



# GUÍA DOCENTE 2010 - 2011

Asignatura (31558) COMUNICACIONES DE DATOS II

## Resumen

---

### Índice

- Descripción general de la asignatura
- Competencias
- Conocimientos recomendados
- Selección y estructuración de las Unidades Didácticas
- Distribución
- Metodología de enseñanza-aprendizaje
- Evaluación
- Recursos
- Bibliografía

### Descripción general de la asignatura

---

Los objetivos de esta asignatura se centran en entender el funcionamiento tanto de los sistemas criptográficos simétricos o de clave secreta, como de los asimétricos o de clave pública, así como de distintos esquemas de firma digital, con el objetivo de ser utilizados como mecanismos de seguridad para proveer servicios criptográficos. Asimismo, se estudian distintos protocolos y aplicaciones criptográficas que se emplean en la actualidad y previsiblemente en el futuro.

---

### Competencias

---

Titulación	Competencia	Nivel
MÁSTER UNIVERSITARIO EN TECNOLOGÍAS, SISTEMAS Y REDES DE COMUNICACIÓN	Formar investigadores y profesionales de alta cualificación en el conocimiento y diseño de sistemas de tiempo real distribuidos, y en particular de las arquitecturas y protocolos necesarios para las comunicaciones multimedia y sus mecanismos de distribución y seguridad utilizados.	Necesaria (2)
MÁSTER UNIVERSITARIO EN TECNOLOGÍAS, SISTEMAS Y REDES DE COMUNICACIÓN	Formar investigadores y profesionales de alta cualificación en el diseño de elementos y subsistemas que formen parte de un sistema de comunicaciones.	Recomendable (4)
MÁSTER UNIVERSITARIO EN TECNOLOGÍAS, SISTEMAS Y REDES DE COMUNICACIÓN	Formar investigadores y profesionales de alta cualificación en el diseño, implementación y evaluación de prestaciones de las redes de comunicaciones tanto fijas como móviles, así como en el proceso de creación de la Sociedad de la Información.	Recomendable (4)
MÁSTER UNIVERSITARIO EN TECNOLOGÍAS, SISTEMAS Y REDES DE COMUNICACIÓN	Formar investigadores y profesionales de alta cualificación en el tratamiento de señales tanto de información en general (imágenes, voz, audio, infrarrojos, ultrasonidos, sónar, etc.) como de comunicaciones.	Necesaria (2)
MÁSTER UNIVERSITARIO EN TECNOLOGÍAS, SISTEMAS Y REDES DE COMUNICACIÓN	Formar investigadores y profesionales de alta cualificación en las técnicas de generación, propagación y detección de señales electromagnéticas que se propaguen a través de medios abiertos y guiados.	Indispensable (1)

Titulación	Materia	Competencia	Nivel
------------	---------	-------------	-------

### Conocimientos recomendados

#### Previos

Titulación	Asignatura
MÁSTER UNIVERSITARIO EN TECNOLOGÍAS, SISTEMAS Y REDES DE COMUNICACIÓN	(31069) COMUNICACIÓN DE DATOS

#### Simultaneos

Titulación	Asignatura
------------	------------

### Selección y estructuración de las Unidades Didácticas

1. Introducción
  1. Introducción a la Criptografía
2. Criptografía simétrica o de clave secreta
  1. Criptografía simétrica o de clave secreta
3. Criptografía asimétrica o de clave pública
  1. Criptografía asimétrica o de clave pública

## 4. Firmas digitales

## 1. Firmas digitales

## 5. Protocolos y aplicaciones criptográficas

## 1. Protocolos y aplicaciones criptográficas

**Distribución**

Unidad didáctica	Trab. Presencial	Trab. no presencial
Introducción	2,00	3,00
Criptografía simétrica o de clave secreta	8,00	12,00
Criptografía asimétrica o de clave pública	8,00	12,00
Firmas digitales	4,00	6,00
Protocolos y aplicaciones criptográficas	8,00	12,00
<b>Total horas</b>	<b>30,00</b>	<b>45,00</b>

**Metodología de enseñanza-aprendizaje****Presenciales**

Nombre	Descripción	horas
Clase presencial	Exposición de contenidos mediante presentación o explicación por parte de un profesor (posiblemente incluyendo demostraciones).	29,00
Evaluación	Conjunto de pruebas escritas, orales, prácticas, proyectos, trabajos, etc. utilizados en la evaluación del progreso del estudiante.	1,00
<b>Total horas</b>		<b>30,00</b>

**Autónomas**

Nombre	Descripción	horas
Trabajos prácticos	Preparación de actividades para exponer o entregar en las clases prácticas.	15,00
Estudio teórico	Estudio de contenidos relacionados con las "clases teóricas": Incluye cualquier actividad de estudio que no se haya computado en el apartado anterior (estudiar exámenes, trabajo en biblioteca, lecturas complementarias, hacer problemas y ejercicios, etc.).	20,00
Estudio práctico	Relacionado con las "clases prácticas".	10,00
<b>Total horas</b>		<b>45,00</b>

**Evaluación**

Nombre	Descripción
Pruebas objetivas (tipo test)	Examen escrito estructurado con diversas preguntas o ítems en los que el alumno no elabora la respuesta; sólo ha de señalarla o completarla con elementos muy precisos.

**Recursos**

---

Laboratorio: PC. Software: Java

---

- pizarra
- copia de las transparencias
- laboratorio (especificar tipo en observaciones)
- software informático(especificar en observaciones)
- transparencias
- materiales multimedia
- apuntes
- exámenes resueltos

**Bibliografía**

---

- Fundamentos de seguridad en redes : aplicaciones y estándares (Stallings, William)
  - Criptografía digital : fundamentos y aplicaciones (Pastor Franco, José)
  - Handbook of applied cryptography (Menezes, Alfred J.)
  - A course in number theory and cryptography (Koblitz, Neal)
  - Applied cryptography : protocols, algorithms, and source code in C (Schneier, Bruce)
-