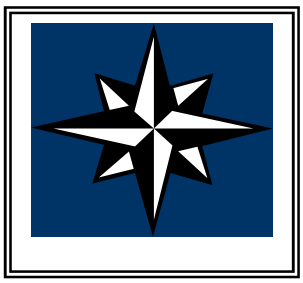
Plan docente de Sistemas de Comunicación



Guía docente
Programación de actividades

Curso académico: 2011/2012 **Trimestre:** Primer trimestre
Nombre de la asignatura: Sistemas de Comunicación
Código de la asignatura: 21978 y 21978
Estudios: Grado en Ingeniería Telemática y Grado en Informática
Número de créditos ECTS: 4 ECTS
Número total de horas de dedicación: 100
Distribución temporal:
Curso: Segundo
Tipo: Trimestral
Período: Primer Trimestre
Profesorado: Vanesa Daza, Gonzalo Vazquez y Mathieu De Craene
Grupo: T1

Guía Docente

1. Datos descriptivos de la asignatura

- **Curso académico:** 2011 / 2012
- **Nombre de la asignatura:** Sistemas de Comunicación **Código:** 21978 y 21464
- **Tipo de asignatura:** Obligatoria del Grado en Ingeniería Telemática y Optativa del Grado en Ingeniería Informática
- **Titulación / Estudios:** Grado en Ingeniería Telemática y Grado en Ingeniería Informática
- **Número de créditos ECTS:** 4
- **Número total de horas de dedicación a la asignatura:** 100 h
- **Distribución temporal:**
    - Curso: 1er curso
    - Tipo: trimestre
    - Periodo: 1r trimestre
- **Coordinación:** Vanesa Daza y Mathieu De Craene
- **Departamento:** Departamento de Tecnologías de la Información y las Comunicaciones
- **Profesorado:** Vanesa Daza, Gonzalo Vazquez y Mathieu De Craene
- **Grupos:** T1 y T2
- **Lengua de docencia:** catalán, castellano e inglés
- **Edificio donde se imparte la asignatura:** Edificio 52
-

2. Presentación de la asignatura

La asignatura Sistemas de Comunicación (21978) es una asignatura obligatoria que se ofrece del Grado en Ingeniería Telemática de la Universitat Pompeu Fabra. Consta de 4 créditos ECTS y se imparte en el primer trimestre del segundo curso académico.

Esta asignatura está dividida en dos partes bien diferenciadas en lo referente a sus contenidos. En este documento se describe con detalle el plan docente de la asignatura, que se corresponde temporalmente con las primeras cinco semanas del trimestre.

Durante la primera mitad del curso, se presentan los fundamentos y las aplicaciones principales de la criptología. La criptología es la ciencia de la comunicación secreta. Tiene dos subcampos principales: la criptografía, que es la ciencia de la creación de cifras secretas, y el criptoanálisis, que es la ciencia de romper estas cifras. Estas herramientas criptográficas serán fundamentales más a delante en otras asignaturas donde se estudie la seguridad en las comunicaciones, clave en el desarrollo de la sociedad de la información. Históricamente, la criptografía siempre ha tenido un papel especial en las comunicaciones militares y diplomáticas y, en los últimos años, se ha convertido en esencial en el desarrollo de la sociedad de la información.

Por otro lado, la otra parte del curso tiene como objetivo principal la introducción de los conceptos básicos presentes en cualquier sistema de transmisión: modulación, canal y ruido, filtros y desmodulación. Después se focalizará en las etapas de cuantificación y codificación de fuente. Se tiene que tener en cuenta que muchos de los conocimientos se impartirán en otras asignaturas del Grado con una estrecha relación con Sistemas de Comunicación. No obstante, no es un curso de matemáticas básico para ingenieros, porque se requiere una buena base matemática para poder adquirir un conocimiento de señales, transformadas de Fourier y de los principales axiomas de probabilidad.

