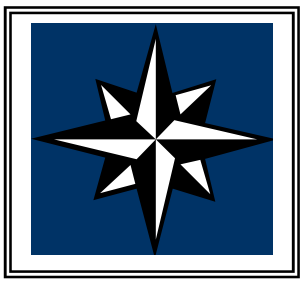
Pla docent de Sistemes de Comunicació

Guia docent
Programació d'activitats



Curs acadèmic: 2012/2013 **Trimestre:** Primer
Nom de l'assignatura: Sistemes de Comunicació
Codi de l'assignatura: 21978
Estudis: Grau en Enginyeria Telemàtica
Nombre de crèdits ECTS: 4 ECTS
Nombre total d'hores de dedicació: 100
Temporalització:
Curs: Segon
Tipus: Trimestral
Període: Primer Trimestre
Professorat: Vanesa Daza, Gonzalo Vázquez
Grup: T1

Guia Docent

1. Dades descriptives de l'assignatura

- **Curs acadèmic:** 2012/2013
- **Nom de l'assignatura:** Sistemes de Comunicació **Codi:** 21978
- **Tipus d'assignatura:** Obligatòria
- **Titulació / Estudis:** Grau en Enginyeria Telemàtica
- **Nombre de crèdits ECTS:** 4
- **Nombre total d'hores de dedicació a l'assignatura:** 100 h
- **Temporalització:**
    - Curs: 1r curs
    - Tipus: Trimestral
    - Període: 1r trimestre
- **Coordinació:** Vanesa Daza
- **Departament:** Departament de Tecnologies de la Informació i les Comunicacions
- **Professorat:** Vanesa Daza, Gonzalo Vázquez
- **Departament:** Departament de Tecnologies de la Informació i les Comunicacions
- **Grup:** T1, T2
- **Llengua de docència:** català, castellà
- **Edifici on s'imparteix l'assignatura:** Edifici 52
- **Horari:**
  - Dilluns 16:30 – 18:30
  - Dimecres 14:30 – 16:30
  - Divendres 18:30 – 20:30

2. Presentació de l'assignatura

L'assignatura *Sistemes de Comunicació* (21978) és una assignatura obligatòria que s'ofereix del Grau en Enginyeria Telemàtica de la Universitat Pompeu Fabra. Consta de 4 crèdits ECTS i s'imparteix al primer trimestre del segon curs acadèmic.

Aquesta assignatura està dividida en dues parts ben diferenciades pel que fa referència als seus continguts. Un bloc dedicat a la criptografia i un altre boc dedicat a les comunicacions.

Durant el primer bloc es presenten els fonaments i les aplicacions principals de la criptologia. La criptologia és la ciència de la comunicació secreta. Té dos subcamps principals: la criptografia, que és la ciència de la creació de xifres secretes, i el criptoanàlisi, que és la ciència de trencar aquestes xifres. Aquestes eines criptogràfiques esdevindran fonamentals més endavant en altres assignatures on s'estudiï la seguretat en les comunicacions. Històricament, la criptografia sempre ha tingut un paper especial en les comunicacions militars i diplomàtiques i en els últims anys ha esdevingut essencial en el desenvolupament de la societat de la informació. Es requereix un domini important d'eines aritmètiques i de matemàtica discreta per tal d'entendre els principals criptosistemes presentats durant el bloc.

Per una altra banda, el segon bloc té com a objectiu principal la introducció dels conceptes fonamentals d'un sistema de comunicacions. S'explicaran els conceptes bàsics presents en qualsevol sistema de transmissió: quantificació, codificació de font, modulació, canal i soroll, filtres i desmodulació. Cal tenir en compte que molts dels coneixements s'impartiran en altres assignatures del grau amb una estreta relació amb Sistemes de Comunicació. Malgrat no és un curs de matemàtiques bàsic per enginyers, requereix també una bona base matemàtica per a poder adquirir coneixements de senyals, transformades de Fourier i dels principals axiomes de probabilitat.

3. Competències a assolir en l'assignatura

Competències generals	Competències específiques
Instrumentals 1. Resolució de problemes. 2. Habilitat de cerca i la gestió de la informació. 3. Capacitat d'anàlisi i síntesi. **Interpersonals** 4. Capacitat crítica i autocrítica. **Sistèmiques** 5. Capacitat d'aplicar amb flexibilitat i creativitat els coneixements adquirits i d'adaptar-los a contextos i situacions noves	6. Utilitzar un programa de processat matemàtic vectorial (Octave) per representar senyals i simular etapes i elements d'un sistema de comunicacions. 7. Poder explicar i visualitzar en Octave el efecte d´elements simples d´un sistema de comunicació (modulació i quantificació) en el temps i frequència 8. Conèixer els conceptes bàsics de codificació de fonts i les seves aplicacions en exemples concrets 9. Determinar la relació senyal a soroll d'un sistema de transmissió. 10. Conèixer les principals etapes per quantificar i codificar seqüències de bits. 11. Conèixer els fonaments teòrics de la criptografia clàssica. 12. Conèixer els fonaments teòrics de la criptografia moderna, tant de clau compartida com pública. 13. Aplicar els coneixements necessaris per a implementar xifres de clau compartida i privada. 14. Definir les principals components i aplicacions de la criptografia per a garantir confidencialitat, integritat, autenticació i no repudi.

