Tecnologies de la Informació i Seguretat 2014/2015

Codi: 43341
Crèdits: 6

Titulació	Tipus	Curs	Semestre
4314660 Enginyeria Informàtica / Computer Engineering	OB	1	1

Professor de contacte

Nom: Joaquim Borges Ayats
Correu electrònic: Joaquim.Borges@uab.cat

Utilització de llengües

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

Equip docent

Jordi Herrera Joancomarti
Mercè Villanueva Gay

Prerequisits

No hi ha prerequisits.

Objectius

L'objectiu d'aquest mòdul consisteix a proveir una introducció al processament de la informació, emfatitzant la teoria matemàtica de la informació i el seu tractament, la codificació per a la correcció d'errors, tècniques i codificació criptogràfica per a la seguretat de la informació, aplicacions a xarxes de comunicació i disseny d'aplicacions.

Competències

- Demostrar un esperit emprenedor i innovador en la recerca de nous espais o àmbits en el camp de treball propi, amb una visió àmplia de les possibilitats de la carrera professional en l'àmbit de l'enginyeria informàtica.
- Gestionar de manera responsable la informació i el coneixement en la direcció de grups i/o projectes multidisciplinaris.
- Que els estudiants siguin capaços d'integrar coneixements i enfrontar-se a la complexitat de formular judicis a partir d'una informació que, tot i ser incompleta o limitada, inclogui reflexions sobre les responsabilitats socials i ètiques vinculades a l'aplicació dels seus coneixements i judicis
- Ser capaç d'aplicar els coneixements adquirits i de resoldre problemes en entorns nous o poc coneguts dins de contextos més amplis i multidisciplinaris, integrant-hi aquests coneixements.
- Ser capaç de comprendre i saber aplicar el funcionament i lorganització d'Internet, les tecnologies i els protocols de xarxes de nova generació, els models de components, programari intermediari i serveis.
- Ser capaç de dirigir obres i instal·lacions de sistemes informàtics, complint la normativa vigent i assegurant la qualitat del servei.
- Ser capaç de dissenyar, desenvolupar, gestionar i avaluar mecanismes de certificació i garantia de seguretat en el tractament i laccés a la informació en un sistema de processament local o distribuït.

- Ser capaç de dur a terme la direcció general, la direcció tècnica i la direcció de projectes de recerca, desenvolupament i innovació, en empreses i centres tecnològics, en l'àmbit de l'enginyeria informàtica.
- Ser capaç de fer modelatge matemàtic, càlcul i simulació en centres tecnològics i d'enginyeria d'empresa, particularment en tasques de recerca, desenvolupament i innovació en tots els àmbits relacionats amb l'enginyeria informàtica.
- Ser capaç de projectar, calcular i dissenyar productes, processos i instal·lacions en tots els àmbits de l'enginyeria informàtica.
- Tenir coneixements que aportin la base o l'oportunitat de ser originals en el desenvolupament o l'aplicació d'idees, sovint en un context de recerca