3. Competencias a alcanzar en la asignatura

Competencias generales	Competencias específicas
Instrumentales 1. Resolución de problemas. 2. Habilidad de búsqueda y la gestión de la información. 3. Capacidad de análisis y síntesis. **Interpersonales** 4. Capacidad crítica y autocrítica. 5. Capacidad de trabajo en equipo. **Sistémicas** 6. Capacidad de aplicar los conocimientos en la práctica.	7. Utilizar un programa de procesado matemático vectorial (Octave) para representar señales y simular etapas y elementos de un sistema de comunicaciones. 8. Poder explicar y visualizar en Octave el efecto de elementos simples de un sistema de comunicación (modulación y cuantificación) en el tiempo y frecuencia 9. Conocer los conceptos básicos de codificación de fuentes y sus aplicaciones en ejemplos concretos. 10. Determinar la relación señal a ruido de un sistema de transmisión. 11. Conocer las etapas principales para cuantificar y codificar secuencias de bits. 12. Conocer los fundamentos teóricos de la criptografía clásica. 13. Conocer los fundamentos teóricos de la criptografía moderna, tanto de clave compartida como pública. 14. Aplicar los conocimientos necesarios para implementar cifras de clave compartida y privada. 15. Definir los principales componentes y aplicaciones de la criptografía para garantir confidencialidad, integridad, autenticación y no repudio.

4. Objetivos de aprendizaje

Los objetivos de aprendizaje a través de los cuales la asignatura contribuye al alcance de las competencias anteriores son los siguientes:

- Aplicar los conocimientos de matemáticas a la ingeniería (01).
- Aplicar el cifrado y protección de datos (O2).
- Reconocer los algoritmos actuales de cifrado mediante criptografía de clave secreta (03).
- Reconocer los algoritmos actuales de cifrado mediante criptografía de clave pública (04).
- Reconocer los algoritmos actuales de cifrado y signatura digital con criptografía de clave pública (05).
- Aplicar las herramientas criptográficas para transmitir datos de forma confidencial, íntegra, autenticada y no repudiable (06).
- Describir el funcionamiento general de un sistema de comunicaciones digitales, identificar sus diferentes componentes y explicar brevemente su finalidad (07).
- Identificar las ventajas de un sistema de comunicaciones digital en comparación con uno analógico (08).
- Transformar la información de entrada digital mediante la codificación de fuente (O9).
- Calcular la relación señal a ruido en modelos de canal sencillos (O10).
- Utilizar Octave como programa para analizar sistemas simples de comunicaciones y estudiar el impacto de varios parámetros sobre el rendimiento del sistema (011).

5. Contenidos

- Bloque 1. Introducción y conceptos básicos
  - Concepto de esteganografía. Limitaciones y riesgos.
  - Conceptos de criptología, criptografía i criptoanálisis.
  - Conceptos de confidencialidad, autenticación, integridad y no repudio.
  - Tipo de atacante: pasivo y activo.
  - Conceptos de seguridad incondicional y seguridad computacional.

- Bloque 2. Criptografía de clave compartida clásica
  - Cifras de transposición y substitución simple.
  - Cifras de substitución polialfabética (Vigenère, Vernam y Máquinas de Rotors).

- Bloque 3. Criptografía de clave compartida moderna
  - Cifras de bloque (DES, AES)
  - Cifras de flujo (RC4)

  - Protocoles de autenticación reto-respuesta basados en cifras de clave compartida.
  - Ataque del hombre a medio camino contra las cifras de clave compartida.

- Bloque 4. Criptografía de clave pública
  - Funcionamiento de una cifra de clave pública.
  - Fundamentos de aritmética modular.
  - El problema de la factorización entera.
  - La cifra RSA.
  - El problema del logaritmo discreto.
  - La cifra ElGamal.
  - El sobre digital.
  - Signatura digital en RSA y ElGamal
  - Protocoles de autenticación reto-respuesta basados en cifras de clave pública.
  - Ataque del hombre a medio camino contra las cifras de clave pública.

