Criptografía

Curso Académico: (2021 / 2022) **Fecha de revisión: 31-08-2021**

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

REQUISITOS (ASIGNATURAS O MATERIAS CUYO CONOCIMIENTO SE PRESUPONE)

Programación (1 curso, cuatrimeste 1)
Matemática Discreta (1 curso, cuatrimeste 2)
Técnicas de Programación (1 curso, cuatrimeste 2)

DESCRIPCIÓN DE CONTENIDOS: PROGRAMA

1.- Introducción a la criptografía.
2.- Fundamentos matemáticos de la criptografía.
3.- Criptografía clásica.
4.- Conceptos fundamentales de la criptografía.
5.- Cifrado simétrico.
6.- Distribución de claves y cifrado asimétrico.
7.- Funciones resumen, MAC y cifrado autenticado.
8.- Esquemas de firma digital.
9.- Infraestructuras de clave pública.
10.- Autenticación de usuarios.

ACTIVIDADES FORMATIVAS, METODOLOGÍA A UTILIZAR Y RÉGIMEN DE TUTORÍAS

ACTIVIDADES FORMATIVAS, METODOLOGÍA A USAR Y REGIMEN DE TUTORIAS

CLASES TEÓRICO-PRÁCTICAS [44 horas con un 100% de presencialidad, 1.67 ECTS]
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.

TUTORÍAS [4 horas con un 100% de presencialidad, 0.15 ECTS]
Asistencia individualizada (tutorías individuales) o en grupo (tutorías colectivas) a los estudiantes por parte del profesor.

TRABAJO INDIVIDUAL O EN GRUPO DEL ESTUDIANTE. [98 horas con 0% de presencialidad, 3.72 ECTS]

TALLERES Y LABORATORIOS. [8 horas con 100% de presencialidad, 0.3 ECTS]

EXAMEN FINAL. [4 horas con 100% de presencialidad, 0.15 ECTS]
Se valorarán de forma global los conocimientos, destrezas y capacidades adquiridas a lo largo del curso.

METODOLOGÍAS DOCENTES

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.

PRÁCTICAS. Resolución de casos prácticos, problemas, etc. planteados por el profesor de manera individual o en grupo.

TUTORÍAS. Asistencia individualizada (tutorías individuales) o en grupo (tutorías colectivas) a los estudiantes por parte del profesor.

PRÁCTICAS DE LABORATORIO. Docencia aplicada/experimental a talleres y laboratorios bajo la supervisión de un tutor.

SISTEMA DE EVALUACIÓN

SE1 - EXAMEN FINAL. [40 %]
En el que se valorarán de forma global los conocimientos, destrezas y capacidades adquiridas a lo largo del curso.

SE2 - EVALUACIÓN CONTINUA. [60 %]
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.

Se requiere la obtención de una nota mínima del 50% en el examen final para poder aprobar la asignatura.

Peso porcentual del Examen Final:	40
Peso porcentual del resto de la evaluación:	60

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.