

Plan 413 GRADO EN INGENIERÍA INFORMÁTICA DE SERVICIOS Y APLICACIONES

Asignatura 40843 PROTOCOLOS Y COMUNICACIONES SEGURAS

Tipo de asignatura (básica, obligatoria u optativa)

Optativa

Créditos ECTS

6

Competencias que contribuye a desarrollar

2.1

Generales

- G01 : Conocimientos generales básicos.
- G03 : Capacidad de análisis y síntesis.
- G05 : Comunicación oral y escrita en la lengua propia.
- G06 : Conocimiento de una segunda lengua (Inglés).
- G07 : Habilidades básicas en el manejo del ordenador.
- G09 : Resolución de problemas.
- G16 : Capacidad de aplicar los conocimientos en la práctica.
- G18 : Capacidad de aprender.

2.2

Específicas

- E01 : Capacidad para la resolución de los problemas matemáticos que puedan plantearse en la ingeniería. Aptitud para aplicar los conocimientos sobre: álgebra lineal; cálculo diferencial e integral; métodos numéricos; algorítmica numérica; estadística y optimización.
- E02 : Comprensión y dominio de los conceptos básicos de matemática discreta, lógica, algorítmica y complejidad computacional, y su aplicación para el tratamiento automático de la información por medio de sistemas computacionales y para la resolución de problemas propios de la ingeniería.
- E03 : Conocimientos básicos sobre el uso y programación de los ordenadores, sistemas operativos, bases de datos y programas informáticos con aplicación en ingeniería.
- E11 : Conocimiento y aplicación de los procedimientos algorítmicos básicos de las tecnologías informáticas para diseñar soluciones a problemas, analizando la idoneidad y complejidad de los algoritmos propuestos.

Objetivos/Resultados de aprendizaje

- Plantear en lenguaje matemático y resolver problemas relacionados con la representación matemática de la información, su encriptación, y sus aplicaciones en la Seguridad Informática.
- Describir algorítmicamente la resolución de problemas relativos a la encriptación de datos, e implementarla eficientemente mediante software matemático.
- Comprender, discutir y expresar (oralmente y por escrito) conceptos y argumentos de tipo lógico matemático relacionados con la Seguridad Informática.
- Construcción de los modelos matemáticos necesarios para la resolución de problemas aplicados a la Seguridad Informática y su uso en la Empresa.
- Manejar software matemático en aplicaciones prácticas, con un énfasis especial en la interpretación de resultados y la escritura de informes.
- Comprender la interrelación de la Criptología con otras materias de la titulación.

Contenidos

1. Criptología y comunicaciones seguras
2. Criptografía simétrica
3. Algoritmos básicos
4. Criptografía de clave pública
5. Protocolos criptográficos

LABORATORIO: lenguaje PYTHON

Principios Metodológicos/Métodos Docentes

- Se alternará la exposición de contenidos teóricos (clase magistral) con resolución de problemas (prácticas en aula) y prácticas de ordenador (laboratorio).
- Se dará la posibilidad de superar al asignatura mediante evaluación continua, así como en las dos convocatorias finales.

Criterios y sistemas de evaluación

La asignatura se podrá superar mediante evaluación continua de acuerdo a los siguientes criterios:

INSTRUMENTO/PROCEDIMIENTO

PESO EN LA NOTA FINAL

OBSERVACIONES

Realización de un Proyecto de software en grupo sobre los contenidos del curso.

75%

Se entregará una Memoria, y se expondrá en clase el Proyecto con una demo, durante la última semana del curso.

Realización de una práctica de ordenador, de carácter individual.

15%

Al finalizar el bloque temático 4.

Realización de examen escrito de carácter teórico-práctico.

10%

Al finalizar el bloque temático 5.

Realización individual o en grupo de un trabajo de carácter teórico, y su exposición en clase durante la última semana del curso.

OPCIONAL

Para mejorar la nota obtenida en los apartados anteriores hasta en 1 punto sobre 10.

CRITERIOS DE CALIFICACIÓN

- Convocatoria ordinaria:
 - Examen escrito de carácter teórico práctico sobre el temario completo de la asignatura (50%).
 - Examen práctico de ordenador (50%).
 - La nota final será la media ponderada (50-50) de las dos pruebas anteriores.
- Convocatoria extraordinaria:
 - Igual que en la convocatoria ordinaria.

Consideraciones finales:

- La asignatura se podrá superar, cumpliendo con las notas mínimas, mediante la evaluación continua anteriormente descrita, haciendo la media ponderada de las tres notas, si dicha media supera el 5.
- Aun habiendo aprobado en la evaluación continua, cualquier alumno puede presentarse voluntariamente con toda la materia al examen ordinario para subir nota, y esta sería entonces la máxima de las dos notas obtenidas.
- En caso de no superar la asignatura mediante evaluación continua, la evaluación de la asignatura se realizará en las convocatorias finales (ordinaria y extraordinaria).
 - No se guardará ninguna nota de la evaluación continua (con la excepción del trabajo OPCIONAL) ni del examen ordinario para posteriores convocatorias, es decir, a los exámenes ordinario y extraordinario se va con toda la asignatura.
 - Ni en la convocatoria ordinaria ni extraordinaria se exige una nota mínima para hacer la media ponderada.

Recursos de aprendizaje y apoyo tutorial

Aula con pizarra y ordenador con proyector, laboratorio de informática con software matemático, biblioteca, sala de estudio, y despacho o seminario para tutorías.

Calendario y horario

Disponible en www.inf5g.uva.es

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

ACTIVIDADES PRESENCIALES

HORAS

ACTIVIDADES NO PRESENCIALES

HORAS

Clases teórico-prácticas (T/M)

26

Estudio y trabajo autónomo individual

50

Clases prácticas de aula (A)

Estudio y trabajo autónomo grupal

40

Laboratorios (L)

30

Prácticas externas, clínicas o de campo

Seminarios (S)

Tutorías grupales (TG)

Evaluación

4

Total presencial

60

Total no presencial

90

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)

José Ignacio Farrán Martín

Área: Matemática Aplicada

Escuela de Ingeniería Informática

Plaza de la Universidad 1 - 40005 Segovia

Teléfono : (+34) 921 11 24 20

Fax : (+34) 921 11 24 01

e-mail : jifarran@eii.uva.es

web : <http://wmatem.eis.uva.es/~ignfar>

Idioma en que se imparte

Español