Universitat Autònoma de Barcelona

2023/2024

Informació i Seguretat

Codi: 104418
Crèdits: 6

Titulació	Tipus	Curs	Semestre
2503740 Matemàtica Computacional i Analítica de Dades	OT	4	2

Professor/a de contacte

Nom: Carlos Borrego Iglesias

Correu electrònic: carlos.borrego@uab.cat

Idiomes dels grups

Podeu accedir-hi des d'aquest enllaç. Per consultar l'idioma us caldrà introduir el CODI de l'assignatura. Tingueu en compte que la informació és provisional fins a 30 de novembre de 2023.

Equip docent

Carlos Borrego Iglesias

Prerequisits

No hi ha prerequisits obligatoris tot i que es recomana haver adquirit els coneixements sobre algebra, probabilitat, teoria de la informació y programació de cursos anteriors.

Objectius

En aquesta assignatura es donarà una introducció a la criptografia. L'objectiu es que l'alumnat aprengui els principis fonamentals i eines que es fan servir en criptografia actualment.

Competències

- Aplicar l'esperit crític i el rigor per validar o refutar arguments tant propis com d'altres.
- Avaluar de manera crítica i amb criteris qualitat el treball realitzat.
- Dissenyar, desenvolupar i avaluar solucions algorísmiques eficients per a problemes computacionals d'acord amb els requisits establerts.
- Formular hipòtesis i imaginar estratègies per confirmar-les o refutar-les.
- Que els estudiants hagin demostrat que comprenen i tenen coneixements en una àrea d'estudi que parteix de la base de l'educació secundària general, i se sol trobar a un nivell que, si bé es basa en llibres de text avançats, inclou també alguns aspectes que impliquen coneixements procedents de l'avantguarda d'aquell camp d'estudi.

- Que els estudiants hagin desenvolupat aquelles habilitats d'aprenentatge necessàries per emprendre estudis posteriors amb un alt grau d'autonomia.
- Que els estudiants sàpiguen aplicar els coneixements propis a la seva feina o vocació d'una manera professional i tinguin les competències que se solen demostrar per mitjà de l'elaboració i la defensa d'arguments i la resolució de problemes dins de la seva àrea d'estudi.
- Que els estudiants tinguin la capacitat de reunir i interpretar dades rellevants (normalment dins de la seva àrea d'estudi) per emetre judicis que incloguin una reflexió sobre temes destacats d'índole social, científica o ètica.
- Relacionar objectes matemàtics nous amb altres de coneguts i deduir-ne les propietats.
- Treballar cooperativament en un context multidisciplinar asumiendo y respetando el rol de los diferentes miembros del equipo.
- Utilitzar eficaçment la bibliografia i els recursos electrònics per obtenir informació.

Resultats d'aprenentatge

1. Aplicar l'esperit crític i el rigor per validar o refutar arguments tant propis com d'altres.
2. Avaluar de manera crítica i amb criteris de qualitat el treball desenvolupat.
3. Conèixer els resultats bàsics de la seguretat en la informació i la criptografia.
4. Identificar els paràmetres que determinen el funcionament d'un sistema.
5. Que els estudiants hagin demostrat que comprenen i tenen coneixements en una àrea d'estudi que parteix de la base de l'educació secundària general, i se sol trobar a un nivell que, si bé es basa en llibres de text avançats, inclou també alguns aspectes que impliquen coneixements procedents de l'avantguarda d'aquell camp d'estudi.
6. Que els estudiants hagin desenvolupat aquelles habilitats d'aprenentatge necessàries per emprendre estudis posteriors amb un alt grau d'autonomia.
7. Que els estudiants sàpiguen aplicar els coneixements propis a la seva feina o vocació d'una manera professional i tinguin les competències que se solen demostrar per mitjà de l'elaboració i la defensa d'arguments i la resolució de problemes dins de la seva àrea d'estudi.
8. Que els estudiants tinguin la capacitat de reunir i interpretar dades rellevants (normalment dins de la seva àrea d'estudi) per emetre judicis que incloguin una reflexió sobre temes destacats d'índole social, científica o ètica.
9. Treballar cooperativament en un context multidisciplinari assumint i respectant el rol dels diferents membres de l'equip.
10. Utilitzar eficaçment la bibliografia i els recursos electrònics per obtenir informació.
11. Utilitzar mètodes numèrics per resoldre problemes en criptografia i seguretat.

