UAB
Universitat Autònoma de Barcelona

Transmissió de Dades i Criptografia

Codi: 44734
Crèdits: 6

2024/2025

Titulació	Tipus	Curs
4318303 Recerca i Innovació en Ciència i Enginyeria Basades en Computadors	OT	0

Professor/a de contacte

Nom: Guillermo Navarro Arribas

Correu electrònic: guillermo.navarro@uab.cat

Idiomes dels grups

Podeu consultar aquesta informació al final del document.

Prerequisits

No hi ha requisits formals previs. S'assumeixen coneixements de grau sobre temes relacionats amb la transmissió de dades.

Objectius

L'objectiu d'aquesta assignatura és estudiar i aprofundir en diferents temes de recerca de transmissió de dades. Per això l'assignatura se centra en proporcionar una introducció a la recerca en tres blocs principals:

- la teoria de la codificació,
- la compressió de dades i
- la seguretat.

L'alumnat coneixerà conceptes avançats d'aquests temes i serà introduït a la recerca que es fa en l'actualitat.

Resultats d'aprenentatge

1. CA06 (Competència) El graduat o graduada ha de ser capaç de dissenyar sistemes fiables, eficients i segurs de transmissió i emmagatzematge de dades, usant codis correctors d'errors, i tècniques de compressió i seguretat.
2. CA06 (Competència) El graduat o graduada ha de ser capaç de dissenyar sistemes fiables, eficients i segurs de transmissió i emmagatzematge de dades, usant codis correctors d'errors, i tècniques de compressió i seguretat.
3. CA07 (Competència) El graduat o graduada ha de ser capaç de planificar i desenvolupar projectes de recerca amb contingut dins de l'àrea del tractament de la informació.
4. CA07 (Competència) El graduat o graduada ha de ser capaç de planificar i desenvolupar projectes de recerca amb contingut dins de l'àrea del tractament de la informació.
5. KA16 (Coneixement) El graduat o graduada ha de ser capaç de descriure diferents sistemes per a la correcció d'errors aplicats a la criptografia postquàntica, i basats en codis LDPC.

6. KA17 (Coneixement) El graduat o graduada ha de ser capaç de descriure diferents mètodes de compressió utilitzats per a dades IoT, de xarxes socials, telepresència, núvols de punts i imatges mèdiques.
7. KA18 (Coneixement) El graduat o graduada ha de ser capaç de descriure diferents mètodes criptogràfics basats en corbes el·líptiques i utilitzats en la tecnologia blockchain, així com mètodes per a garantir la privadesa de les dades.
8. SA21 (Habilitat) Ser capaç d'aplicar diferents mètodes de codificació per a corregir errors utilitzats en el camp de la criptografia postquàntica i transmissions massives de dades.
9. SA22 (Habilitat) Ser capaç d'aplicar diferents algoritmes de compressió per a diferents tipus de dades.
10. SA23 (Habilitat) Ser capaç d'aplicar diferents mecanismes de criptografia, basats en corbes el·líptiques i tecnologia blockchain, i privadesa de dades.

Continguts

Els continguts principals del curs estan dividits en els tres blocs principals de l'assignatura:

- Teoria de codis: Codis de correcció d'errors aplicats a l'esteganografia i criptografia post-quantica, i codis LPDC utilitzats, p.e. a la televisió digital.
- Compressió de dades: compressió per a diferents tipus de dades, com ara Internet de les coses, xarxes socials, telepresència, imatges mèdiques i tècniques basades en l'aprenentatge automàtic.
- Seguretat i privacitat: criptografia de corbes el·líptiques, tecnologia blockchain i la seva aplicació a criptomonedes, privadesa de dades.

En funció dels antecedents i interessos de l'alumnat, aquests tindran l'oportunitat d'aprofundir més o menys en determinats temes.

Activitats formatives i Metodologia

Títol	Hores	ECTS	Resultats d'aprenentatge
Tipus: Dirigides			
Estudi per test i presentacions	15	0,6	
Preparació de treballs escrits	25	1	
Sessions dirigides pel professorat	45	1,8	
Tipus: Supervisades			
Activitats presencials	15	0,6	
Tipus: Autònomes			
Preparació de tests de sintesi	15	0,6	
Treball i preparació de classes	35	1,4	

La metodologia d'aquest curs està dissenyada per exposar els estudiants a alguns dels temes de recerca rellevants en les àrees de la teoria de la codificació, la compressió de dades i la seguretat. Es basarà en el

concepte "aprendre fent", i s'adaptarà al nombre d'alumnes que es matriculin al curs. En general, hi haurà una combinació de sessions teòriques i pràctiques, incloent-hi classes magistrals, treballs per part dels estudiants, presentacions i treball col·laboratiu.

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.

Avaluació

Activitats d'avaluació continuada

Títol	Pes	Hores	ECTS	Resultats d'aprenentatge
Test de síntesi	30%	0	0	CA06, CA07, KA16, KA17, KA18, SA21, SA22, SA23
Treballs	70%	0	0	CA06, CA07, KA16, KA17, KA18, SA21, SA22, SA23

Es vol adoptar una metodologia d'avaluació que sigui prou flexible per adaptar-se al treball concret fet a classe, això vol dir que pot variar lleugerament d'un curs a un altre. L'avaluació es basarà en 2 tipus d'activitats diferenciades:

- Treballs: es proposaran diferents treballs a l'alumnat durant el curs. Aquests poden incloure treballs individuals i en grup i poden tenir una orientació teòrica o pràctica. En poden ser exemples: exercicis, estudi i exposició d'un tema relacionat amb l'assignatura, pràctiques, ...
- Prova de síntesi: s'utilitzaran proves de síntesi com a activitat d'avaluació individual. Aquestes proves es poden substituir per altres activitats d'avaluació si, per exemple, el nombre d'alumnes és baix.

Al principi de curs s'explicarà amb detall les activitats d'avaluació.

Bibliografia

La bibliografia es facilitarà a l'inici del curs. Donat el caràcter dinàmic dels temes a presentar, la bibliografia específica canviarà cada curs per adaptar-la a l'estat de la recerca actual en aquest àmbit. Normalment inclourà articles rellevants.

Programari

S'oferirà a l'inici del curs.

Llista d'idiomes

Nom	Grup	Idioma	Semestre	Torn
(PLABm) Pràctiques de laboratori (màster)	1	Anglès	segon quadrimestre	matí-mixt

(TEm) Teoria (màster)	1	Anglès	segon quadrimestre	matí-mixt