ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA

GUIA DOCENTE

CURSO 2018/2019

Grado en Ingeniería Informática

DATOS DE LA ASIGNATURA			
Nombre:			
Técnicas Numéricas para la Computación			
Denominación en inglés:			
Numerical Techniques for the Computation			
Código:		**Carácter:**	
606010316		Optativo	
Horas:			
	Totales	**Presenciales**	**No presenciales**
Trabajo estimado:	150	60	90

Créditos:

	Grupos reducidos			
Grupos grandes	**Aula estándar**	**Laboratorio**	**Prácticas de campo**	**Aula de informática**
4.44	1.56	0	0	0

Departamentos:	**Áreas de Conocimiento:**
Ciencias Integradas	Matemática Aplicada
Curso:	**Cuatrimestre:**
4º - Cuarto	Primer cuatrimestre

DATOS DE LOS PROFESORES			
Nombre:	**E-Mail:**	**Teléfono:**	**Despacho:**
*Algaba Durán, Antonio	algaba@dmat.uhu.es	959219913	P4-N4-11 (F. Experimentales)

*Profesor coordinador de la asignatura

Consultar los horarios de la asignatura

DATOS ESPECÍFICOS DE LA ASIGNATURA

1. Descripción de contenidos

1.1. Breve descripción (en castellano):

Análisis del error. Complejidad computacional.
Aritmética de números grandes y su aplicación a la criptografía.
Interpolación polinomial a trozos. Aplicaciones.
Modelos discretos y contínuos. Aplicaciones.

1.2. Breve descripción (en inglés):

Error Analysis. Computational Complexity.
Arithmetic of large numbers and its application to cryptography.
Piecewise polynomial interpolation. Applications.
Discrete and continuous models. Applications.

2. Situación de la asignatura

2.1. Contexto dentro de la titulación:

La asignatura, en un primer bloque, pretende desarrollar los conocimiento mínimos para resolver numéricamente algunos problemas que se plantean en ciencia e ingeniería. Entre ellos, las implicaciones que conlleva la implementación en máquinas con aritmética inexacta de algoritmos matemáticos, las adaptaciones de los algoritmos estudiados a problemas específicos y el análsis de las características de convergencia y eficiencia computacional de los métodos numéricos estudiados así como de sus implementaciones.
Una vez cursada, proporcionará las técnicas elementales para resolver problemas que se plantean con frecuencia, aportando conocimientos y técnicas de trabajo que pueden ser útiles para otras asignaturas de la titulación.
Por otro lado, la necesidad de ocultar información a destinatarios no autorizados ha contribuido decisivamente al desarrollo de la Criptografía, cuyo objetivo principal es el desarrollo de algoritmos que permitan garantizar la confidencialidad e integridad del mensaje, así como la autentificación de remitente.
En los últimos años los ordenadores han pasado de ser instrumentos relativamente aislados, a formar parte de una intrincada red global de comunicaciones. Las transacciones bancarias y el pago de impuestos a través de Internet, el uso del correo electrónico y el comercio electrónico son ejemplos de actividades cada vez más habituales que requieren el intercambio de una gran cantidad de información y de datos personales que no deberían caer en manos de terceras personas. Se
hace por tanto imprescindible, para un graduado en Informática, el poseer conocimientos sobre las técnicas criptográficas más comunes que permiten garantizar el intercambio seguro de información.

2.2. Recomendaciones:

3. Objetivos (Expresados como resultados del aprendizaje):

-Conocer las implicaciones que conlleva la implementación en máquina, con aritmética inexacta y recursos finitos, de algoritmos matemáticos.
- Dar una introducción a las técnicas modernas de aproximación; sabiendo cómo, por qué y cuándo se espera que funcionen.
- Proporcionar al alumno un amplio catálogo de métodos que aproximan las soluciones de los problemas abordados.
- Que el alumno sea capaz de realizar el análisis, desarrollo e implementación práctica de métodos numéricos elementales.
-Capacidad para implementar adaptaciones de los algoritmos estudiados a problemas específicos.
-Capacidad para discernir las características de convergencia y eficiencia computacional de los métodos numéricos estudiados y sus implementaciones.
-Conocer la aritmética de números grandes.
-Conocer los fundamentos teóricos de la criptografía moderna.
- Comprender los componentes y el funcionamiento de una infraestructura de clave pública.
- Realización de una memoria científico-técnica.

