

## Transmisión de Datos y Criptografía

Código: 44734  
Créditos ECTS: 6

**2024/2025**

Titulación	Tipo	Curso
4318303 Investigación e Innovación en Ciencia e Ingeniería Basadas en Computadores	OT	0

### Contacto

Nombre: Guillermo Navarro Arribas  
Correo electrónico: guillermo.navarro@uab.cat

### Idiomas de los grupos

Puede consultar esta información al [final](#) del documento.

### Prerrequisitos

No hay requisitos formales previos. Se asumen conocimientos de posgrado en temas relacionados con la transmisión de datos.

### Objetivos y contextualización

El objetivo de esta asignatura es estudiar y profundizar en distintos temas de búsqueda de transmisión de datos. Para ello, la asignatura se centra en proporcionar una introducción a la investigación en tres bloques principales:

- la teoría de la codificación,
- la compresión de datos y
- la seguridad.

El alumnado conocerá conceptos avanzados de estos temas y será introducido en la investigación que se realiza en la actualidad.

### Resultados de aprendizaje

1. CA06 (Competencia) El graduado o graduada será capaz de diseñar sistemas fiables, eficientes y seguros de transmisión y almacenamiento de datos, usando códigos correctores de errores, y técnicas de compresión y seguridad.
2. CA06 (Competencia) El graduado o graduada será capaz de diseñar sistemas fiables, eficientes y seguros de transmisión y almacenamiento de datos, usando códigos correctores de errores, y técnicas de compresión y seguridad.
3. CA07 (Competencia) El graduado o graduada será capaz de planificar y desarrollar proyectos de investigación con contenido dentro del área del tratamiento de la información.
4. CA07 (Competencia) El graduado o graduada será capaz de planificar y desarrollar proyectos de investigación con contenido dentro del área del tratamiento de la información.
5. KA16 (Conocimiento) El graduado o graduada será capaz de describir diferentes sistemas para la corrección de errores aplicados a la criptografía post cuántica, y basados en códigos LDPC.

6. KA17 (Conocimiento) El graduado o graduada será capaz de describir diferentes métodos de compresión utilizados para datos IoT, de redes sociales, telepresencia, nubes de puntos e imágenes médicas.
7. KA18 (Conocimiento) El graduado o graduada será capaz de describir diferentes métodos criptográficos basados en curvas elípticas y utilizados en la tecnología blockchain, así como métodos para garantizar la privacidad de los datos.
8. SA21 (Habilidad) Ser capaz de aplicar diferentes métodos de codificación para la corrección de errores utilizados en el campo de la criptografía post cuántica y transmisiones masivas de datos.
9. SA22 (Habilidad) Ser capaz de aplicar diferentes algoritmos de compresión para distintos tipos de datos.
10. SA23 (Habilidad) Ser capaz de aplicar diferentes mecanismos de criptografía, basados en curvas elípticas y tecnología blockchain, y privacidad de datos.

## Contenido

Los contenidos principales del curso están divididos en los tres bloques principales de la asignatura:

- Teoría de códigos: Códigos de corrección de errores aplicados a la estenografía y criptografía postcuántica y códigos LDPC utilizados, p.e. en la televisión digital.
- Compresión de datos: compresión para diferentes tipos de datos, tales como Internet de las cosas, redes sociales, telepresencia, imágenes médicas y técnicas basadas en el aprendizaje automático.
- Seguridad y privacidad: criptografía de curvas elípticas, tecnología blockchain y su aplicación a criptomonedas, privacidad de datos.

En función de los antecedentes e intereses del alumnado, estos tendrán la oportunidad de profundizar más o menos en determinados temas.

## Actividades formativas y Metodología

Título	Horas	ECTS	Resultados de aprendizaje
<b>Tipo: Dirigidas</b>			
Estudio para tests y presentaciones	15	0,6	
Preparación the trabajos escritos	25	1	
Sessiones dirigidas por el profesorado	45	1,8	
<b>Tipo: Supervisadas</b>			
Actividades presenciales	15	0,6	
<b>Tipo: Autónomas</b>			
Preparación de tests de síntesis	15	0,6	
Trabajo y preparación de clases	35	1,4	

La metodología de este curso está diseñada para exponer a los estudiantes a algunos de los temas de investigación relevantes en las áreas de la teoría de la codificación, la compresión de datos y la seguridad. Se basará en el concepto "aprender haciendo", y se adaptará al número de alumnos que se matriculen en el

curso. Por lo general, habrá una combinación de sesiones teóricas y prácticas, incluyendo clases magistrales, trabajos por parte de los estudiantes, presentaciones y trabajo colaborativo.

Nota: se reservarán 15 minutos de una clase dentro del calendario establecido por el centro o por la titulación para que el alumnado rellene las encuestas de evaluación de la actuación del profesorado y de evaluación de la asignatura o módulo.

## Evaluación

### Actividades de evaluación continuada

Título	Peso	Horas	ECTS	Resultados de aprendizaje
Test de síntesis	30%	0	0	CA06, CA07, KA16, KA17, KA18, SA21, SA22, SA23
Trabajos	70%	0	0	CA06, CA07, KA16, KA17, KA18, SA21, SA22, SA23

Se quiere adoptar una metodología de evaluación que sea suficientemente flexible para adaptarse al trabajo concreto realizado en clase, esto significa que puede variar ligeramente de un curso a otro. La evaluación se basará en 2 tipos de actividades diferenciadas:

- Trabajos: se propondrán distintos trabajos al alumnado durante el curso. Estos pueden incluir trabajos individuales y en grupo y pueden tener una orientación teórica o práctica. Pueden ser ejemplos: ejercicios, estudio y exposición de un tema relacionado con la asignatura, prácticas, ...
- Prueba de síntesis: se utilizarán pruebas de síntesis como actividad de evaluación individual. Estas pruebas pueden sustituirse por otras actividades de evaluación si, por ejemplo, el número de alumnos es bajo.

A principio de curso se explicará con detalle las actividades de evaluación.

## Bibliografía

La bibliografía se facilitará al inicio del curso. Dado el carácter dinámico de los temas a presentar, la bibliografía específica se modificará en cada curso para adaptarla al estado del arte actual de la investigación en esta área. Por lo general, incluirá artículos relevantes.

## Software

Se facilitará al inicio del curso.

## Lista de idiomas

Nombre	Grupo	Idioma	Semestre	Turno
(PLABm) Prácticas de laboratorio (máster)	1	Inglés	segundo cuatrimestre	mañana-mixto

