UAB
Universitat Autònoma de Barcelona

Informació i Seguretat

2026/2027

Codi: 102769
Crèdits: 6

Titulació	Tipus	Curs
Enginyeria Informàtica	OB	2

Professor/a de contacte

Nom : Cristina Fernandez Cordoba

Correu electrònic : cristina.fernandez@uab.cat

Equip docent

Ester Jara Lorente

Adrià Figuerola Torrell

Pau Quintas Torra

Julián Salas Piñón

Natàlia Blasco Andreo

Marc Caravaca Rodriguez

Idiomes dels grups

Podeu consultar aquesta informació al final del document.

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

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.

Resultats d'aprenentatge

- (CM17) Integrar metodologies de criptografia, compressió i codificació en la resolució de problemes informàtics.
- (KM18) Explicar els conceptes de criptografia, de codificació i de compressió de dades en el marc de la teoria de la informació en la resolució de problemes.
- (SM22) Analitzar serveis, aplicacions i sistemes informàtics des de la perspectiva de la teoria de la informació.

Continguts

1. Motivació. Planteig dels problemes de la comunicació (1 hora)

- Esquema de comunicació. Elements.
- Soroll, errors de transmissió.
- Espies: privacitat i autenticitat.

2. Conceptes bàsics de teoria de la informació (4 hores)

- Mesura de la informació.
- Model de Shannon de font discreta sense memòria.
- Entropia d'una variable aleatòria discreta.
- Informació mútua entre dues v.a. discretes. Capacitat d'un canal.

3. Codificació de la font (3 hores)

- Codis de longitud fixa, variable, a descodificació única i instantanis.
- Primer teorema de Shannon. Existència de codis òptims.
- Construcció de codis òptims: mètode de Huffman.

4. Compressió de dades (3 hores)

- Tipus de compressió.
- Mètodes estadístics i tècniques de diccionari.

5. Codificació del canal (3 hores)

- Models importants de canals discrets sense memòria.
- Regles de descodificació.
- Segon teorema de Shannon.

6. Codis detectors i correctors d'errors (4 hores)

- Codificació. Codis bloc. Errors.
- Codis binaris lineals. Paràmetres.
- Matrius generadora i de control.
- Descodificació.
- Alguns codis importants.

7. Criptografia i seguretat (8 hores)

- Conceptes bàsics. Seguretat i autenticitat.
- Criptografia de clau simètrica.
- Criptografia de clau pública.
- Certificats digitals i infraestructures de clau pública.

Activitats formatives i Metodologia

Títol	Hores	ECTS	Resultats d'aprenentatge
Tipus: Autònoma			
Preparació de problemes i pràctiques	25	1	CM17, SM22
Preparació examen final	25	1	CM17, KM18, SM22
Treball personal	25	1	CM17, SM22

Tipus: Dirigida			
Classes de problemes	12	0,48	CM17, KM18
Classes de teoria	26	1,04	CM17, KM18, SM22
Pràctiques obligatòries	12	0,48	SM22
Tipus: Supervisada			
Tutories i consultes	17	0,68	KM18

Les classes de teoria es basaran en lliçons magistrals, si bé s'intentarà fomentar la participació de l'alumnat 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 de l'alumnat. 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 professorat cap a l'alumnat (material, notícies, etc.).

Nota: es reservaran 15 minuts d'una classe, dins del calendari establert pel centre/titulació, perquè l'alumnat completi les enquestes d'avaluació de l'actuació del professorat i d'avaluació de l'assignatura.

Avaluació

Activitats d'avaluació continuada

Títol	Pes	Hores	ECTS	Resultats d'aprenentatge
Examen final	6	2	0,08	CM17, KM18, SM22
Proves individuals d'avaluació continuada	6	3	0,12	CM17, KM18, SM22
Pràctiques obligatòries	2.5	2	0,08	SM22
Resolució d'exercicis	1.5	1	0,04	CM17, SM22

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 professorat i alumnat.

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. Cal obtenir almenys 3 punts (dels 6 punts) de mitja dels dos parcials per poder superar l'assignatura.
- Resolució d'exercicis, 1.5 punts. Com a part de l'avaluació continuada, s'hauran de realitzar activitats o bé resoldre exercicis via qüestionaris en línia. En algun cas es podria programar alguna altra activitat d'avaluació i es posarà en coneixement de l'alumnat a través del Campus Virtual.
- Pràctiques obligatòries, 2.5 punts. Com a part de l'avaluació continuada, s'hauran de realitzar pràctiques en grup en el laboratori. Les qualificacions de les pràctiques es validaran a l'aula o, en cas de dubte, mitjançant un examen final. Cal obtenir almenys 1 punt (dels 2.5 punts) per poder superar l'assignatura.