- Bloque 5. Introducción a los sistemas de comunicaciones:
  - Comunicaciones digitales y analógicas.
  - Elementos de un sistema de comunicación.
  - Canales.
  - Ruido:
    - Señales y procesos aleatorios.
    - Ruido blanco aditivo gaussiano (AWGN).
    - Probabilidad de error.

- Bloque 6. Comunicaciones analógicas:
  - Concepto de modulación.
  - Amplitud modulada.
    - Esquemas de modulación y desmodulación.
    - Cálculo de potencia
    - Sobremodulación y aliasing
  - Frecuencia modulada.

- Bloque 7. Cuantificación:
  - Cuantificación escalar y vectorial.
  - Error de cuantificación.
  - Ley A y Ley μ.
  - DPCM:
    - Modulación diferencial por codificación por pulsos.
    - Error de predicción.
    - Cálculo de la relación señal a ruido.
    - ADPCM.
  - DM:
    - Modulación delta.
    - ADM.
  - LPC (*Linear Predictive Code*) de señales de voz.

- Bloque 8. Codificación de fuente:
    - Mesurada de información.
    - Teorema de la codificación de fuente.
    - Codificación de Huffman.
    - Codificación Lempel-Ziv.

6. Metodología

Esta asignatura se llevará a cabo mediante sesiones presenciales y sesiones no presenciales. Las sesiones presenciales serán tan sesiones de teoría, sesiones de seminario como sesiones de laboratorio. Las sesiones de teoría y de laboratorio tendrán una duración de dos horas, mientras que las de seminario serán de una hora.

En las sesiones de seminario se plantearán uno o varios ejercicios que los estudiantes resolverán en clase. Previamente, los alumnos dispondrán de material necesario para preparar la sesión. Tendrán que entregar antes del inicio de la sesión el trabajo realizado para garantizar el aprovechamiento de la sesión de seminario. Durante la resolución de estos ejercicios podrán preguntar cualquier duda al profesor o a otros compañeros. En los días siguientes tendrán que escribir y entregar un documento detallando su solución.

En las sesiones de laboratorio, los alumnos realizarán en grupos pequeños ejercicios frente al ordenador implementando en el entorno Octave ejemplos simples de sistemas de comunicación. Los alumnos deberán discutir los resultados obtenidos confrontando los razonamientos teóricos simples. Un enunciado será distribuido en cada sesión y el alumno entregará su informe a través de la plataforma Moodle.

Las sesiones no presenciales se dedicarán a la realización de ejercicios frente al ordenador. Estos ejercicios consistirán en la implementación de pequeños programas o en la utilización de herramientas criptográficas de libre distribución. De cada sesión no presencial se deberá entregar un documento mostrando el trabajo que se ha realizado.

Todo el material de la asignatura (diapositivas y enunciados) estará disponible a través del Aula Moodle de la asignatura en el Aula Global. Con ello se facilitará el seguimiento de la asignatura por parte de los estudiantes que no puedan asistir a clase.

Al finalizar cada bloque, los alumnos deberán realizar un cuestionario on-line a través de la plataforma Moodle del bloque temático finalizado. El objetivo es, pues, utilizar los cuestionarios de opción múltiple de Moodle como una herramienta didáctica asíncrona que permita hacer un seguimiento del alumno al finalizar cada uno de los diferentes apartados de cada uno de los bloques temáticos de la asignatura, con la principal finalidad de mejorar el aprendizaje del estudiante. Así pues, se identifican las dificultades de aprendizaje, y se tiene la oportunidad de tomar medidas en consecuencia, ofreciendo apoyo complementario.

7. Evaluación

La evaluación del curso está basada principalmente en la evaluación por competencias. Además, se han diseñado dos itinerarios bien diferenciados para la evaluación del estudiante. Por un lado, un itinerario propone una evaluación continuada a través de las actividades de aprendizaje propuestas en la asignatura. Por otro lado, hay un itinerario donde un gran porcentaje de la evaluación recae en una prueba final. A continuación, se describe con más detalle los dos itinerarios.