4. Competencias a adquirir por los estudiantes

4.1. Competencias específicas:

4.2. Competencias básicas, generales o transversales:

- **CG0:** Capacidad de análisis y síntesis: Encontrar, analizar, criticar (razonamiento crítico), relacionar, estructurar y sintetizar información proveniente de diversas fuentes, así como integrar ideas y conocimientos.
- **G02:** Capacidad de comunicación oral y escrita en el ámbito académico y profesional con especial énfasis, en la redacción de documentación técnica
- **G03:** Capacidad para la resolución de problemas
- **G04:** Capacidad para tomar decisiones basadas en criterios objetivos (datos experimentales, científicos o de simulación disponibles) así como capacidad de argumentar y justificar lógicamente dichas decisiones, sabiendo aceptar otros puntos de vista
- **G05:** Capacidad de trabajo en equipo.
- **G06:** Capacidad para el aprendizaje autónomo así como iniciativa y espíritu emprendedor
- **G09:** Capacidad para innovar y generar nuevas ideas.
- **T02:** Conocimiento y perfeccionamiento en el ámbito de las TIC’s

5. Actividades Formativas y Metodologías Docentes

5.1. Actividades formativas:

- Sesiones de Teoría sobre los contenidos del Programa.
- Sesiones de Resolución de Problemas.
- Sesiones Prácticas en Laboratorios Especializados o en Aulas de Informática.
- Actividades Académicamente Dirigidas por el Profesorado: seminarios, conferencias, desarrollo de trabajos, debates, tutorías colectivas, actividades de evaluación y autoevaluación.

5.2. Metologías docentes:

- Clase Magistral Participativa.
- Desarrollo de Prácticas en Laboratorios Especializados o Aulas de Informática en grupos reducidos.
- Resolución de Problemas y Ejercicios Prácticos.
- Planteamiento, Realización, Tutorización y Presentación de Trabajos.
- Evaluaciones y Exámenes.

5.3. Desarrollo y justificación:

Las sesiones académicas de teoría, de 1.5 horas de duración, se irán desarrollando en el aula, alternando explicaciones teóricas y resolución de problemas cuando se considere oportuno. En ellas se expondrán los conceptos y procedimientos propios de la asignatura, ilustrados con ejemplos y aplicaciones. Asimismo, los alumnos podrán realizar exposiciones de los trabajos realizados durante el curso. Se usarán los recursos disponibles como pizarra, proyector de transparencias o cañón de vídeo. Paralelamente se impartirán sesiones prácticas en el aula de informática donde se implementarán los algoritmos estudiados en las sesiones de teoría, fundamentalmente en matlab en lo que se refiere a la computación numérica. En dichas prácticas se propondrá a los alumnos la resolución de ejercicios y trabajos, relacionados con el contenido de las mismas, para su posterior evaluación. Estos trabajos se podrán realizar en el lenguaje que el alumno prefiera.

6. Temario desarrollado:

0. Introducción a Matlab.
1. Análisis del error. Complejidad computacional.
Representación de números.
Error de redondeo y aritmética punto flotante (en coma flotante).
Propagación del error. Condición de un problema y estabilidad numérica de un algoritmo.
Complejidad computacional.
2. Aritmética de números grandes. Aplicación a la criptografía.
Sistemas criptográficos clásicos.
Aritmética modular.
Aritmética de números grandes.
Criptosistemas asimétricos: sistemas de clave pública. RSA.
3. Interpolación polinomial a trozos. Aplicaciones.
Interpolación polinomial
Interpolación polinomial a trozos. Aplicación al diseño.
Interpolación trigonométrica. FFT. Aplicación a las comunicaciones.
4. Modelos discretos y contínuos. Aplicaciones.
Diferenciación e integración numérica.
Sistemas dinámicos discretos: Puntos fijos y estabilidad. Aplicación a la dinámica de poblaciones.
Sistemas dinámicos contínuos: Equilibrios y estabilidad. Aplicación a la ingenieria de control.