4. Objectius d'aprenentatge

Els objectius d'aprenentatge a través dels quals l'assignatura contribueix a l'assoliment de les competències anteriors són:

- Aplicar els coneixements de matemàtiques a l'enginyeria (O1).
- Aplicar el xifrat i la protecció de dades (O2).
- Reconèixer els algorismes actuals de xifratge mitjançant criptografia de clau secreta (O3).
- Reconèixer els algorismes actuals de xifratge mitjançant criptografia de clau pública (O4).
- Reconèixer els algorismes actuals de xifratge i signatura digital amb criptografia de clau pública (O5).
- Aplicar eines criptogràfiques per transmetre dades de forma confidencial, íntegra, autenticada i no repudiable (O6).
- Descriure el funcionament general d'un sistema de comunicacions analògic i digital, identificar els seus diferents components i explicar breument la seva finalitat (O7).
- Identificar les avantatges d'un sistema de comunicacions digital envers d'un analògic (O8).
- Transformar la informació d'entrada digital mitjançant la codificació de font (O9).
- Calcular la relació senyal a soroll en models de canal senzills (O10).
- Aplicar transformades de Fourier per conèixer la resposta en freqüència de diverses modulacions analògiques i digitals (O11).
- Utilitzar l'Octave com a programa per analitzar sistemes senzills de comunicacions i estudiar l´impacte de diversos paràmetres sobre el rendiment del sistema (O12).

5. Continguts

Bloc 1. Criptografia i criptoanàlisi:

- Introducció i conceptes bàsics
  - Concepte d'esteganografia. Limitacions i riscos.
  - Conceptes de criptologia, criptografia i criptoanàlisi.
  - Conceptes de confidencialitat, autenticació, integritat i no repudi.
  - Tipus d'atacant: passiu i actiu.
  - Conceptes de seguretat incondicional i seguretat computacional.

- Criptografia de clau compartida clàssica
  - Xifres de transposició i substitució simple.
  - Xifres de substitució polialfabètica (Vigenère, Vernam, Màquines de Rotors).

- Criptografia de clau compartida moderna
  - Xifres de bloc (DES, AES)

- Xifres de flux (RC4)
- Protocols d'autenticació repte-resposta basats en xifres de clau compartida.
- Atac de l'home a mig camí contra les xifres de clau compartida.

o Criptografia de clau pública
- Funcionament d'una xifra de clau pública.
- Fonaments d'aritmètica modular.
- El problema de la factorització entera.
- La xifra RSA.
- El problema del logaritme discret.
- La xifra ElGamal.
- Signatura digital en RSA i ElGamal
- Protocols d'autenticació repte-resposta basats en xifres de clau pública.
- Atac de l'home a mig camí contra les xifres de clau pública.

- Bloc 2. Comunicacions

o Introducció a les sistemes de comunicacions:

- Canals i soroll.
- Elements d'un sistema de comunicació.
- Comunicacions digitals i analògiques.
- Modulacions analògiques.
  - Concepte de modulació.
  - Amplitud modulada.

o Quantificació:
- Quantificació escalar i vectorial.
- Error de quantificació.
- Llei A i Llei μ.
- DPCM:
  - Codificació diferencial per polsos.
  - ADPCM.
- DM:
  - Modulació delta.
  - ADM.

o Codificació de font:
- Mesura de la informació.
- Teorema de la codificació de font.
- Codificació de Huffman.
- Codificació Lempel-Ziv.

o Modulacions analògiques i digitals:
- Concepte de modulació.
- Amplitud modulada.
  - Esquemes de modulació i desmodulació.
  - Càlcul de potencia.

    - Sobremodulació i aliasing.
- Freqüència modulada.
- Modulacions digitals.

6. Metodologia

Aquesta assignatura es durà a terme mitjançant sessions presencials i sessions no presencials.

Les sessions presencials seran tant sessions de teoria, sessions de seminari com sessions de laboratori. Les sessions de teoria i de laboratori tindran una durada de dues hores, mentre que les de seminari d'una hora.

