Proyecto docente de la asignatura

Asignatura	Criptografía		
Materia	Codificación y seguridad		
Curso	2019-20		
Plan	394	**Código**	40035
Periodo de impartición	1º Cuatrimestre	**Tipo**	Optativa
Nivel/Ciclo	Grado	**Curso**	Cuarto
Créditos ECTS	6		
Profesor	Félix Delgado de la Mata		
Datos de contacto (E-mail, teléfono…)	fdelgado@agt.uva.es / 983423050 . Despacho A337		
Horario	Clases: L,M,X de 14 a 15. V de 13 a 14. Tutorías: L, X: de 17 a 19. M, J: de 13 a 14. Despacho A337 Otras posibilidades bajo petición.		
Departamento	Álgebra, Análisis Matemático, Geometría y Topología		
Pruebas	Una prueba corta intermedia. Trabajos. Prácticas. Examen final.		
Examen (C. ordinaria)	10/01/2020 M		
Examen (C. extraordinaria)	31/01/2020 M		

1. Relación con otras materias y prerrequisitos

Es recomendable haber cursado las asignaturas: “Ecuaciones algebraicas”, “Estructuras algebraicas” e “Informática”.

2. Competencias

2.1. 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.

2.2. Específicas

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 computacional adecuado.
E11. Identificar las diferentes fases del proceso de modelización matemática, diferenciando la formulación, análisis, resolución e interpretación de resultados.

3. Objetivos

- Conocer el estado actual de las técnicas criptográficas y su evolución histórica.
- Manejar con soltura los principales algoritmos de cifrado tanto de clave privada (cifrado en bloque y cifrado en flujo) como de clave pública (con especial atención al sistema RSA y los basados en el logaritmo discreto).
- Comprender y utilizar las bases matemáticas, especialmente las que proceden de la teoría de números, para modelizar los criptosistemas y protocolos criptográficos adecuados para situaciones y aplicaciones concretas.
- Implementar y programar los principales criptosistemas discriminando en función de su uso concreto.
- Desarrollar nuevos métodos y adaptar los ya conocidos a nuevas situaciones.
- Conocer y manejar los principales protocolos criptográficos, sus objetivos y sus técnicas. Implementar y programar algunos de estos protocolos.
- Analizar la seguridad y los posibles ataques a los protocolos estudiados.

4. Contenidos

- Evolución histórica de la criptología. Criptología clásica. La máquina Enigma.
- Cifrado simétrico en bloques. Métodos matriciales. DES. AES.
- Cifrado simétrico en flujo. LFSR. Combinadores lineales.
- Criptografía de clave pública. Condiciones de Diffie-Hellman. Complejidad.
- Métodos de logaritmo discreto. El Gamal. Massey-Omura.
- Métodos de factorización: .Sistema RSA y de Rabin.
- Análisis del RSA: Complejidad, factorización, primalidad.
- Autentificación y firma digital en RSA y El Gamal. Funciones Hash.
- Protocolos criptográficos.

5. Actividades docentes

Clases teóricas.
Resolución de problemas en el aula.
Tutorías y seminarios, incluyendo presentaciones de trabajos y ejercicios propuestos.
Muestra de sistemas en el Laboratorio y realización de prácticas en MAPLE.

6. Tabla de dedicación del estudiante a la asignatura

ACTIVIDADES PRESENCIALES	HORAS	ACTIVIDADES NO PRESENCIALES	HORAS
Clases Teóricas	25	Estudio Autónomo Individual o en grupo	50
Resolución de problemas en grupos reducidos	15	Preparación y redacción de ejercicios y otros trabajos	15
Tutorías y seminarios, incluyendo presentaciones de trabajos y ejercicios propuestos.	10	Documentación: consultas bibliográficas, Internet	5
Clases con ordenador en el Laboratorio de Informática	15	Elaboración de prácticas de ordenador	20
Sesiones de evaluación	5		
Total presencial	**60**	**Total no presencial**	**90**

7. Evaluación

La calificación en **la convocatoria ordinaria** se obtendrá de la forma siguiente:

- Evaluación mediante Examen Final: El 60% de la calificación corresponderá a un examen final escrito.
- Evaluación Continua:
  - 20 % se obtendrá de un control realizado a mitad de curso y de la entrega de trabajos.
  - 20% se obtendrá del desarrollo y entrega de las prácticas de programación que se especifiquen.

En el caso de la **convocatoria extraordinaria** se tomará como calificación final el máximo entre la calificación del examen final escrito y el mismo sistema descrito para la calificación de la convocatoria ordinaria. Nótese que en este último caso la calificación de la evaluación continua no puede modificarse en la convocatoria extraordinaria, y que esa calificación representa el 40% de la calificación.

8. Bibliografía

LECTURA:

Singh, Simon: Los Códigos Secr3tos. Ed. Debate. 2000. ISBN: 84-8306-278-X

MUY RECOMENDADOS:

Buchmann, Johannes A.: Introduction to cryptography. Springer Verlag. Undergraduate Texts in Mathematics 2000. ISBN: 0-387-95034-6.
Fuster, A., de la Guía, D., Hernandez, L., Montoya, F. y Muñoz, J. : Técnicas criptografícas de protección de datos. 2ª ed. Ra-Ma. Textos Universitarios, 2000. ISBN: 84-7897-421-0.
Lucena López, Manuel José. Criptografía y Seguridad en Computadores. 4ª Ed. Accesible en http://wwwdi.ujaen.es/~mlucena
Koblitz, N.: A course in number theory and cryptography 2nd ed.. Springer Verlag. Graduate Texts in Math. 114. 1994.

OTROS BUENOS LIBROS:

Durán, R., Hernández, L.,, Muñoz, J.: El criptosistema RSA. Editorial RAMA. ISBN. 8478976515
Munuera,C. - Tena, J. Codificación de la información. Pub. de la Universidad de Valladolid. 1997. ISBN: 84-7762-764-9.
Pastor, J. y Sarasa, M.A. Criptografía digital. Prensas de la Universidad de Zaragoza. 1997.
Caballero, Pino. Introducción a la Criptografía. Ra-Ma. Textos Universitarios, 1996. ISBN: 84-7897-210-2
Stallings, W.: Cryptography and network security. Principles ad practice. Prentice Univ. Press. 1999.

Kahn, David: The Code-breakers. Scribner. 1967, 1996. ISBN: 0-684-83130-9