Guía docente
230358 - BMAC - Principios Matemáticos para Códigos Algebraicos con Aplicaciones a la Criptografía

Última modificación: 29/04/2020

Unidad responsable: Escuela Técnica Superior de Ingeniería de Telecomunicación de Barcelona
Unidad que imparte: 749 - MAT - Departamento de Matemáticas.

Titulación: MÁSTER UNIVERSITARIO EN INGENIERÍA DE TELECOMUNICACIÓN (Plan 2013). (Asignatura optativa).

Curso: 2020 **Créditos ECTS:** 2.5 **Idiomas:** Inglés

PROFESORADO

Profesorado responsable: Jorge Jimenez

Otros: Marcel Fernandez
Jorge Jimenez

COMPETENCIAS DE LA TITULACIÓN A LAS QUE CONTRIBUYE LA ASIGNATURA

Específicas:
CE1. Capacidad para aplicar métodos de la teoría de la información, la modulación adaptativa y codificación de canal, así como técnicas avanzadas de procesado digital de señal a los sistemas de comunicaciones y audiovisuales.
CE4. Capacidad para diseñar y dimensionar redes de transporte, difusión y distribución de señales multimedia.
CE8. Capacidad de comprender y saber aplicar el funcionamiento y organización de Internet, las tecnologías y protocolos de Internet de nueva generación, los modelos de componentes, software intermediario y servicios.
CE9. Capacidad para resolver la convergencia, interoperabilidad y diseño de redes heterogéneas con redes locales, de acceso y troncales, así como la integración de servicios de telefonía, datos, televisión e interactivos.
CE15. Capacidad para la integración de tecnologías y sistemas propios de la Ingeniería de Telecomunicación, con carácter generalista, y en contextos más amplios y multidisciplinares como por ejemplo en bioingeniería, conversión fotovoltaica, nanotecnología, telemedicina.

Transversales:
CT1a. EMPRENDIMIENTO E INNOVACIÓN: Conocer y entender la organización de una empresa y las ciencias que rigen su actividad; tener capacidad para entender las normas laborales y las relaciones entre la planificación, las estrategias industriales y comerciales, la calidad y el beneficio.

CT2. SOSTENIBILIDAD Y COMPROMISO SOCIAL: Conocer y comprender la complejidad de los fenómenos económicos y sociales típicos de la sociedad del bienestar; tener capacidad para relacionar el bienestar con la globalización y la sostenibilidad; lograr habilidades para utilizar de forma equilibrada y compatible la técnica, la tecnología, la economía y la sostenibilidad.
CT3. TRABAJO EN EQUIPO: Ser capaz de trabajar como miembro de un equipo interdisciplinar, ya sea como un miembro más o realizando tareas de dirección, con la finalidad de contribuir a desarrollar proyectos con pragmatismo y sentido de la responsabilidad, asumiendo compromisos teniendo en cuenta los recursos disponibles.

CT4. USO SOLVENTE DE LOS RECURSOS DE INFORMACIÓN: Gestionar la adquisición, la estructuración, el análisis y la visualización de datos e información en el ámbito de especialidad, y valorar de forma crítica los resultados de dicha gestión.

CT5. TERCERA LENGUA: Conocer una tercera lengua, preferentemente el inglés, con un nivel adecuado oral y escrito y en consonancia con las necesidades que tendrán los titulados y tituladas.

METODOLOGÍAS DOCENTES

- Lectures
- Application classes
- Exercises
- Oral presentations
- Other activities

OBJETIVOS DE APRENDIZAJE DE LA ASIGNATURA

Learning objectives of the subject:
The aim of this course is to train the students in the knowledge of the actual mathematics used in coding theory and cryptography. They will learn the most modern applications and will be able to follow new research in engineering security and coding theory.

Learning results of the subject:
- Ability to understand mathematics on finite fields, algebraic curves and basic factorization algorithms as Berlekamp.
- Ability to understand the new algorithms for coding and cryptography
- Ability to analysis current developments in geometric coding theory and its applications to information security
- Ability to analyse, model and apply advanced techniques both security, including cryptographic protocols, as identifying traitors.