7. Bibliografía

7.1. Bibliografía básica:

- NUMERICAL COMPUTING WITH MATLAB. C. Moler. http://www.mathworks.com/moler
- MÉTODOS NUMÉRICOS CON MATLAB. Mathews-Fink (2000). Prentice- Hall. ISBN 84-8322-181-0.
Tercera edición.
- ANÁLISIS NUMÉRICO. Burden-Faires (2002). Thomson. ISBN 970-686-134-3. Séptima edición.
- MÉTODOS NUMÉRICOS PARA INGENIEROS. Chapra S.C., Canale, R.P. (2007). McGraw-Hill.
ISBN 970-10-6114-4. Quinta edición.
- CRIPTOGRAFÍA Y SEGURIDAD EN COMPUTADORES. Lucena López. M. J.
http://sertel.upc.edu/tdatos/Libros/Lucena.pdf
- CRIPTOGRAFÍA DIGITAL. FUNDAMENTOS Y APLICACIONES. Pastor, J., Sarasa, M. A.
Prensas Universitarias de Zaragoza. 1998.
- LIBRO ELÉCTRÓNICO DE SEGURIDAD INFORMÁTICA Y CRIPTOGRAFÍA 4.1, Ramió Aguirre, J.
Sexta edición. http://www.criptored.upm.es/descarga/SegInfoCripPDFc_v41.zip
-INGENIERÍA DE CONTROL MODERNA. Katsuhiko Ogata. Prentice Hall. 1993

7.2. Bibliografía complementaria:

- ANÁLISIS NUMÉRICO: LAS MATEMÁTICAS DEL CÁLCULO CIENTÍFICO. Kincaid-Cheney (1994). Addison-Wesley
Iberoamérica. ISBN 0-201-60130-3.
- ANÁLISIS NUMÉRICO Y VISUALIZACIÓN GRÁFICA CON MATLAB. Nakamura S (1997).
Prentice Hall. ISBN 968-880-860-1.
- MATLAB Y SUS APLICACIONES EN LAS CIENCIAS Y LA INGENIERÍA. Pérez C (2002).
Prentice-Hall. ISBN 84-205-3537-0.
- APPLIED CRYPTOGRAPHY: PROTOCOLS, ALGORITHMS AND SOURCE CODE IN C, Schneier, B.
2th edition. 1995.
- CRYPTOGRAPHY AND NETWORK SECURITY: PRINCIPLES AND PRACTICE, Stallings, W.
3rd edition. Prentice Hall. 2002.

8. Sistemas y criterios de evaluación.

8.1. Sistemas de evaluación:

- Defensa de Prácticas
- Defensa de Trabajos e Informes Escritos

8.2. Criterios de evaluación y calificación:

La evaluación de la asignatura se realizará en base a pruebas de laboratorio (implementación de los algorítmos desarrolados en clase, con una ponderación de 30%) y, la elaboración y exposición oral de un trabajo adicional, propuesto por el profesor a cada alumno o a un grupo de alumnos, que versará sobre aplicaciones de los contenidos teóricos estudiados con una ponderación del 70%. En los criterios de evaluación se tendrá en cuenta la adecuación de las respuestas, el nivel de razonamiento, de análisis y de síntesis, la exactitud, el nivel de expresión y la presentación.
Los alumnos tendrán la posibilidad de recuperar la asignatura mediante un examen práctico en el aula de informática.

9. Organización docente semanal orientativa:

Semanas	Grupos Grandes	Grupos Reducidos Aula Estándar	Grupos Reducidos Aula de Informática	Grupos Reducidos Laboratorio	Grupos Reducidos prácticas de campo	Pruebas y/o actividades evaluables	Contenido desarrollado
#1	3	0	0	0	0	Matlab	
#2	3	0	0	0	0	Bloque 1	
#3	3	0	0	0	0	Bloque 1	
#4	3	0	3	0	0	Bloque 1	
#5	3	0	0	0	0	Bloque 2	
#6	3	0	0	0	0	Bloque 2	
#7	3	0	0	0	0	Bloque 2	
#8	3	0	3	0	0	Bloque 2	
#9	3	0	0	0	0	Bloque 3	
#10	3	0	0	0	0	Bloque 3	
#11	3	0	3	0	0	Bloque 3	
#12	3	0	0	0	0	Bloque 4	
#13	3	0	3	0	0	Bloque 4	
#14	3	0	0	0	0	Bloque 4	
#15	3	0	3	0	0	Bloque 4	
	45	0	15	0	0		