Informació i Seguretat 2014/2015

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 de llengües

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

Equip docent

Joaquim Borges Ayats
Jaume Pujol Capdevila
Jordi Herrera Joancomarti

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.

Resultats d'aprenentatge

1. Desenvolupar el pensament sistèmic.
2. Dissenyar, desenvolupar, seleccionar i avaluar aplicacions, assegurant la seva fiabilitat i seguretat.

3. 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.
4. 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 infrastructures 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.

Activitats dirigides (33%)

Exposició per part del professor dels conceptes i tècniques bàsics de la matèria, amb indicacions de com completar el seu aprenentatge i aprofundir-hi.

Resolució de problemes i casos a classe que treballin els conceptes explicats pel professor. La participació de l'estudiant haurà de ser activa, proposant solucions, analitzant críticament les solucions proposades, i presentant nous enfocs del problema.

Sessions en laboratoris en les quals l'estudiant posarà en pràctica els coneixements adquirits i s'exercitarà en el maneig de l'equipamient HW/SW propi de la matèria.

Activitats autònomes (50%)

Estudi individual de l'estudiant, preparació d'esquemes, mapes conceptuals, resums, etc.

Recerca i consulta de la bibliografia pròpia del tema.

Resolució individual o en grups reduïts de problemes i casos, fora de l'entorn de l'aula.

Activitats supervisades (12%)

Preparació per part de l'estudiant d'accions i treballs, sota la tutela del professor.

Tutories en grup i individuals

Activitats d'avaluació (5%)

Proves individuals i grupals que constatin l'adquisició per part de l'estudiant dels resultats d'aprenentatge esperats.

Es valoraran també altres accions d'avaluació el desenvolupament de les quals s'inclou en les activitats dirigides, autònomes i supervisades.

Activitats formatives

Títol	Hores	ECTS	Resultats d'aprenentatge
Tipus: Dirigides			
Classes de problemes	12	0,48	1, 2, 3, 4
Classes de teoria	26	1,04	1, 2, 3, 4

Pràctiques Obligatòries	12	0,48	1, 2, 3, 4
Tipus: Supervisades			
Tutories i consultes	17	0,68	1, 2, 3, 4
Tipus: Autònomes			
Preparació de problemes i pràctiques	25	1	1, 2, 3, 4
Preparació examen final	25	1	1, 2, 3, 4
Treball personal	25	1	1, 2, 3, 4

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, aquestes proves es realitzaran durant les sessions de teoria. 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 per poder superar l'assignatura.

-Resolució d'exercicis, 1.5 punts. Com a part de l'avaluació continuada, es lliurarà la resolució d'activitats o exercicis a classe. Per a la resolució d'aquesta part, es pot fer ús de material en format paper (apunts de l'assignatura, material extra, llistat de problemes, llibres, etc.).

-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 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. 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.

Obtindran la qualificació de "No Presentat" aquells estudiants que no es presentin a cap de les proves individuals (ni les proves parcials ni l'examen final). La participació en alguna d'aquestes activitats d'avaluació suposarà rebre una qualificació diferent de "No Presentat". En el cas de no arribar al mínim exigit en alguna de les activitats d'avaluació, si el càlcul de la nota final és igual o superior a 5, es posarà un 4,5 de nota a l'expedient.

Normativa d'avaluació de la UAB aprovada pel Consell de Govern de la UAB (30/09/2010): http://webs2002.uab.es/afers_academics/info_ac/0036.htm

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). Per exemple, plagiar, copiar, deixar copiar, ..., una activitat d'avaluació, implicarà suspendre aquesta activitat d'avaluació 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.

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.

Activitats d'avaluació

Títol	Pes	Hores	ECTS	Resultats d'aprenentatge
Examen Final	6	2	0,08	1, 2, 3, 4
Proves Individuals Avaluació Continuada	6	3	0,12	1, 2, 3, 4
Pràctiques Obligatòries	2.5	2	0,08	1, 2, 3, 4
Resolucio Exercicis	1.5	1	0,04	1, 2, 3, 4

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/