Continguts

- Introducció a la criptografia
- Fonaments matemàtics de la criptografia
- Criptografia de clau simètrica
- Funcions hash
- Criptografia de clau pública
- Infrastructures de clau pública
- Comunicació i transmissió de dades segures

Metodologia

L'assignatura s'imparteix en dues sessions setmanals de 2 hores cadascuna. Les sessions es faran en una única aula amb ordinadors o possibilitat d'endollar els portàtils de l'alumnat. No hi ha una clara distinció entre sessions de teoria, problemes i pràctiques al laboratori. Aquestes s'aniran alternant durant el curs segons convingui al seguiment de l'assignatura. En general, i per cada tema a tractar, s'introduiran conceptes teòrics i

es realitzaran activitats més aplicades com la resolució de problemes o seminaris. Es recomana que l'alumnat revisi els materials corresponents a cada sessió amb anterioritat. Es fomentarà la participació activa en la resolució de problemes participant en la seva resolució, exposició i debat a l'aula. Durant el curs es realitzaran algunes pràctiques de laboratori o seminaris de treball pràctic, on es plantejarà un o més problemes que requeriran el disseny i implementació d'una solució completa.

De forma més específica, durant el curs s'aniran alternant:

- Sessions de teoria: classes de tipus magistral on l'objectiu es introduir els conceptes bàsics que permetin a l'alumnat obtenir una visió general i una bona base a partir de la que desenvolupar els continguts i competències de l'assignatura. Es fomentarà la interactivitat i participació activa de l'alumnat.
- Sessions de problemes: sessions en les que es plantegen problemes o exercicis concrets principalment de caire pràctic i de seguiment. Aquests exercicis han de servir a l'estudiant per assolir i practicar el conceptes i competències relacionades amb l'assignatura. Els problemes es realitzen en el cas general de forma individual.
- Pràctiques / seminaris: es plantejarà algun problema més ampli que els tractats a les sessions de problemes com un projecte o pràctica de laboratori. Aquest es realitzarà i s'avaluarà en grup. El nombre de pràctiques a realitzar dependrà de la seva dificultat i llargada i pot canviar en cada curs.

Durant tot el curs es farà servir l'aula Moodle del Campus Virtual de la UAB com a mitjà principal de comunicació entre el professorat i l'alumnat. Això inclou la publicació de materials, publicació de notes parcials, fòrum de discussió, lliurament de treballs, ...

Nota: es reservaran 15 minuts d'una classe, dins del calendari establert pel centre/titulació, per a la complementació per part de l'alumnat de les enquestes d'avaluació de l'actuació del professorat i d'avaluació de l'assignatura/mòdul.

Activitats formatives

Títol	Hores	ECTS	Resultats d'aprenentatge
Tipus: Dirigides			
Seminaris / pràctiques	15	0,6	
Sessions de problemes	15	0,6	
Sessions teoria	30	1,2	
Tipus: Supervisades			
Preparació de sessions	15	0,6	
Tutories	15	0,6	
Tipus: Autònomes			
Estudi / preparació examen	22,5	0,9	
Treball personal	30	1,2	

Avaluació

L'evaluació de l'assignatura consta de les següents parts:

- Exàmens parcials: examen parcial que constarà de preguntes teòriques i/o exercicis. El primer es realitzarà aproximadament a meitat de curs i el segon a final de curs. Nota mínima de cada parcial per separat: 4.5.
- Exercicis i problemes: resolució de problemes i exercicis durant les sessions de problemes. Poden ser activitats de tipus practic o teòric. No requereix nota mínima.
- Pràctiques / seminaris: resolució en grup d'algun cas pràctic o pràctica durant el curs. Nota mínima de cada pràctica per separat: 4.5

Per tal d'aprovar l'assignatura cal que l'avaluació de cadascuna de les parts superi el mínim exigit i que l'avaluació final superi els 5 punts sobre 10.