A les sessions de seminari es plantejaran un o diversos exercicis que els estudiants resoldran a classe. Prèviament els alumnes disposaran de material necessari per preparar la sessió. En alumnes hauran de preparar en avançada els exercicis proposats pels professors per tal de discutir-los i corregir-los a classe. En algunes de les sessions es demanarà l'entrega d'alguns exercicis a l'inici de la sessió (prèviament s'hauran especificat quins).

A les sessions de laboratori els alumnes realitzaran en grups petits exercicis davant l'ordinador implementant, tant amb un software criptogràfic per analitzar alguns criptosistemes com en l´entorn Octave veient exemples senzills de sistemes de comunicació. Els alumnes hauran de discutir els resultats obtinguts confrontant els raonaments teòrics simples. Un enunciat serà distribuït en cada sessió i l´alumne lliurarà el seu informe a través de la plataforma Moodle.

Tot el material de l'assignatura (diapositives i enunciats) estarà disponible a través de l'Aula Moodle de l'assignatura a l'Aula Global.

Puntualment es programaran sessions no presencials on es realitzaran qüestionaris on-line a través de la plataforma Moodle.

7. Avaluació

L'avaluació del curs està basada principalment en l'avaluació per competències.

S'ha dissenyat un itinerari per l'avaluació de l'estudiant. L'itinerari proposa una avaluació contínua a través de les activitats d'aprenentatge proposades a l'assignatura. Per una altra banda, un percentatge de l'avaluació recau en una prova final.

Es descriu tot seguit amb més detalls aquest itinerari.

Per a cadascun dels blocs, la nota final depèn de quatre factors:

- Participació i lliurament d'exercicis a les sessions de seminari (5%)
- Lliurament de les pràctiques a les sessions de laboratori (5%)

- Qüestionaris on-line no presencials (5%)
- Prova global al final de del bloc (35%)

A cadascun dels blocs es requereix un 50% de la qualificació de pràctiques per tal de poder superar el bloc corresponent.

Cal aprovar cadascun dels blocs amb un 50% per tal de poder superar l'assignatura.

Al juliol només serà recuperable la prova global per a aquells blocs que no s'hagin superat.

8. Bibliografia i recursos didàctics

- Bibliografia bàsica
  - Cryptography: theory and practice, Douglas Stinson, Chapman & Hall, CRC, 2006.
  - B. Schneier, Applied cryptography. Wiley. 1996.
  - Digital Commnications: Fundamentals and Applications, Sklar, Bernard.
  - Sistemas de Comunicación, Haykin, Simon S., Limusa Wiley, edición 2002

- Bibliografia complementària
  - W. Stallings, Cryptography and network security. Prentice-Hall, 2nd edition. 1999.
  - A. Menezes, P.Oorschot, S.Vanstone, Handbook of applied cryptography. CRC Press. 1997.
  - Communication Systems, Carlson, A. B. Et al., McGraw-Hill, edición 2002.
  - Comunicaciones Digitales, Artés, A. V. et. al., Pearson - Prentice Hall 2007

- Recursos didàctics i material docent
  - A l'aula Moodle de l'assignatura, l'alumne podrà obtenir el material docent corresponent a les sessions de teoria.
  - A l'aula Moodle de l'assignatura, l'alumne podrà obtenir la col·lecció de problemes corresponent a les sessions de seminaris.

Programació d'activitats

Setmana	*Activitat a l'aula* *agrupament / tipus d'activitat*	*Activitat fora de l'aula* *agrupament / tipus d'activitat*
Setmana 1	Sessió 1 : Teoria Sessió 2: Seminari	
Setmana 2	Sessió 1 : Teoria Sessió 2 : Seminari Sessió 3 : -	
Setmana 3	Sessió 1 : Teoria Sessió 2 : Seminari Sessió 3 : Festiu	
Setmana 4	Sessió 1 : Teoria Sessió 2 : Teoria Sessió 3 : -	
Setmana 5	Sessió 1 : Seminari Sessió 2 : Lab1 Sessió 3 : -	
Setmana 6	Sessió 1 : Examen Bloc Cripto Sessió 2 : Teoria Sessió 3 : Festiu	
Setmana 7	Sessió 1 : Teoria Sessió 2 : Seminari Sessió 3 : -	
Setmana 8	Sessió 1 : Teoria Sessió 2 : Seminari Sessió 3 : Lab2	
Setmana 9	Sessió 1 : Teoria Sessió 2 : Seminari Sessió 3 : -	
Setmana 10	Sessió 1 : Teoria Sessió 2 : Seminari Sessió 3 : Lab3	
Setmana 11	Sessió 1 : - Sessió 2 : - Sessió 3 : Festiu	
Exàmens	Examen Bloc Comunicacions	