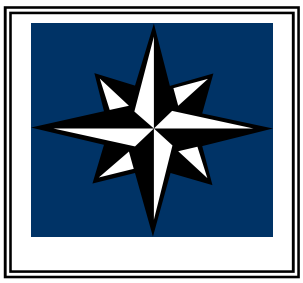
Pla docent de Sistemes de Comunicació

Guia docent
Programació d'activitats



Curs acadèmic: 2011/2012 **Trimestre:** Primer
Nom de l'assignatura: Sistemes de Comunicació
Codi de l'assignatura: 21978 i 21464
Estudis: Grau en Enginyeria Telemàtica i Grau en Enginyeria Informàtica
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 Vazquez i Mathieu De Craene
Grup: T1

Guia Docent

1. Dades descriptives de l'assignatura

- **Curs acadèmic:** 2011/2012
- **Nom de l'assignatura:** Sistemes de Comunicació **Codi:** 21978 i 21464
- **Tipus d'assignatura:** Obligatòria pel Grau en Enginyeria Telemàtica i Optativa pel Grau en Enginyeria en Informàtica
- **Titulació / Estudis:** Grau en Enginyeria Telemàtica i Grau en Enginyeria en Informàtica
- **Nombre de crèdits ECTS:** 4
- **Nombre total d'hores de dedicació a l'assignatura:** 100 h
- **Temporalització:**
    - Curs: 1r curs
    - Tipus: trimestre
    - Període: 1r trimestre
- **Coordinació:** Vanesa Daza i Mathieu De Craene
- **Departament:** Departament de Tecnologies de la Informació i les Comunicacions
- **Professorat:** Vanesa Daza, Gonzalo Vazquez i Mathieu De Craene
- **Departament:** Departament de Tecnologies de la Informació i les Comunicacions
- **Grup:** T1, T2
- **Llengua de docència:** català, castellà i anglès
- **Edifici on s'imparteix l'assignatura:** Edifici 52

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.

En aquest document es descriu amb detall el pla docent de l'assignatura.

Durant la primera meitat del curs 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, clau en el desenvolupament de la societat de la informació. 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.

Per una altra banda, la altra part del curs té com objectiu principal la introducció dels conceptes fonamentals d'un sistema de comunicacions. S'explicaran els conceptes bàsics presents en qualsevol sistema de transmissió: modulació, canal i soroll, filtres i desmodulació. Després es focalitzarà a les etapes de quantificació i codificació de font. 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 matemàtica bàsic per enginyers, però requereix una bona base matemàtica per a poder adquirir un coneixement 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. 5. Capacitat de treball en equip. **Sistèmiques** 6. Capacitat d'aplicar els coneixements a la pràctica	7. Utilitzar un programa de processat matemàtic vectorial (Octave) per representar senyals i simular etapes i elements d'un sistema de comunicacions. 8. Poder explicar i visualitzar en Octave el efecte d´elements simples d´un sistema de comunicació (modulació i quantificació) en el temps i freqüència. 9. Conèixer els conceptes bàsics de codificació de fonts i les seves aplicacions en exemples concrets 10. Determinar la relació senyal a soroll d'un sistema de transmissió. 11. Conèixer els principals etapes per quantificar i codificar sequències de bits. 12. Conèixer els fonaments teòrics de la criptografia clàssica. 13. Conèixer els fonaments teòrics de la criptografia moderna, tant de clau compartida com pública. 14. Aplicar els coneixements necessaris per a implementar xifres de clau compartida i privada. 15. 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 protecció de dades (O2).
- Reconéixer els algorismes actuals de xifratge mitjançant criptografia de clau secreta (O3).
- Reconèixer els algorismes actuals de xifratge mitjançant criptografia de clau pública (O4).
- Reconéixer els algorismes actuals de xifratge i signatura digital amb criptografia de clau pública (O5).
- Aplicar les eines criptogràtiques per transmetre dades de forma confidencial, íntegra, autenticada i no repudiable (O6).
- Descriure el funcionament general d'un sistema de comunicacions digitals, 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).
- Utilitzar Octave com programa per analitzar sistemes simples de comunicacions i estudiar l´impacte de diversos paràmetres sobre el rendiment del sistema (O11).

5. Continguts

- Bloc 1. 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.

- Bloc 2. Criptografia de clau compartida clàssica
  - Xifres de transposició i substitució simple.
  - Xifres de substitució polialfabètica (Vigenère, Vernam, Màquines de Rotors).

- Bloc 3. 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.

- Bloc 4. 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.
  - El sobre digital.
  - 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 5. Introducció a les sistemes de comunicacions:
  - Comunicacions digitals i analògiques.
  - Elements d'un sistema de comunicació.
  - Canals.
  - Soroll:
    - Senyals i processos aleatoris.
    - Soroll blanc additiu gaussià (AWGN).
    - Probabilitat d'error.

- Bloc 6. Comunicacions analògiques:
  - Concepte de modulació.
  - Amplitud modulada.
    - Esquemes de modulació i desmodulació.
    - Càlcul de potencia
    - Sobremodulació i aliasing
  - Freqüència modulada.

- Bloc 7. Quantificació:
  - Quantificació escalar i vectorial.
  - Error de quantificació.
  - Llei A i Llei μ.
  - DPCM:
    - Modulació diferencial per codificació per polsos.
    - Error de predicció.
    - Càlcul de la relació senyal a soroll.
    - ADPCM.
  - DM:
    - Modulació delta.
    - ADM.
  - LPC (Linear Predictive Code) de señales de voz.

- Bloc 8. Codificació de font:
    - Mesurada d'informació.
    - Teorema de la codificació de font.
    - Codificació de Huffman.
    - Codificació Lempel-Ziv.