Para aquellos alumnos que sigan la evaluación continuada, la nota final de la asignatura depende de tres factores:

- Entrega de los ejercicios planteados en las sesiones de seminario (20%)
- Entrega de las prácticas planteadas en las sesiones de laboratorio (20%)
- Cuestionarios *on-line* no presenciales al finalizar cada uno de los bloques temáticos (25%)
- Cuestionario on-line presencial en finalizar cada una de las partes (criptografía y comunicación) de la asignatura (35%)

Para que un estudiante pueda optar a la evaluación continuada, garantiendo la adquisición de las competencias de la segunda parte de la asignatura, hace falta que supere, con más del 40% la calificación de todos los cuestionarios, así como las prácticas tanto presenciales como no presenciales. Además, la calificación del cuestionario final tendrá que ser de más de un 40%.

En las prácticas presenciales y no presenciales, se evalúan las competencias generales que se propone trabajar en la asignatura. En estos casos donde no se supere la evaluación de estas competencias, el alumno o alumna tendrá que recuperarlas para superar satisfactoriamente la asignatura.

Los estudiantes que opten por el segundo itinerario, tendrán que seguir la evaluación continuada mediante la realización de una prueba global al final del curso. En este caso, la nota final depende principalmente de dos factores:

- Entrega de les prácticas de la asignatura, tanto las presenciales (aunque que no asistan a clase) como las no presenciales. La superación de las prácticas con más de un 40% de la cualificación máxima de la práctica es obligatoria para superar la asignatura (20%).
- Prueba global al final de curso (80%).

Para quien no supere esta primera convocatoria, hay una segunda convocatoria en el mes de septiembre. En el caso de aprobar una de las dos partes (criptografía y comunicación), el alumno o alumna tendrá que volver a presentar únicamente la parte suspendida.

8. Bibliografía y recursos didácticos

- Bibliografía básica
  - 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

- Bibliografía complementaria
  - 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 didácticos y material docente
  - En el Aula Moodle de la asignatura, el alumno podrá obtener el material docente correspondiente a las sesiones de teoría.
  - En el Aula Moodle de la asignatura, el alumno podrá obtener la colección de problemas correspondiente a las sesiones de seminarios.

Programación de actividades

Semana	*Actividad en el aula* *agrupamiento / tipo de actividad*	*Actividad fuera del aula* *agrupamiento / tipo de actividad*
Semana 1	Sesión 2 : Teoría (ST1)	
Semana 2	Sesión 1 : Teoría (ST2) Sesión 2 : Seminario (SS1) Sesión 3 : Seminario (SS1)	
Semana 3	Sesión 1 : Lab1 Sesión 2 : Teoría (ST3) Sesión 3 : Seminario (SS2)	Práctica No Presencial 1
Semana 4	Sesión 1 : Seminario (SS2) Sesión 2 : Teoría (ST4) Sesión 3 : Seminario (SS3)	Práctica No Presencial 2
Semana 5	Sesión 1 : Seminario (SS3) Sesión 2 : Teoría (ST5) Sesión 3 : Seminario (SS4)	
Semana 6	Sesión 1 : Seminario (SS4)	

	Sesión 2 : Teoría (ST6) Sesión 3 : Teoría (ST7)	
Semana 7	Sesión 1 : Festivo Sesión 2 : Lab2 Sesión 3 : Seminario (SS5)	
Semana 8	Sesión 1 : Teoría (ST8) Sesión 2 : - Sesión 3 : Seminario (SS6)	
Semana 9	Sesión 1 : Teoría (ST9) Sesión 2 : Lab3 Sesión 3 : Seminario (SS7)	
Semana 10	Sesión 1 : Teoría (ST10) Sesión 2 : - Sesión 3 : Seminario (SS8)	Práctica No Presencial 3
Semana 11	Sesión 1 : Teoría (ST11) Sesión 2 : - Sesión 3: -	