Plan 394 GRADO DE MATEMATICAS

Asignatura 40035 CRIPTOGRAFIA

Grupo 1

Tipo de asignatura (básica, obligatoria u optativa)

Asignatura optativa.

Créditos ECTS

Seis (6)

Competencias que contribuye a desarrollar

GENERALES

G1. Demostrar poseer y comprender conocimientos en el área de las Matemáticas a partir de la base de la educación secundaria general, a un nivel que, apoyado en libros de texto avanzados, incluye también algunos aspectos que implican conocimientos procedentes de la vanguardia en el estudio de las Matemáticas.

G2. Saber aplicar los conocimientos matemáticos a su trabajo o vocación de una forma profesional y poseer las competencias que suelen demostrarse por medio de la elaboración y defensa de argumentos y la resolución de problemas dentro del área de las Matemáticas.

G3. Tener la capacidad de reunir e interpretar datos relevantes, dentro del área de las Matemáticas, para emitir juicios que incluyan una reflexión sobre temas relevantes de índole social, científica o ética.

G4. Poder transmitir, tanto de forma oral como escrita, información, ideas, conocimientos, problemas y soluciones del ámbito matemático a un público tanto especializado como no especializado.

G5. Haber desarrollado aquellas habilidades de aprendizaje necesarias para emprender estudios posteriores en Matemáticas con un alto grado de autonomía.

G6. Utilizar bibliografía y herramientas de búsqueda de recursos bibliográficos en Matemáticas, incluyendo los recursos telemáticos.

G7. Leer y comprender textos científicos tanto en lengua propia como en otras de relevancia en el ámbito científico, especialmente la inglesa.

G8. Conocer y utilizar recursos informáticos de carácter general y tecnologías de la información y las comunicaciones como medios de comunicación, organización, aprendizaje e investigación.

G9. Gestionar de forma óptima, tanto en el trabajo individual como en equipo, el tiempo de trabajo y organizar los recursos disponibles, estableciendo prioridades, caminos alternativos e identificando errores lógicos en la toma de decisiones.

G10. Tener la capacidad de trabajar en equipo, aportando orden, abstracción y razonamiento lógico; comprobando o refutando razonadamente los argumentos de otras personas y contribuyendo con profesionalidad al buen funcionamiento y organización del grupo.

ESPECIFICAS

E1. Comprender y utilizar el lenguaje matemático. Adquirir la capacidad para enunciar proposiciones en distintos campos de las Matemáticas, para construir demostraciones y para transmitir los conocimientos matemáticos adquiridos.

E2. Conocer demostraciones rigurosas de algunos teoremas clásicos en distintas áreas de las Matemáticas.

E3. Asimilar la definición de un nuevo objeto matemático, en términos de otros ya conocidos, y ser capaz de utilizar este objeto en diferentes contextos

E4. Saber abstraer las propiedades estructurales (de objetos matemáticos, de la realidad observada, y de otros ámbitos) distinguiéndolas de aquellas puramente ocasionales y poder comprobarlas con demostraciones o refutarlas con contraejemplos, así como identificar errores en razonamientos incorrectos.

E5. Capacitar para el aprendizaje autónomo de nuevos conocimientos y técnicas.

E6. Resolver problemas de Matemáticas, mediante habilidades de cálculo básico y otras técnicas.

E7. Proponer, analizar, validar e interpretar modelos de situaciones reales sencillas, utilizando las herramientas matemáticas más adecuadas a los fines que se persigan.

E8. Planificar la resolución de un problema en función de las herramientas de que se disponga y de las restricciones de tiempo y recursos.

E9. Utilizar aplicaciones informáticas de análisis estadístico, cálculo numérico y simbólico, visualización gráfica, optimización u otras para experimentar en Matemáticas y resolver

problemas.
E10. Desarrollar programas que resuelvan problemas matemáticos utilizando para cada caso el entorno

Objetivos/Resultados de aprendizaje

Proporcionar al alumno una visión general de los problemas y métodos de la Criptografía , su desarrollo histórico y su estado actual, así como sus aplicaciones, con especial énfasis en los aspectos y herramientas matemáticas que emplea, poniendo de relieve los métodos propios de investigación en la especialidad.

