Criptografía

Curso Académico: (2020 / 2021) **Fecha de revisión: 10-07-2020**

Departamento asignado a la asignatura: Departamento de Informática

Coordinador/a: GONZALEZ-TABLAS FERRERES, ANA ISABEL

Tipo: Obligatoria Créditos ECTS : 6.0

Curso : 2 Cuatrimestre : 1

OBJETIVOS

CB1.Que los estudiantes hayan demostrado poseer y comprender conocimientos en un área de estudio que parte de la base de la educación secundaria general, y se suele encontrar a un nivel que, si bien se apoya en libros de texto avanzados, incluye también algunos aspectos que implican conocimientos procedentes de la vanguardia de su campo de estudio
CB2.Que los estudiantes sepan aplicar sus conocimientos a su trabajo o vocación de una forma profesional y posean las competencias que suelen demostrarse por medio de la elaboración y defensa de argumentos y la resolución de problemas dentro de su área de estudio
CB3.Que los estudiantes tengan la capacidad de reunir e interpretar datos relevantes (normalmente dentro de su área de estudio) para emitir juicios que incluyan una reflexión sobre temas relevantes de índole social, científica o ética
CB4.Que los estudiantes puedan transmitir información, ideas, problemas y soluciones a un público tanto especializado como no especializado
CB5.Que los estudiantes hayan desarrollado aquellas habilidades de aprendizaje necesarias para emprender estudios posteriores con un alto grado de autonomía
CG1.Que los estudiantes sean capaces de demostrar conocimiento y comprensión de conceptos de matemáticas, estadística y computación y aplicarlos a la resolución de problemas en ciencia e ingeniería con capacidad de análisis y síntesis
CG3.Que los estudiantes puedan resolver computacionalmente con ayuda de las herramientas informáticas más avanzadas los modelos matemáticos que surjan de aplicaciones en la ciencia, la ingeniería, la economía y otras ciencias sociales
CG4.Que los estudiantes demuestren que pueden analizar e interpretar las soluciones obtenidas con ayuda de la informática de los problemas asociados a modelos matemáticos del mundo real, discriminando los comportamientos más relevantes para cada aplicación.
CG6.Que los estudiantes sepan buscar y utilizar los recursos bibliográficos, en soporte físico o digital, necesarios para plantear y resolver matemática y computacionalmente problemas aplicados que surjan en entornos nuevos, poco conocidos o con información insuficiente
CE10.Que los estudiantes hayan demostrado que conocen y comprender los procedimientos algorítmicos para diseñar y construir programas que solucionen problemas matemáticos prestando especial atención al rendimiento.
CE15.Que los estudiantes hayan demostrado que conocen las bases matemáticas de la criptografía y comprenden las ventajas y limitaciones de los distintos algoritmos criptográficos.
RA1.Haber adquirido conocimientos avanzados y demostrado una comprensión de los aspectos teóricos y prácticos y de la metodología de trabajo en el campo de la matemática aplicada y computación con una profundidad que llegue hasta la vanguardia del conocimiento.
RA3.Tener la capacidad de recopilar e interpretar datos e informaciones sobre las que fundamentar sus conclusiones incluyendo, cuando sea preciso y pertinente, la reflexión sobre asuntos de índole social, científica o ética en el ámbito de su campo de estudio.
RA4.Ser capaces de desenvolverse en situaciones complejas o que requieran el desarrollo de nuevas soluciones tanto en el ámbito académico como laboral o profesional dentro de su campo de estudio.
RA5.Saber comunicar a todo tipo de audiencias (especializadas o no) de manera clara y precisa, conocimientos, metodologías, ideas, problemas y soluciones en el ámbito de su campo de estudio.
RA6.Ser capaces de identificar sus propias necesidades formativas en su campo de estudio y entorno laboral o profesional y de organizar su propio aprendizaje con un alto grado de autonomía en todo tipo de contextos (estructurados o no).

DESCRIPCIÓN DE CONTENIDOS: PROGRAMA

1.- Introducción a la seguridad en las tecnologías de la información
2.- Fundamentos matemáticos de la criptografía
3.- Introducción a la criptografía

4.- Criptografía clásica y su criptoanálisis
5.- Cifradores simétricos
6.- Funciones resumen y MAC
7.- Cifrado asimétrico
8.- Generación y distribución de claves
9.- Esquemas de firma digital
10.- Infraestructuras de clave pública
11.- Autenticación de usuarios

ACTIVIDADES FORMATIVAS, METODOLOGÍA A UTILIZAR Y RÉGIMEN DE TUTORÍAS

AF1.CLASES TEÓRICO-PRÁCTICAS. Conocimientos que deben adquirir los alumnos.Estos recibirán las notas de clase y tendrán textos básicos de referencia para facilitar el seguimiento de las clases y el desarrollo del trabajo posterior.Se resolverán ejercicios, prácticas problemas por parte del alumno y se realizarán talleres y prueba de evaluación para adquirirlas capacidades necesarias.Para asignaturas de 6 ECTS se dedicarán 44 horas como norma general con un 100% de presencialidad.(excepto aquellas que no tengan examen que dedicarán 48 horas)
AF2.TUTORÍAS. Asistencia individualizada (tutorías individuales) o en grupo (tutorías colectivas) a los estudiantes por parte del profesor. Para asignaturas de 6 créditos se dedicarán 4 horas con un 100% de presencialidad.
AF3.TRABAJO INDIVIDUAL O EN GRUPO DEL ESTUDIANTE. Para asignaturas de 6 créditos se dedicarán 98 horas 0% presencialidad.
AF8.TALLERES Y LABORATORIOS. Para asignaturas de 3 créditos se dedicarán 4 horas con un 100% de presencialidad. Para las asignaturas de 6 créditos se dedicarán 8 horas con un 100% de presencialidad.
MD1.CLASE TEORÍA. Exposiciones en clase del profesor con soporte de medios informáticos y audiovisuales, en las que se desarrollan los conceptos principales de la materia y se proporcionan los materiales y la bibliografía para complementar el aprendizaje de los alumnos.
MD2.PRÁCTICAS. Resolución de casos prácticos, problemas, etc. planteados por el profesor de manera individual o en grupo.
MD3.TUTORÍAS. Asistencia individualizada (tutorías individuales) o en grupo (tutorías colectivas) a los estudiantes por parte del profesor. Para asignaturas de 6 créditos se dedicarán 4 horas con un 100% de presencialidad.
MD6.PRÁCTICAS DE LABORATORIO. Docencia aplicada/experimental a talleres y laboratorios bajo la supervisión de un tutor.

SISTEMA DE EVALUACIÓN

SE1.EXAMEN FINAL. En el que se valorarán de forma global los conocimientos, destrezas y capacidades adquiridas a lo largo del curso. El porcentaje de valoración varía para cada asignatura en un rango entre el 60% y el 0%.
SE2.EVALUACIÓN CONTINUA. En ella se valorarán los trabajos, presentaciones, actuación en debates, exposiciones en clase, ejercicios, prácticas y trabajo en los talleres a lo largo del curso. El porcentaje de valoración varía para cada asignatura en un rango entre el 40 y el 100 % de la nota final.
Se podrá requerir la obtención de un rendimiento mínimo en el examen final.

Peso porcentual del Examen Final:	20
Peso porcentual del resto de la evaluación:	80

BIBLIOGRAFÍA BÁSICA

- Jean-Philippe Aumasson Serious Cryptography: A Practical Introduction to Modern Encryption , Random House LCC US .
- W. STALLINGS CRYPTOGRAPHY AND NETWORK SECURITY. (5ª EDICIÓN), PRENTICE HALL.