

1. TITULACIÓN	Ingeniero en Informática
----------------------	---------------------------------

2. NOMBRE DE LA ASIGNATURA	Codificación algebraica
-----------------------------------	--------------------------------

3. CÓDIGO DE LA ASIGNATURA	78307
-----------------------------------	-------

4. CARÁCTER	Optativa
--------------------	----------

5. CURSO	Tercero
-----------------	---------

6. PERIODO	Segundo Cuatrimestre
-------------------	----------------------

7. N° DE CRÉDITOS	6 (3 Teóricos + 3 Prácticos)
--------------------------	------------------------------

8. DEPARTAMENTO	Matemáticas
------------------------	-------------

9. ÁREA DE CONOCIMIENTO (*)	Matemática Aplicada
------------------------------------	---------------------

(*) Si la asignatura se imparte desde más de un Área de Conocimiento de manera compartida, indíquese posteriormente el número de créditos de cada tipo impartidos desde cada Área.

10. PROFESORADO
<u>Responsable/s de la materia</u>
David Orden Martín
<u>Resto del profesorado</u>
<u>Personal colaborador</u>

11. HORARIO
<u>Teoría</u>
Días de la semana y horas de comienzo y fin. Para todos los grupos.
<u>Práctica</u>
Horario de cada grupo de prácticas/laboratorio

12. LUGAR DE IMPARTICIÓN

Teoría

Aula/s, zona y edificio

Práctica

Laboratorio/s o Aula/s, zona y edificio

13. OBJETIVOS DOCENTES DE LA ASIGNATURA

- Introducir contenidos básicos de la Teoría de la Codificación de la Información
- Facilitar herramientas para estudiar la codificación y descodificación de la información.
- Estudiar la corrección de errores en una transmisión.
- Familiarizarse con los códigos correctores de errores utilizados en la práctica.
- Fomentar la capacidad de analizar, teórica y experimentalmente, distintos tipos de códigos.
- Favorecer el análisis crítico y la reflexión sobre los procesos que intervienen en la transmisión de la información.

14. CONTENIDO (PROGRAMA)**Parte Teórica****GRUPO TEMÁTICO 1: TEORÍA DE LA INFORMACIÓN (24 horas)****TEMA 1.- CÓDIGOS Y CODIFICACIÓN.**

Transmisión de la información. Codificación de alfabetos y mensajes. Descodificación. Ejemplos (códigos de barras, NIF).

TEMA 2.- MEDIDA DE LA INFORMACIÓN.

Fuentes de información. Entropía como medida de la información.

TEMA 3.- CANALES SIN RUIDO Y CANALES CON RUIDO.

Códigos óptimos. Construcción de códigos óptimos binarios. El papel del ruido. Errores y su corrección. Distancia de Hamming. Teorema de Shannon.

GRUPO TEMÁTICO 2: CÓDIGOS CORRECTORES DE ERRORES (24 horas)**TEMA 4.- CÓDIGOS LINEALES.**

Estructura. Matriz de control. Dualidad. Descodificación de códigos lineales. Códigos construidos a partir de otros. Códigos de Hamming. Cotas en los parámetros de un código.

TEMA 5.- CÓDIGOS CÍCLICOS.

Motivación. Matrices generatriz y de control. Ceros de un código cíclico. Descodificación. Errores a ráfagas. Códigos BCH y su decodificación.

GRUPO TEMÁTICO 3: CRIPTOLOGÍA (12 horas)

TEMA 6.- CRIPTOLOGÍA.

Sistemas criptográficos. Sistemas de clave privada. Sistemas de clave pública. El sistema criptográfico RSA.

Parte Práctica

PRÁCTICA 1: Códigos y codificación.

PRÁCTICA 2: Medida de la información.

PRÁCTICA 3: Canales sin ruido y canales con ruido.

PRÁCTICA 4: Códigos lineales.

PRÁCTICA 5: Códigos cíclicos.

PRÁCTICA 6: Criptología.

15. BIBLIOGRAFÍA

Bibliografía Básica

MUNUERA, C. y TENA, J. 1997. Codificación de la información. Universidad de Valladolid.

RIFÀ, J. y HUGUET, LL. 1991. Comunicación digital. Ed. Masson.

Bibliografía Complementaria

COVER, T. y THOMAS, J. 1991. Elements of information theory. Ed. John Wiley & Sons.

HILL, R. 1993. A first course in coding theory. Oxford Applied Mathematics and Computer Science Series.

FÚSTER, A., DE LA GUÍA, D., HERNÁNDEZ, L., MONTOYA, F. y MUÑOZ, J. 1997. Técnicas criptográficas de protección de datos. Ed. Ra-Ma.

16. CONOCIMIENTOS PREVIOS RECOMENDADOS

Es conveniente que el alumno esté familiarizado con los contenidos de las asignaturas

“Álgebra” y “Matemática discreta”.

17. METODOLOGÍA DE IMPARTICIÓN

Parte Teórica

Se utilizarán las siguientes metodologías de enseñanza-aprendizaje: Clase magistral, Tutorías, Actividades en grupo, Trabajos escritos y proyectos.

Asimismo, se utilizarán y estarán a disposición de los alumnos, los siguientes recursos didácticos: Pizarra, Proyector de transparencias, Ordenador y cañón, Página web de la asignatura, Aulas informáticas.

Parte Práctica

Se utilizarán las siguientes metodologías de enseñanza-aprendizaje: Resolución de problemas y casos, Prácticas de laboratorio, Tutorías, Actividades en grupo, Trabajos escritos y proyectos.

Asimismo, se utilizarán y estarán a disposición de los alumnos, los siguientes recursos didácticos: Pizarra, Proyector de transparencias, Ordenador y cañón, Página web de la asignatura, Aulas informáticas.

18. MÉTODOS Y CRITERIOS DE EVALUACIÓN

Parte Teórica

La parte teórica se evaluará conjuntamente con la parte práctica.

Parte Práctica

Se utilizarán los siguientes métodos de evaluación, con los pesos que se indican:

- Prueba escrita (50%)
- Exposición de proyectos individuales, prácticas y actividades en grupo (50%)

Los criterios de evaluación serán:

- Grado de comprensión de conceptos.
- Habilidad en el uso de procedimientos y técnicas.
- Capacidad de resolución de problemas.
- Corrección en los razonamientos y sus resultados.