1-Conocer la evolución histórica de la Criptografía , sus objetivos y problemas centrales y las técnicas empleadas.

2.- Conocer las herramientas matemáticas utilizadas en Criptográfia clásica y en los desarrollos más recientes de la misma.

.3-. Familiarizarse con los principales sistemas criptográficos tanto de clave pública como de clave privada.

4.- Analizar la seguridad y los posibles ataques de cada sistema criptográfico.

5- Mostrar la aplicación de las técnicas criptográficas anteriores a problemas concretos: firma digital, votaciones electrónicas, comunicaciones móviles, etc.

6- Implementar en ordenador algunos de los algoritmos examinados

Contenidos

Evolución histórica de la Criptograf ¡a y el Criptoanálisis.. Criptografía de Clave Privada y de Clave Pública. Principales sistemas criptográficos actuales en clave pública y privada. Criptografía elíptica y aplicaciones. .Protocolos criptográficos: Métodos de autentificación, Firma Digital, etc..

Principios Metodológicos/Métodos Docentes

El desarrollo de la asignatura combinará las clases teóricas con la resolución de ejercicios en grupo, la preparación y exposición de temas, la implementación en ordenador de algunos de los sistemas y protocolos criptográficos y el trabajo de tutorías.

Criterios y sistemas de evaluación

La calificación se obtendrá como combinación de un examen escrito final que aportara el 50% de la calificación y de una evaluación continua que aportara el otro 50%. Esta última se basara en el desarrollo y entrega de practicas en laboratorio, ejercicios y preparación de trabajos y la exposición de los mismos.

Recursos de aprendizaje y apoyo tutorial

Manuel J. Lucena: Criptografia y Seguridad de Computadores (Edición Electrónica) J.A. Buchman: "Introduction to Cryptography", Springer,2001 D. Hankerson, A. Menezes y S. Vanstone, “Guide to Elliptic Curve Cryptography”, Springer 2004. J. Katz y Y. Lindell, “Introduction to Modern Cryptography”, Chapman and Hall/CRC, 2008. N. Koblitz, “A Course in Number Theory and Cryptography”, Second Edition}, Graduate Texts in Mathematics 114, Springer, 1994.

.

Bibliografía complementaria

J.L. Gomez Pardo: "Introduction to Cryptography with Maple", Springer, 2013 I.Blake, G. Seroussi and N. Smart, “Elliptic Curves in Cryptography”, London Mathematical Society Lecture Note Series 265, Cambridge U. Press, 2000.
I. Blake, G. Seroussi and N. Smart, “Advances in Elliptic Curves in Cryptography”, London Mathematical Society Lecture Note Series, 317, Cambridge University Press, 2005. , LL. Huguet, R. Rifa: "Comunicacion Digital;"; Ed. Masson

Calendario y horario

Lunes a Jueves : 12-13 Clases teóricas y/o prácticas.
Viernes: 12-13 Laboratorio
Horario de tutorias: Lunes, Martes y Miercoles: 9-11h

Tabla de Dedicación del Estudiante a la Asignatura/Plan de Trabajo

ACTIVIDADES PRESENCIALES
HORAS
ACTIVIDADES NO PRESENCIALES
HORAS
Clases teórico-prácticas (T/M)
30
Estudio y trabajo autónomo individual
50
Clases prácticas de aula (A)
--
Estudio y trabajo autónomo grupal
31
Laboratorios (L)
15

Prácticas externas, clínicas o de campo
--

Seminarios (S)
8

Tutorías grupales (TG)
8

Evaluación
8

Total presencial
69
Total no presencial
81

Responsable de la docencia (recomendable que se incluya información de contacto y breve CV en el que aparezcan sus líneas de investigación y alguna publicación relevante)

Juan Tena Ayuso, Departamento de Algebra, Geometría y Topología.
E-mail: tena@agt.uva.es Tfno: 983423045

Idioma en que se imparte

Castellano