Curso Académico 2018-19

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: Por determinar (no genera actas), Primer cuatrimestre (actas en Feb. y Jul.)
Idioma/s en que se imparte: Español
Módulo/Materia: CONTENIDOS INTERMEDIOS/APLICACIONES DEL ÁLGEBRA Y DE LA GEOMETRÍA

PROFESOR COORDINADOR

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

PROFESORADO

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

SINOPSIS

BREVE DESCRIPTOR:

Complejidad de algoritmos en Álgebra. Cuerpos finitos. Códigos Correctores. Criptografía de clave Pública. Criptografía de clave privada: Cifrado en flujo y cifrado en bloque. Implementación en Maple o Sage.

REQUISITOS:

Conocimientos básicos sobre las estructuras algebraicas: grupos, cuerpos, anillos.

OBJETIVOS:

Conocer las matemáticas que hay detrás de los algoritmos de seguridad en las comunicaciones anónimas a distancia, más usados actualmente. Asimismo de los métodos de correción de señales digitales.

COMPETENCIAS:

Generales

1. Saber aplicar los conocimientos adquiridos y desarrollar la capacidad en la resolución de problemas en entornos nuevos o pocos conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con el Álgebra, el Análisis Matemático, la Geometría y Topología o la Matemática Aplicada.
2. Utilizar con soltura herramientas de búsqueda de recursos bibliográficos.
3. Saber trabajar en equipo y gestionar el tiempo de trabajo.

Transversales:

Familiarizarse con algún sistema de software de cálculo simbólico. (Maple o SAGE).

Específicas:

--Entender las matemáticas que hay detrás de los algoritmos de seguridad en las comunicaciones anónimas a distancia, más usados actualmente. Asimismo los métodos de correción de señales digitales.
--Saber analizar y construir demostraciones, así como transmitir conocimientos matemáticos avanzados.
--Saber elegir, utilizar aplicaciones informáticas, de cálculo numérico y simbólico, para experimentar en matemáticas y resolver problemas.

Otras:

CONTENIDOS TEMÁTICOS:

1.Ampliación de estructuras algebraicas: extensiones de cuerpos y cuerpos finitos.
2. Algoritmos básicos en Álgebra y su complejidad. Test de primalidad. Jerarquía de complejidad d e problemas. P versus NP
3. Códigos correctores de errores. Códigos lineales y cíclicos. Códigos BCH.
4. Criptografía de clave privada. Cifrado en flujo: LFSR's.
5. Criptografía de clave pública. Sistemas basados en el problema del logaritmo discreto (DLP). Ataques.
6. Criptografía de clave pública. RSA. Sistemas basados en el problema de la factorización de enteros. Algoritmos de factorización.
7. Firma digital (DSS) y autenticidad: PKI's. Diversos protocolos. Protocolos de prueba sin conocimiento.

ACTIVIDADES DOCENTES:

Clases teóricas:
De 2 a 3 horas por semana.
Seminarios:

Clases prácticas:
Ejercicios en clases prácticas
Trabajos de campo:

Prácticas clínicas:

Laboratorios:
Prácticas de laboratorio una vez por semana.
Exposiciones:

Presentaciones:
Presentación final del trabajo en grupos a lo largo del mes de enero, a modo de conferencia.
Otras actividades:

TOTAL:

EVALUACIÓN:

Evaluación:
Examen de cuestiones teóricas y ejercicios (de 70 a 75%). Será indispensable obtener 5 sobre 10 en el examen para aprobar la asignatura. Entrega de ejercicios teóricos y realizados con herramientas informáticas a lo largo del curso (hasta 5%). Elaboración de un trabajo final en grupos de 3 a 5 alumnos consistente en la implementación de ciertos algoritmos criptográficos y sus protocolos. La exposición de dicho trabajo será pública y en esta los alumnos, para obtener un aprobado, deberán mostrar tanto el conocimiento de los algoritmos subyacentes como la implementación presentada.El profesor podrá hacer en este sentido hasta media hora d e preguntas para cerciorarse de que se cu,mplen los requisitos anteriores. La evaluación del trabajo práctico será individual.

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. Undergradauate Texts in Mathematics. Springer-Verlag, 3rd. ed 2007.
J.L. Gómez- Pardo: Introduction to Cryptography with Maple. Springer- Verlag 2013.
N. Koblitz: Computational Number Theory and Cryptography. 2nd. ed. Springer-Verlag 1994 (reprinted 2012)
R. Lidl, G. Pilz: Applied Abstract Algebra. Undergraduate Texts in Mathematics. Springer-Veralg, 2nd. Ed. 1997.
D. R. Stinson: Cryptography Theory and Practice. 3rd. ed. In ¿Discrete Mathematics and its Applications. Taylor&Francis., LLC, CRC Press (2005).

Bibliografía Complementaria :

J. Menezes, P.C. van Orschot, S. A. Vanstone: Handbook of Applied Cryptography. CRC Press, (1996), 5th printing 2001.
N. P. Smart: Cryptography made simple. Springer-Verlag 2016. (a través de la Bibl. de la UCM:
---
http://link.springer.com/book/10.1007/978-3-319-21936-3).
C.A. H. Tilborg: Fundamentals of Cryptology. Kluwe Academic Publisher, 2000.
W. Trappe, L. Washington: Cryptography with Coding Theory. Prentice Hall, 2nd.ed.(2005).

OTRA INFORMACIÓN RELEVANTE