

Guía docente

230300 - COMSECRET - Álgebra Lineal, Códigos Lineales y Esquemas de Compartición de Secretos

Última modificación: 24/03/2026

Unidad responsable: Escuela Técnica Superior de Ingeniería de Telecomunicación de Barcelona

Unidad que imparte: 749 - MAT - Departamento de Matemáticas.

Titulación: GRADO EN INGENIERÍA DE TECNOLOGÍAS Y SERVICIOS DE TELECOMUNICACIÓN (Plan 2015). (Asignatura optativa).

GRADO EN INGENIERÍA ELECTRÓNICA DE TELECOMUNICACIÓN (Plan 2018). (Asignatura optativa).

Curso: 2026

Créditos ECTS: 2.0

Idiomas: Catalán

PROFESORADO

Profesorado responsable: GERMAN SAEZ MORENO

Otros: Primer quadrimestre:
FRANCISCO JAVIER MUÑOZ LOPEZ - 10
GERMAN SAEZ MORENO - 10

CAPACIDADES PREVIAS

Conceptos y técnicas básicas de álgebra lineal.

METODOLOGÍAS DOCENTES

El seminario combina sesiones de teoría y de problemas, y de aplicación práctica en sesiones de laboratorio.

OBJETIVOS DE APRENDIZAJE DE LA ASIGNATURA

El objetivo del seminario es hacer una breve introducción, utilizando métodos elementales del álgebra lineal, a algunos objetos y técnicas de la ingeniería de telecomunicaciones que son centrales en el diseño de sistemas de comunicaciones fiables y seguros, llegando al planteamiento de problemas punteros de investigación en estos campos. Concretamente, se presentarán las nociones más básicas sobre los códigos binarios lineales correctores de errores y los protocolos criptográficos de compartición de secretos, así como una introducción a la criptografía de clave pública.

HORAS TOTALES DE DEDICACIÓN DEL ESTUDIANTE

Tipo	Horas	Porcentaje
Horas aprendizaje autónomo	30,0	60.00
Horas grupo grande	20,0	40.00

Dedicación total: 50 h

CONTENIDOS

Introducción a la aritmética modular.

Descripción:

Introducción a la aritmética modular poniendo énfasis en la aritmética que no se trata en otras asignaturas. Espacios vectoriales sobre el cuerpo finito de dos elementos y otros cuerpos finitos.

Dedicación: 5h

Grupo grande/Teoría: 5h

Introducción a los esquemas de compartición de secretos.

Descripción:

Introducción a los esquemas de compartición de secretos. Esquemas lineales vectoriales sobre el cuerpo finito de dos elementos. Proceso de distribución del secreto y proceso de reconstrucción. Seguridad del esquema. Conjuntos autorizados. Estudio de algun problema abierto.

Dedicación: 5h

Grupo grande/Teoría: 5h

Introducción a los códigos correctores de errores.

Descripción:

Introducción a los códigos correctores de errores. Códigos lineales en espacios vectoriales sobre el cuerpo finito de dos elementos. Matriz generadora y matriz de control. Codificación y decodificación. Distancia de Hamming. Detección y corrección de errores.

Dedicación: 5h

Grupo grande/Teoría: 5h

Introducción a la criptografía.

Descripción:

Introducción a la criptografía. Historia. Métodos criptográficos clásicos. Criptografía de clave pública. RSA. Firma y autenticación. Trabajo final práctico combinando las tres técnicas introducidas.

Dedicación: 5h

Grupo grande/Teoría: 5h

SISTEMA DE CALIFICACIÓN

Cualquier acto de fraude académico, plagio o uso o mera tenencia al alcance de medios no autorizados en cualquier actividad de evaluación comportará la calificación de cero (0) en la prueba o entrega afectada. Además, de acuerdo con la normativa de la Universidad, la posible derivación de los hechos para la apertura de un expediente disciplinario implicará que la asignatura quede en el estado provisional de "pendiente de evaluación" hasta la resolución del expediente. La gestión de estas incidencias se lleva a cabo de acuerdo con el [Marco de actuación para la integridad académica en la evaluación de la UPC](#).

La nota se obtendrá de la valoración de las actividades realizadas durante el curso (participación activa durante las sesiones, entrega de ejercicios o realización de actividades guiadas). En su caso, la nota así obtenida se podrá mejorar con un control al final del seminario.



BIBLIOGRAFÍA

Básica:

- Biggs, N.L. Matemática discreta. Barcelona: Vicens-Vives, 1994. ISBN 8431633115.