HORAS TOTALES DE DEDICACIÓN DEL ESTUDIANTADO

Tipo	Horas	Porcentaje
Horas grupo grande	20,0	32.00
Horas aprendizaje autónomo	42,5	68.00

Dedicación total: 62.5 h

CONTENIDOS

1. Finite fields

Descripción:
- Properties
- Existence and uniqueness
- Extensions
- Ring of polynomials over finite fields

? Ring of polynomials over finite fields

Dedicación: 12h
Grupo grande/Teoría: 3h
Grupo mediano/Prácticas: 1h
Aprendizaje autónomo: 8h

2. Algebraic curves over finite fields

Descripción:
- Basic properties: smooth and singular curves
- Zeta functions and curves with many rational points, Hasse-Weil Theorem
- Funciton fields
- Riemann Roch
- Examples

Dedicación: 12h
Grupo grande/Teoría: 3h
Grupo mediano/Prácticas: 1h
Aprendizaje autónomo: 8h

3. Polynomial Arithmetic

Descripción:
- Basic arithmetic
- Resultant and discriminants
- Basic Factorization algorithms

Dedicación: 11h
Grupo grande/Teoría: 2h
Grupo mediano/Prácticas: 1h
Aprendizaje autónomo: 8h

4. Error Correcting Codes

Descripción:
- Basics of error correction.
- Polynomial codes. Reed Solomon codes.
- Classical decoding. Berlekamp-Massey Algorithm

Dedicación: 11h
Grupo grande/Teoría: 2h
Grupo mediano/Prácticas: 1h
Aprendizaje autónomo: 8h

5. List Decoding

Descripción:
- List decoding vs Minimum distance decoding
- Guruswami-Sudan algorithm
- Koetter-Vardy algorithm

Dedicación: 12h
Grupo grande/Teoría: 3h
Grupo mediano/Prácticas: 1h
Aprendizaje autónomo: 8h

6. Applications of List Decoding

Descripción:
- Traceability codes
- Tracing algorithms

Dedicación: 4h 30m
Grupo grande/Teoría: 2h 30m
Aprendizaje autónomo: 2h

SISTEMA DE CALIFICACIÓN

Exercises: 50%
Oral presentation: 50%

Exercises:
- Description: Exercises to strengthen the theoretical knowledge.
Oral presentation:
- Description: Presentation of a work group.

BIBLIOGRAFÍA

Básica:
- McEliece, R. J. Finite fields for computer scientists and engineers. Boston etc.: Kluwer Academic Publishers, 1987. ISBN 0898381916.
- Fernandez, M.; Moreira, J.; Soriano, M. "Identifying Traitors Using the Koetter-Vardy Algorithm". IEEE Transactions on Information Theory [en línea]. vol. 57, no. 2, February 2011 [Consulta: 22/11/2016]. Disponible a: http://ieeexplore.ieee.org/document/5695104/.
- Koetter, R.; Vardy, A. "Algebraic soft-decision decoding of Reed-Solomon codes". IEEE Transactions on Information Theory [en línea]. vol. 49, no. 11, November 2003 [Consulta: 22/11/2016]. Disponible a: http://ieeexplore.ieee.org/document/1246007/.
- Guruswami, V. "Improved Decoding of Reed-Solomon and Algebraic-Geometry Codes". IEEE Transactions on Information Theory [en línea]. 1999, vol. 45, no. 6, p. 1757-1767 [Consulta: 22/11/2016]. Disponible a: http://ieeexplore.ieee.org/document/782097/.

RECURSOS

Otros recursos:
- J.W.P. Hirschfeld, G. Korchmáros & F. Torres, Algebraic Curves over a Finite Field eBook | ISBN: 9781400847419 |
- Judy Walker, ?Codes and Curves?,
Online: http://www.math.unl.edu/ jwalker7/papers/rev.pdf