

<b>1. TITULACIÓN</b>	Ingeniero en Informática
----------------------	--------------------------

<b>2. NOMBRE DE LA ASIGNATURA</b>	Codificación algebraica
-----------------------------------	-------------------------

<b>3. CÓDIGO DE LA ASIGNATURA</b>	78307
-----------------------------------	-------

<b>4. CARÁCTER</b>	Optativa
--------------------	----------

<b>5. CURSO</b>	Tercero
-----------------	---------

<b>6. PERIODO</b>	Segundo Cuatrimestre
-------------------	----------------------

<b>7. N° DE CRÉDITOS</b>	6 (3 Teóricos + 3 Prácticos)
--------------------------	------------------------------

<b>8. DEPARTAMENTO</b>	Matemáticas
------------------------	-------------

<b>9. ÁREA DE CONOCIMIENTO (*)</b>	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.

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

<b>11. HORARIO</b>
<b><u>Teoría y práctica:</u></b>
Sesión presencial los miércoles de 12 a 12:55. Resto de sesiones en el Aula virtual.

<b>12. LUGAR DE IMPARTICIÓN</b>
<b><u>Teoría</u></b>
Laboratorio EL2 y Aula virtual
<b><u>Práctica</u></b>
Laboratorio EL2 y Aula virtual

### **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 (36 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**

Códigos instantáneos. Longitud media. Eficacia. Construcción de códigos óptimos. Algoritmos dinámicos de tipo Ziv-Lempel.

##### **TEMA 4.- CANALES CON RUIDO**

El papel del ruido. Información mutua y capacidad de un canal. Canales simétricos. Corrección de errores. Distancia de Hamming. Teorema de Shannon.

#### **GRUPO TEMÁTICO 2: CÓDIGOS CORRECTORES DE ERRORES (18 horas)**

##### **TEMA 5.- CÓDIGOS LINEALES.**

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

## TEMA 6.- CÓDIGOS CÍCLICOS.

Motivación. Matrices generatriz y de control. Ceros de un código cíclico.

Descodificación. Errores a ráfagas. Códigos BCH y su descodificación.

### **GRUPO TEMÁTICO 3: CRIPTOLOGÍA (6 horas)**

## TEMA 7.- 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.

Se realizarán además varios trabajos consistentes en implementar algunos de los contenidos tratados, entre ellos códigos de barras, cantidad de información, códigos óptimos y algoritmos dinámicos.

## **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

No son necesarios conocimientos previos en especial. Ayudará haber cursado la asignatura “Fundamentos matemáticos: Álgebra”.

## 17. METODOLOGÍA DE IMPARTICIÓN

**El carácter de la asignatura será semipresencial.** Para ello se utilizará el Aula virtual de la Universidad de Alcalá, desde la que se distribuirán los materiales básicos, se establecerán las tareas a realizar, se debatirán los contenidos teóricos y prácticos y se proporcionarán materiales de profundización. Además se realizará una sesión presencial a la semana de puesta en común del trabajo realizado. Así, de las 4 horas semanales de carga docente, 3 tendrán carácter no presencial y 1 tendrá carácter presencial.

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

Asimismo se utilizarán y estarán a disposición de los alumnos los siguientes recursos didácticos: Pizarra, Ordenador y cañón proyector, Aula virtual y página web de la asignatura, Laboratorios informáticos.

## 18. MÉTODOS Y CRITERIOS DE EVALUACIÓN

**El método de evaluación se negociará con los alumnos,** que deberán llegar a una propuesta consensuada. Algunos de los elementos de evaluación que se podrían considerar son:

- Prácticas.
- Trabajos de implementación.
- Actividades en grupo.
- Participación activa.
- Prueba escrita.
- Otros propuestos por los alumnos.

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.
- Grado de implicación en la asignatura.