (com telèfons mòbils, smart watches, etc.) accessibles durant les proves d'avaluació teórico-pràctiques individuals (exàmens).

Per aprovar és necessari que l'avaluació de cadascuna de les parts superi el mínim exigít i que l'avaluació total superi els 5 punts. En cas de no superar l'assignatura degut a que alguna de les activitats d'avaluació no arriba a la nota mínima requerida, la nota numèrica de l'expedient serà el valor menor entre 4.5 i la mitjana ponderada de les notes. Amb les excepcions de que s'atorgarà la qualificació de "no avaluable" als estudiants que no participin en cap de les activitats d'avaluació, i de que la nota numèrica de l'expedient serà el valor menor entre 3.0 i la mitjana ponderada de les notes en cas que l'estudiant hagi comès irregularitats en un acte d'avaluació (i per tant no serà possible l'aprovat per compensació). Per poder obtenir una MH la nota final ha

de ser igual o superior als 9 punts. Com que el nombre de MH no pot superar el 5% dels estudiants matriculats, es concediran als estudiants que tinguin les notes finals més altes. En cas d'empat, es tindran en compte les resolucions de les proves parcials.

És important tenir en compte que no es farà cap activitat d'avaluació a cap alumne en un horari diferent de l'establert si no existeix una causa justificada, s'ha avisat amb anterioritat a l'activitat i el professor ha donat el seu consentiment. En qualsevol altre cas, si un alumne no ha assistit a una activitat, aquesta no es pot recuperar.

Podeu consultar la normativa acadèmica de la UAB aprovada pel Consell de Govern de la UAB:
http://webs2002.uab.es/afers_academics/info_ac/0041.htm

Activitats d'avaluació

Títol	Pes	Hores	ECTS	Resultats d'aprenentatge
Examen final	6	2	0,08	1, 3, 4, 5, 6
Pràctiques obligatòries	2.5	2	0,08	1, 2, 3, 4, 5, 6
Proves individuals d'avaluació continuada	6	3	0,12	1, 3, 6
Resolució d'exercicis	1.5	1	0,04	1, 3, 5, 6

Bibliografia

Bibliografia bàsica

- L. Huguet i J. Rifà. *Comunicación Digital*. Ed. Masson, 1991.
- David Salomon: *Data compression - The Complete Reference*, 4th Edition. Springer 2007.
- R.B. Ash. *Information Theory*. John Wiley and Sons Inc, 1965.
- Gil Alvarez. *Teoría matemática de la información*. Ediciones ICE, 1981.
- T.C. Bell, J.G. Cleary i I.H. Witten. *Text Compression*. Prentice Hall, 1990.
- Josep Domingo i Ferrer and Jordi Herrera i Joancomartí, *Criptografia per als Serveis Telemàtics i el Comerç Electrònic*, Col·lecció Manuals no. 31, Barcelona: Editorial UOC, 1999. ISBN 84-8429-007-7.
- A. Menezes, P. van Oorschot and S.Vanstone.: *Handbook of Applied Cryptography*, CRC Press. (1996). Available at <http://www.cacr.math.uwaterloo.ca/hac> .

Bibliografia complementària

- C.E. Shannon, "A mathematical theory of communications," *Bell Syst. Tech. J.*, 27, 379-423, 1948.
- B. McMillan, "The basic theorems of Information Theory," *Ann. Math. Stat.*, 24, 196-219, 1953.
- A.I. Khinchin. *Mathematical foundations of Information Theory*. Dover Publications, Inc., 1957.
- Richard W. Hamming. *Coding and Information Theory*. Prentice Hall, Inc., 1980.
- Masud Mansuripur. *Introduction to Information Theory*. Prentice Hall, Inc., 1987.
- G.J. Chaitin. *Algorithmic Information Theory*. Cambridge University Press., 1987.
- *An Introduction to Computer Security: The NIST Handbook*. Special Publication 800-12. NIST(1995). <http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf>
- Robling Denning D.E.: *Cryptography and Data Security*. Addison-Wesley Publishing Company (1988).
- Schneier, B.: *Applied Criptography*, John Wiley and Sons, Inc. 1996.
- Simmons, G.S.: *Contemporary Criptology. The Science of Information Integrity*, IEEEPress (1991).
- Anderson, R.: *Security Engineering: A Guide to Building Dependable Distributed System*,Wiley (2001).
- Pfleeger, C.P.: *Security in Computing*. , Prentice Hall (1997).
- V. Shoup. : *A computational Introduction tonumber theory and Algebra*. <http://shoup.net/ntb/>