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, mentres 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. Hauran d'entregar abans de l'inici de la sessió el treball realitzat per tal de garantir l'aprofitament de la sessió de seminari. Durant la resolució d'aquests exercicis podran preguntar qualsevol dubte al professor o a altres companys. En els propers dies hauran d'escriure i lliurar un document detallant la seva solució.

A les sessions de laboratori els alumnes realitzaran en grups petits exercicis davant l'ordinador implementant en l´entorn Octave exemples simples de sistemes de comunicació. Els alumnes hauran de discutir els resultats obtinguts confrontant els raonaments teórics simples. Un enunciat serà distribuit en cada sessió i l´alumne lliurarà el seu informe a través de la plataforma Moodle.

Les sessions no presencials es dedicaran a la realització d'exercicis davant de l'ordinador. Aquests exercicis consistiran en la implementació de petits programes o en la utilització d'eines criptogràfiques de lliure distribució. De cada sessió no presencial caldrà lliurar un document mostrant la feina feta.

Tot el material de l'assignatura (diapositives i enunciats) estarà disponible a través de l'Aula Moodle de l'assignatura a l'Aula Global. Amb això es facilitarà el seguiment de l'assignatura per part d'estudiants que no poden assistir a classe.

En acabar cada bloc, els alumnes hauran de realitzar un qüestionari on-line a través de la plataforma Moodle del bloc temàtic finalitzat. L'objectiu és doncs utilitzar els qüestionaris d'opció múltiple de Moodle com a una eina didàctica asíncrona que permeti fer un seguiment de l'alumne en finalitzar cadascun dels diferents apartats de cadascun dels blocs temàtics de l'assignatura, amb la principal finalitat de millorar l'aprenentatge de l'estudiant. Així doncs s'identifiquen les dificultats d'aprenentatge, i es té l'oportunitat de prendre mesures en conseqüència, oferint recolzament complementari.

7. Avaluació

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

S'han dissenyat dos itineraris ben diferenciats per a l'avaluació de l'estudiant. Per una banda, un itinerari proposa una avaluació continuada a través de les activitats d'aprenentatge proposades a l'assignatura. Per una altra banda, un itinerari on un gran percentatge de l'avaluació recau en una prova final.

Es descriu tot seguit amb més detalls ambós itineraris.

Per a aquells alumnes que segueixin l'avaluació continuada, la nota final de l'assignatura depèn de tres factors:

- Lliurament dels exercicis plantejats a les sessions de seminari (20%)
- Lliurament de les pràctiques plantejades a les sessions de laboratori (20%)
- Qüestionaris on-line no presencials en finalitzar cadascun dels blocs temàtics (25%)
- Qüestionari on-line presencial en finalitzar cadascuna de les partes (criptografia i comunicació) de l'asignatura (35%)

Per tal de que un estudiant pugui optar a l'avaluació continuada, garantint l'assoliment de les competències de la segona part de l'assignatura cal que superi, amb més del 40% la qualificació de tots els qüestionaris així com les pràctiques tant presencials com no presencials. A més a més, caldrà que la qualificació del qüestionari final sigui de més d'un 40%.

A les pràctiques presencials i no presencials s'avaluen les competències generals que es proposa treballar a l'assignatura. En aquells casos on no es superi l'avaluació d'aquestes competències, l'alumne haurà de recuperar-les per tal de superar satisfactòriament l'assignatura.

Els estudiants que opten pel segon itinerari, hauran de seguir l'avaluació continuada mitjançant la realització d'una prova global a final de curs. En aquest cas, la nota final depèn principalment de dos factors:

- Lliurament de les pràctiques de l'assignatura, tant les presencials (encara que no assisteixin a classe) com les no presencials. La superació de les pràctiques amb més d'un 40% de la qualificació màxima de la pràctica és obligatòria per tal de superar l'assignatura (20%).
- Prova global a final de curs (80%).

Per a qui no superi aquesta primera convocatòria, hi ha una segona convocatòria al mes de setembre. En el cas d´aprovar una sola de las dues

parts (criptografia i comunicació), l´alumne haurà de tornar a presentar únicament la part suspesa.

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 2 : Teoria (ST1)	
Setmana 2	Sessió 1 : Teoria (ST2) Sessió 2 : Seminari (SS1) Sessió 3 : Seminari (SS1)	
Setmana 3	Sessió 1 : Lab1 Sessió 2 : Teoria (ST3) Sessió 3 : Seminari (SS2)	Pràctica No Presencial 1
Setmana 4	Sessió 1 : Seminari (SS2) Sessió 2 : Teoria (ST4) Sessió 3 : Seminari (SS3)	Pràctica No Presencial 2

Setmana 5	Sessió 1 : Seminari (SS3) Sessió 2 : Teoria (ST5) Sessió 3 : Seminari (SS4)	
Setmana 6	Sessió 1 : Seminari (SS4) Sessió 2 : Teoria (ST6) Sessió 3 : Teoria (ST7)	
Setmana 7	Sessió 1 : Festiu Sessió 2 : Lab2 Sessió 3 : Seminari (SS5)	
Setmana 8	Sessió 1 : Teoria (ST8) Sessió 2 : - Sessió 3 : Seminari (SS6)	
Setmana 9	Sessió 1 : Teoria (ST9) Sessió 2 : Lab3 Sessió 3 : Seminari (SS7)	
Setmana 10	Sessió 1 : Teoria (ST10) Sessió 2 : - Sessió 3 : Seminari (SS8)	Pràctica No Presencial 3
Setmana 11	Sessió 1 : Teoria (ST11) Sessió 2 : - Sessió 3: -	