En cas de no superar l'assignatura perquè 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.

La qualificació de "no avaluable" s'atorgarà a l'alumnat que no participi en cap de les activitats d'avaluació.

La qualificació de "matricula d'honor" s'otorgarà a l'alumnat amb nota igual o superior a 9 per ordre de millor nota final.

Es pot donar el cas d'alguna petita variació en la ponderació de cada part de l'assignatura. Si això fos així, es comunicaria a principi de curs.

Recuperació de notes de l'avaluació continuada:

Es realitzarà un examen final de recuperació que permetrà recuperar els exàmens parcials per separat. Així mateix es pemetrà un lliuramentfinal per recuperar aquelles pràctiques suspeses (aquest lliurament addicional comportarà una penalització a la nota final de la pràctica). La part de problemes i exercicis que no requereix nota mínima no es podrà recuperar.

Convalidacions parcials a l'alumnat repetidor:

Inicialment no es planteja la possibilitat de convalidar parts de l'assignatura, ni la realització de proves de síntesis especials a l'alumnat repetidor. Tot i així aquest fet es pot reconsiderar a començament de curs en funció dels continguts de cada part.

Dates d'activitats d'avaluació:

Les dates d'avaluació continuada i lliurament de treballs i pràctiques es publicaran al campus virtual i poden estar subjectes a canvis de programació per motius d'adaptació a possiblesincidències. Sempre s'informarà al campus virtual sobre aquests canvis ja que s'entén és el mecanisme habitual d'intercanvi d'informació entre el professorat i l'alumnat.

Així mateix, es detallaran amb prou temps d'antelació els mecanismes d'avaluació, metodologia o funcionament general de l'assignatura que no s'hagin concretat en aquesta guia.

Per a cada activitat d'avaluació, s'indicarà un lloc, data i hora de revisió en la que l'estudiant podrà revisar l'activitat amb el professor. 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.

Compromís ètic:

Sense perjudici d'altres mesures disciplinàries que s'estimin oportunes, i d'acord amb la normativa acadèmica

vigent, les irregularitats comeses per l'alumnat 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 teorico-pràctiques individuals (exàmens).

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 aprovar l'assignatura per compensació).

Activitats d'avaluació continuada

Títol	Pes	Hores	ECTS	Resultats d'aprenentatge
Examens parcials	45	3	0,12	1, 2, 3, 4, 5, 6, 7, 8, 10, 11
Problemes i exercicis	15	1,5	0,06	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11
Pràctiques / seminaris	40	3	0,12	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11

Bibliografia

- Jordi Herrera-Joancomartí, Cristina Pérez-Solà, (2021) Criptografia.
- Paar, C., Pelzl, J., *Understanding Cryptography: A Textbook for Students and Practitioners*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010. https://doi.org/10.1007/978-3-642-04101-3. Biblioteca UAB: https://cataleg.uab.cat/iii/encore/record/C__Rb1956470
- Smart, N. P., *Cryptography Made Simple*. Springer International Publishing, 2016. https://doi.org/10.1007/978-3-319-21936-3. Biblioteca UAB: https://cataleg.uab.cat/iii/encore/record/C__Rb1980662

Programari

Durant el curs es farà servir diferent programari en funció de l'activitat concreta que es dugui a terme. Es preveu l'ús del llenguatge de programació Python con a llenguatge principal per la resolució d'exercicis i pràctiques, i l'ús d'eines del sistema Linux com OpenSSL per alguna activitat concreta.