- Examen final, 6 punts. Qui no hagi superat l'assignatura arran de les proves parcials individuals i tingui almenys 1 punt (dels 2.5 punts) de les pràctiques, tindrà 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. Cal obtenir almenys 3 punts (dels 6 punts) per poder superar l'assignatura.

Activitats que no es poden recuperar:

D'acord amb la coordinació del Grau i la direcció de l'Escola d'Enginyeria les activitats següents no es podran recuperar:

- Resolució d'exercicis.
- Pràctiques obligatòries.

Alumnat repetidor:

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).

Integritat acadèmica:

Sense perjudici d'altres mesures disciplinàries que s'estimin oportunes, i d'acord amb la normativa acadèmica vigent, les activitats d'avaluació (pràctiques, problemes o exàmens) amb irregularitats comeses per un/a estudiant que puguin conduir a una variació de la qualificació es qualificaran íntegrament 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 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;
- l'ús no autoritzat de la IA (p. ex, Copilot, ChatGPT o equivalents);
- tenir dispositius de comunicació (com telèfons mòbils, smart watches, etc.) accessibles durant les proves d'avaluació teorico-pràctiques individuals (exàmens).

Per aprovar és necessari que l'avaluació de cadascuna de les parts superi el mínim exigit 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" a qui no participi 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 s'hagi comès irregularitats en un acte d'avaluació (i per tant no serà possible l'aprovat per compensació).

En aquesta assignatura, no es permet l'ús de tecnologies d'Intel·ligència Artificial (IA) en cap de les seves fases. Qualsevol treball que inclogui fragments generats amb IA serà considerat una falta d'honestedat acadèmica i pot comportar una penalització parcial o total en la nota de l'activitat, o sancions majors en casos de gravetat.

Matrícules d'honor:

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% del nombre d'estudiants matriculats, es concediran a qui tingui les notes finals més altes. En cas d'empat, es tindran en compte les resolucions de les proves parcials.

Realització i revisió de les activitats d'avaluació:

És important tenir en compte que els casos en que es pot demanar una reprogramació d'una prova, i el procediment per fer-ho, està descrit a:
https://www.uab.cat/ca/enginyeria/doc/criteris-avaluacio-esola-enginyeria.pdf.

En el cas d'avaluacions en línia de qüestionaris, es podrà demanar una revisió posteriorment a la data de tancament del qüestionari. Per a la resta d'activitats d'avaluació, s'indicarà un lloc, data i hora de revisió en la que l'estudiant podrà revisar l'activitat amb el/la professor/a. En aquest context, es podran fer reclamacions sobre la nota de l'activitat, que seran avaluades pel professorat responsable de l'assignatura. Si l'estudiant no es presenta a aquesta revisió, no es revisarà posteriorment aquesta activitat.

Avaluació única:

Aquesta assignatura no preveu avaluació única.

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

Bibliografia

Bibliografia bàsica

- L. Huguet i J. Rifà. Comunicación Digital. Ed. Masson, 1991.
- D. Salomon: Data compression - The Complete Reference, 4th Edition. Springer 2007.
- R.B. Ash. Information Theory. John Wiley and Sons Inc, 1965.
- G. Alvarez. Teoría matemática de la información. Ediciones ICE, 1981.
- T.C. Bell, J.G. Cleary i I.H. Witten. Text Compression. Prentice Hall, 1990.
- J. Herrera-Joancomartí, C. Pérez-Solà, La criptografia que et cal saber. 2023. Available at https://criptografia.cat.
- 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.
- R. W. Hamming. Coding and Information Theory. Prentice Hall, Inc., 1980.
- M. 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
- D. E. Robling Denning. Cryptography and Data Security. Addison-Wesley Publishing Company (1988).
- B. Schneier. Applied Criptography, John Wiley and Sons, Inc. 1996.
- G.S. Simmons. Contemporary Criptology. The Science of Information Integrity, IEEEPress (1991).
- R. Anderson. Security Engineering: A Guide to Building Dependable Distributed System,Wiley (2001).
- C.P. Pfleeger. Security in Computing. , Prentice Hall (1997).
- V. Shoup. A computational Introduction to number theory and Algebra. http://shoup.net/ntb/

Programari

Les activitats pràctiques es realitzaran en un entorn dockeritzat, amb un contenidor de Jupyter Notebook que contindrà com a kernel una de les últimes versions de SageMath.

