Curso Académico 2014-15

ÁLGEBRA APLICADA Y CRIPTOGRAFÍA

Ficha Docente

ASIGNATURA

Nombre de asignatura (Código GeA): ÁLGEBRA APLICADA Y CRIPTOGRAFÍA (800697)
Créditos: 6
Créditos presenciales: 6
Créditos no presenciales:
Semestre: 1

PLAN/ES DONDE SE IMPARTE

Titulación: GRADO EN INGENIERÍA MATEMÁTICA
Plan: GRADO EN INGENIERÍA MATEMÁTICA
Curso: 3 **Ciclo:** 1
Carácter: OBLIGATORIA
Duración/es: Primer cuatrimestre (actas en Feb. y Sep.), Por determinar (no genera actas)
Idioma/s en que se imparte:
Módulo/Materia: CONTENIDOS INTERMEDIOS/APLICACIONES DEL ÁLGEBRA Y DE LA GEOMETRÍA

PROFESOR COORDINADOR

Nombre	Departamento	Centro	Correo electrónico	Teléfono

PROFESORADO

Nombre	Departamento	Centro	Correo electrónico	Teléfono
ALONSO GARCIA, MARIA EMILIA	Álgebra	Facultad de Informática	mariemi@ucm.es	

SINOPSIS

BREVE DESCRIPTOR:

Complejidad de algoritmos en álgebra. Cuerpos finitos. Criptografía de clave pública. Resultante de polinomios. Cáculo simbólico con números algebraicos. Ideales en el anillo de polinomios, bases de Groebner y aplicaciones.

REQUISITOS:

Asignatura de Estructuras algebraicas

OBJETIVOS:

Familiarizar al alumno con el álgebra que se utiliza en la teoría de la información y en la modelización geométrica.

COMPETENCIAS:

Generales

Reconocer los problemas y soluciones en Criptografía de clave pública, y en modelización geométrica con polinomios. Capacidad para desarrollar un programa en Maple en esos temas.

Transversales:

Específicas:

Conocer y manejar algoritmos en álgebra.
Construir algoritmos en álgebra en un lenguaje de programación.

Otras:

CONTENIDOS TEMÁTICOS:

Algoritmos en teoría de números: factorización y primalidad.

Algoritmos del álgebra que se utilizan en modelización geométrica. Bases de Gröebner.

ACTIVIDADES DOCENTES:

Clases teóricas:
50% = 30 h
Seminarios:
5%
Clases prácticas:
20%
Trabajos de campo:

Prácticas clínicas:

Laboratorios:
Prácticas de laboratorio: 15%
Exposiciones:

Presentaciones:

Otras actividades:
Presentación de un trabajo de implementación en Maple.
Resolución de problemas en grupo: 10%
TOTAL:

EVALUACIÓN:
Examen de cuestiones teóricas y ejercicios (70%) que será indispensable aprobar, y entrega de ejercicios a lo largo del año junto con trabajo de implementación que habrá que exponer (20%), dependiendo del número de alumnos.

BIBLIOGRAFÍA BÁSICA:

-J. Buchmann: Introduction to Cryptography. Undergraduate Texts in Mathematics. Springer-Verlag, 2nd. ed. 2004.
--D. Cox, J. little, D. O'Shea: Ideals, Varieties and Algorithms. Undergraduate Texts in Mathematics, Springer-Verlag, 3rd. ed. 2007.
-- R. Lidl, G. Pilz: Applied Abstract Algebra. Undergraduate Texts in Mathematics,Springer-Verlag, 2nd. ed. 1997.
- W. Trappe, L. Washington: Introduction to cryptography with coding theory. Edit. Pearson Higher, 2nd Ed. USA, 2005.
BIBLIOGRAFIA COMPLEMENTARIA
--Tilborg C.A. Henk. Fundamentals of Cryptology. Kluwer Acad. Publisher, 2000.
--Bruce W. Char , K.O. Gedde, Gaston H. Gonnet , B. Leong, M.B. Monagan, , S.M. Wat . Maple V Reference Manual. Springer-Verlag, 1991.
- Hojas de ejercicios con explicaciones.

OTRA INFORMACIÓN RELEVANTE