



Guia docent

230358 - BMAC - Principis Matemàtics per a Codis Algebraics amb Aplicacions a la Criptografia

Última modificació: 11/05/2022

Unitat responsable: Escola Tècnica Superior d'Enginyeria de Telecomunicació de Barcelona
Unitat que imparteix: 749 - MAT - Departament de Matemàtiques.

Titulació: **Curs:** 2022 **Crèdits ECTS:** 2.5
Idiomes: Anglès

PROFESSORAT

Professorat responsable: Jorge Jimenez

Altres: Marcel Fernandez
Jorge Jimenez

COMPETÈNCIES DE LA TITULACIÓ A LES QUALS CONTRIBUEIX L'ASSIGNATURA

Específiques:

CE1. Capacitat per aplicar mètodes de la teoria de la informació, la modulació adaptativa i codificació de canal, així com tècniques avançades de processat digital del senyal als sistemes de comunicacions i audiovisuals.

CE4. Capacitat per dissenyar i dimensionar xarxes de transport, difusió i distribució de senyals multimèdia.

CE8. Capacitat de comprendre i saber aplicar el funcionament i organització d'Internet, les tecnologies i protocols d'Internet de nova generació, els models de components, software intermediari i serveis.

CE9. Capacitat per resoldre la convergència, interoperabilitat i disseny de xarxes heterogènies amb xarxes locals, d'accés i troncs, així com la integració de serveis de telefonia, dades, televisió i interactius.

CE15. Capacitat per a la integració de tecnologies i sistemes propis de la Enginyeria de Telecomunicació, amb caràcter generalista, i en contextos més amplis i multidisciplinaris com per exemple en bio-enginyeria, conversió fotovoltaica, nanotecnologia o telemedicina.

Transversals:

CT1a. EMPRENEDORIA I INNOVACIÓ: Conèixer i comprendre l'organització d'una empresa i les ciències que en regeixen l'activitat; tenir capacitat per comprendre les regles laborals i les relacions entre la planificació, les estratègies industrials i comercials, la qualitat i el benefici.

CT2. SOSTENIBILITAT I COMPROMÍS SOCIAL: Conèixer i comprendre la complexitat dels fenòmens econòmics i socials típics de la societat del benestar; tenir capacitat per relacionar el benestar amb la globalització i la sostenibilitat; assolir habilitats per usar de forma equilibrada i compatible la tècnica, la tecnologia, l'economia i la sostenibilitat.

CT3. TREBALL EN EQUIP: Ser capaç de treballar com a membre d'un equip interdisciplinari, ja sigui com un membre més o duent a terme tasques de direcció, amb la finalitat de contribuir a desenvolupar projectes amb pragmatisme i sentit de la responsabilitat, tot assumint compromisos considerant els recursos disponibles.

CT4. ÚS SOLVENT DELS RECURSOS D'INFORMACIÓ: Gestionar l'adquisició, l'estructuració, l'anàlisi i la visualització de dades i informació de l'àmbit d'especialitat, i valorar de forma crítica els resultats d'aquesta gestió.

CT5. TERCERA LLENGUA: Conèixer una tercera llengua, preferentment l'anglès, amb un nivell adequat oral i escrit i en consonància amb les necessitats que tindran els titulats i titulades.

METODOLOGIES DOCENTS

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

OBJECTIUS D'APRENTATGE DE L'ASSIGNATURA

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.

HORES TOTS DE DEDICACIÓ DE L'ESTUDIANTAT

Tipus	Hores	Percentatge
Hores grup gran	20,0	32.00
Hores aprenentatge autònom	42,5	68.00

Dedicació total: 62.5 h

CONTINGUTS

1. Finite fields

Descripció:

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

Dedicació: 12h

Grup gran/Teoria: 3h

Grup mitjà/Pràctiques: 1h

Aprenentatge autònom: 8h



2. Algebraic curves over finite fields

Descripció:

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

Dedicació: 12h

Grup gran/Teoria: 3h

Grup mitjà/Pràctiques: 1h

Aprenentatge autònom: 8h

3. Polynomial Arithmetic

Descripció:

- Basic arithmetic
- Resultant and discriminants
- Basic Factorization algorithms

Dedicació: 11h

Grup gran/Teoria: 2h

Grup mitjà/Pràctiques: 1h

Aprenentatge autònom: 8h

4. Error Correcting Codes

Descripció:

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

Dedicació: 11h

Grup gran/Teoria: 2h

Grup mitjà/Pràctiques: 1h

Aprenentatge autònom: 8h

5. List Decoding

Descripció:

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

Dedicació: 12h

Grup gran/Teoria: 3h

Grup mitjà/Pràctiques: 1h

Aprenentatge autònom: 8h



6. Applications of List Decoding

Descripció:

- Traceability codes
- Tracing algorithms

Dedicació: 4h 30m

Grup gran/Teoria: 2h 30m

Aprenentatge autònom: 2h

SISTEMA DE QUALIFICACIÓ

Exercises: 50%

Oral presentation: 50%

Exercises:

- Description: Exercises to strengthen the theoretical knowledge.

Oral presentation:

- Description: Presentation of a work group.

BIBLIOGRAFIA

Bàsica:

- 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 línia]. 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 línia]. 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 línia]. 1999, vol. 45, no. 6, p. 1757-1767 [Consulta: 22/11/2016]. Disponible a:

<http://ieeexplore.ieee.org/document/782097/>.

RECURSOS

Altres 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>