- SageMath és un sistema de programari de matemàtiques de codi obert gratuït amb llicència GPL. Es basa en molts paquets de codi obert existents: NumPy, SciPy, matplotlib, Sympy, Maxima, GAP, FLINT, R i molts més. S'accedeix a la seva potència combinada mitjançant un llenguatge comú basat en Python o directament mitjançant interfícies. Des de la versió 9.0 publicada el gener del 2020, SageMath utilitza Python 3. (https://www.sagemath.org/)
- Jupyter Notebook és un projecte dirigit per la comunitat amb l'objectiu de "desenvolupar programari de codi obert, estàndards oberts i serveis per a la informàtica interactiva en dotzenes de llenguatges de programació". (https://jupyter.org/)
- Docker és un projecte de codi obert que automatitza el desplegament d'aplicacions dins de contenidors de programari, proporcionant així una capa addicional d'abstracció i automatització de virtualització d'aplicacions en diferents sistemes operatius. (https://www.docker.com/resources/what-container/)

Grups i idiomes de l'assignatura

La informació proporcionada és provisional fins al 30 de novembre. A partir d'aquesta data, podreu consultar l'idioma de cada grup a través d'aquest enllaç. Per accedir a la informació, caldrà introduir el CODI de l'assignatura

Tipus de docència	Grup	Idioma	Semestre	Torn
(TE) Teoria	41	Anglès	segon quadrimestre	matí-mixt
(TE) Teoria	43	Català/Castellà	segon quadrimestre	matí-mixt
(TE) Teoria	45	Català/Castellà	segon quadrimestre	tarda
(TE) Teoria	47	Català/Castellà	segon quadrimestre	matí-mixt
(PAUL) Pràctiques d'aula	411	Anglès	segon quadrimestre	matí-mixt
(PAUL) Pràctiques d'aula	412	Anglès	segon quadrimestre	matí-mixt
(PAUL) Pràctiques d'aula	431	Català/Castellà	segon quadrimestre	matí-mixt
(PAUL) Pràctiques d'aula	432	Català/Castellà	segon quadrimestre	matí-mixt
(PAUL) Pràctiques d'aula	451	Català/Castellà	segon quadrimestre	tarda
(PAUL) Pràctiques d'aula	452	Català/Castellà	segon quadrimestre	tarda
(PAUL) Pràctiques d'aula	471	Català/Castellà	segon quadrimestre	matí-mixt
(PLAB) Pràctiques de laboratori	411	Anglès	segon quadrimestre	matí-mixt
(PLAB) Pràctiques de laboratori	412	Anglès	segon quadrimestre	matí-mixt
(PLAB) Pràctiques de laboratori	413	Anglès	segon quadrimestre	matí-mixt
(PLAB) Pràctiques de laboratori	414	Català/Castellà	segon quadrimestre	matí-mixt
(PLAB) Pràctiques de laboratori	415	Català/Castellà	segon quadrimestre	matí-mixt
(PLAB) Pràctiques de laboratori	416	Català/Castellà	segon quadrimestre	matí-mixt

(PLAB) Pràctiques de laboratori	417	Català/Castellà	segon quadrimestre	matí-mixt
(PLAB) Pràctiques de laboratori	418	Català/Castellà	segon quadrimestre	matí-mixt
(PLAB) Pràctiques de laboratori	419	Català/Castellà	segon quadrimestre	matí-mixt
(PLAB) Pràctiques de laboratori	420	Català/Castellà	segon quadrimestre	matí-mixt
(PLAB) Pràctiques de laboratori	421	Català/Castellà	segon quadrimestre	matí-mixt
(PLAB) Pràctiques de laboratori	422	Català/Castellà	segon quadrimestre	matí-mixt
(PLAB) Pràctiques de laboratori	423	Català/Castellà	segon quadrimestre	matí-mixt
(PLAB) Pràctiques de laboratori	424	Català/Castellà	segon quadrimestre	matí-mixt