Resultats d'aprenentatge

1. Avaluar la seguretat dels protocols de xarxes partint dels components criptogràfics utilitzats.
2. Decidir quin és el tipus de codificació més idònia, depenent de les característiques del senyal i del canal de transmissió.
3. Demostrar un esperit emprenedor i innovador en la recerca de nous espais o àmbits en el camp de treball propi, amb una visió àmplia de les possibilitats de la carrera professional en l'àmbit de l'enginyeria informàtica.
4. Gestionar de manera responsable la informació i el coneixement en la direcció de grups i/o projectes multidisciplinaris.
5. Que els estudiants siguin capaços d'integrar coneixements i enfrontar-se a la complexitat de formular judicis a partir d'una informació que, tot i ser incompleta o limitada, inclogui reflexions sobre les responsabilitats socials i ètiques vinculades a l'aplicació dels seus coneixements i judicis
6. Ser capaç d'aplicar els coneixements adquirits i de resoldre problemes en entorns nous o poc coneguts dins de contextos més amplis i multidisciplinaris, integrant-hi aquests coneixements.
7. Ser capaç de dirigir obres i instal·lacions de sistemes informàtics, complint la normativa vigent i assegurant la qualitat del servei.
8. Ser capaç de dur a terme la direcció general, la direcció tècnica i la direcció de projectes de recerca, desenvolupament i innovació, en empreses i centres tecnològics, en l'àmbit de l'enginyeria informàtica.
9. Ser capaç de fer modelatge matemàtic, càlcul i simulació en centres tecnològics i d'enginyeria d'empresa, particularment en tasques de recerca, desenvolupament i innovació en tots els àmbits relacionats amb l'enginyeria informàtica.
10. Ser capaç de projectar, calcular i dissenyar productes, processos i instal·lacions en tots els àmbits de l'enginyeria informàtica.
11. Tenir coneixements que aportin la base o l'oportunitat de ser originals en el desenvolupament o l'aplicació d'idees, sovint en un context de recerca

Continguts

Codificació del canal (10 sessions)
1. Introducció a la teoria de la informació
2. Introducció a la codificació del canal
3. Introducció als cossos finits de característica 2
4. Codis lineals sobre cossos finits
5. Mètodes de descodificació per a codis lineals
6. Codis d'Hamming
7. Codis cíclics
8. Codis algebraics I
9. Codis algebraics II
10. Descodificació de codis algebraics

Seguretat i ocultació d'informació (5 sessions)
11. Criptosistemes de clau privada
12. Criptosistemes de clau pública
13. Infraestructures de clau pública
14. Protocols criptogràfics I

15. Protocols criptogràfics II

Metodologia

La metodología de treball combinarà les classes presencials amb la resolució d'exercics per part dels estudiants i també del professor. Una part doncs dels exercicis els farà el professor, altres es prepararan a classe per al següent dia i altres els faran els estudiants de forma autònoma.

Es demanarà el lliurament i exposició d'alguns d'aquests exercics.

Activitats formatives

Títol	Hores	ECTS	Resultats d'aprenentatge
Tipus: Dirigides			
Classes de teoria	30	1,2	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11
Resolució d'exercicis	10	0,4	1, 7, 8, 10
Tipus: Supervisades			
Exposició d'exercicis resolts	30	1,2	2, 3, 4, 5, 8, 9
Tipus: Autònomes			
Preparació per a la resolució d'exercicis	75	3	1, 7, 8, 10

Avaluació

La nota final considerarà la feina entregada al llarg del curs pels estudiants, l'assistència i la participació a classe.
1. L'assistència i l'activa participació és obligatoria. Les faltes poden ser compensades amb alguna feina extra. Pes: 30% (nota mínima: 5 sobre 10).
2. Resolució d'exercicis a la pissarra i lliurament d'exercicis. Pes: 70% (nota mínima: 5 sobre 10).
Per tal de superar el mòdul s'ha d'obtenir una nota igual o superior a 5 en cada un dels apartats.

Activitats d'avaluació

Títol	Pes	Hores	ECTS	Resultats d'aprenentatge
Participació a classe	30%	2	0,08	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11
Resolució i lliurament d'exercicis	70%	3	0,12	2, 3, 4, 5, 8, 9

Bibliografia

- Bruce Schneier, Applied Cryptography, (2nd edition), Wiley, 1995.

- M.A. Sarasa López J.P. Franco. Criptografía Digital: Fundamentos y Aplicaciones. Prensas Universitarias de Zaragoza, 1998.
- Thomas M. Cover and Joy A. Thomas (1991). Elements of Information Theory, John Wiley & Sons, Inc.
- Robert Ash. Information theory. John Wiley and Sons Inc, 1965.
- F.J. MacWilliams and N.J.A. Sloane. The theory of error-correcting codes. North-Holland, 1977.