Guía docente de la asignatura

Curso académico: 2021-2022

Asignatura	Matemáticas de la comunicación		
Materia	Matemáticas		
Módulo	Interdisciplinar		
Titulación	Máster en matemática		
Plan	645	**Código**	55048
Periodo de impartición	Primer cuatrimestre	**Tipo/Carácter**	Optativa
Nivel/Ciclo	Máster	**Curso**	Primero
Créditos ECTS	3		
Lengua en que se imparte	Español		
Profesor responsable	Carlos Munuera		
Datos de contacto	cmunuera@uva.es Despacho 232, ETS de Arquitectura		
Departamento	Matemática Aplicada		

1. SITUACIÓN Y SENTIDO DE LA ASIGNATURA

1.1. Contextualización

La creciente importancia de la información -su uso y su gestión- en nuestra sociedad ha impulsado una nueva rama de las ciencias de la computación y la matemática aplicada: el estudio de la teoría de la información y de los sistemas de codificación. Esta rama se ha desarrollado vertiginosamente durante las últimas décadas. Los códigos y los algoritmos de codificación y descodificación son los responsables de los protocolos que permiten una comunicación fiable en los procesos digitales. Asimismo, la teoría de códigos juega también un papel central en disciplinas relacionadas, como la compresión de datos, la codificación en redes, la seguridad y privacidad, etc.
De forma simultánea al desarrollo de la teoría, hemos asistido al de sus apoyos computacionales, tanto a nivel de capacidad de cálculo, como en el desarrollo de sus bases teóricas. Ambas disciplinas -codificación y computación- han ido de la mano, brindándose entre sí herramientas, líneas de investigación teórica, y problemas y métodos de resolución práctica.
Las matemáticas, y particularmente el álgebra concebida como la modelización algebraica en sentido amplio, son técnicas primordiales en la teoría de códigos correctores de errores y en todas las disciplinas relativas a la seguridad de la información. En esta asignatura nos centraremos en las bases de la teoría de la codificación algebraica y algunas de sus aplicaciones en seguridad informática.

1.2. Relación con otras materias del máster

Esta asignatura está estrechamente relacionada con las siguientes**:** Teoría de números, Álgebra conmutativa, Códigos álgebro-geométricos, Algebra combinatoria, Seminario de álgebra, Geometría algebraica.

1.2. Prerrequisitos

Los requeridos por la titulación.

2. COMPETENCIAS

2.1. Generales

CB6.- Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y/o aplicación de ideas, a menudo en un contexto de investigación.
CB7.- Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio.
CB8.- Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formular juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios.
CB9.- Que los estudiantes sepan comunicar sus conclusiones y los conocimientos y razones últimas que las sustentan a públicos especializados y no especializados de un modo claro y sin ambigüedades.
CB10.- Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo.
G1.- Conocimiento del método científico. Conocer el método científico, en particular en el ámbito de las Matemáticas, formulando modelos e hipótesis de trabajo relevantes y planificando el análisis en relación con dichas hipótesis y la discusión de las conclusiones, de modo que se pueda avanzar en el conocimiento de las Matemáticas.
G2.- Competencia para aplicar los conocimientos adquiridos. Aplicar los conocimientos técnicos adquiridos, de forma coherente y profesional, sobre todo en contextos novedosos o en constante renovación, que impliquen la realización de una actividad matemática.
G3.- Capacidad crítica, de análisis y síntesis, y capacidad de interpretación. Emitir juicios críticos sobre propuestas, hipótesis y validez científica de las conclusiones, así como sintetizar la presentación de propuestas y resultados, en el ámbito de las Matemáticas y de sus aplicaciones.
G4.- Competencias metodológicas. Elegir la metodología más adecuada para el desarrollo de la investigación de un problema, adaptándola al contexto en el que se origina el problema.

G5.- Capacidad para reconocer la originalidad y creatividad. Reconocer la originalidad en la concepción, formulación y resolución de problemas matemáticos.
G6.- Capacidades de comunicación. Presentar, de forma oral y escrita, y tanto ante públicos especializados como no especializados, resultados avanzados de investigación en Matemáticas, teniendo en cuenta los antecedentes en la investigación, las hipótesis de trabajo, los desarrollos y las conclusiones.
G7.- Capacidad de trabajo en equipo. Desarrollar una actividad matemática dentro de un equipo de investigación, bajo supervisión o de forma autónoma, pero al servicio de un proyecto investigador común.
G8.- Capacidad para el uso de las nuevas tecnologías. Adquirir destrezas generales en el uso de las nuevas tecnologías en el ámbito de la actividad matemática, facilitando su utilización en ámbitos diversos, así como el conocimiento de las herramientas informáticas disponibles más importantes.
G9.- Capacidad para poder mantener una formación permanente. Adquirir las destrezas necesarias para poder ampliar conocimientos y mantener una formación continua a lo largo de su vida profesional.
G10.- Capacidad de aprendizaje autónomo. Adquirir las destrezas necesarias para el aprendizaje autónomo en el ámbito de las Matemáticas, conociendo las fuentes de conocimiento para dicho aprendizaje y su utilización, y motivando el aprendizaje a lo largo de la vida en el ejercicio de la actividad matemática.
G11.- Competencias para la internacionalización de la actividad profesional en Matemáticas. Adquirir competencias que favorezcan el desarrollo de una actividad profesional en Matemáticas en contextos internacionales, especialmente mediante el uso de un idioma extranjero, usualmente el inglés, para la comunicación en el ámbito científico internacional de los resultados de la actividad investigadora.

2.2. Específicas .

E1.- Adquisición de destrezas técnicas generales en el ámbito de una o varias áreas de las Matemáticas. Utilizar de forma profesional el lenguaje y las técnicas avanzadas propias de estas áreas, para favorecer la interpretación de las fuentes especializadas, así como la formulación adecuada de nuevos problemas.
E2.- Capacidad de comprensión de las bases teóricas y técnicas en las que se apoyan los conceptos y métodos de las materias propias de las Matemáticas. Adquirir el corpus teórico que sustenta los conceptos y métodos de las materias propias de alguna de las áreas de las Matemáticas, y la capacidad para un manejo experto y fluido de dichos conocimientos.
E3.- Capacidad para iniciarse en la investigación y/o aplicación de las Matemáticas. Adquirir competencias suficientes para iniciar un proyecto de investigación en alguna de las áreas de conocimiento de Matemáticas, de forma supervisada, y en particular, en relación con las líneas de investigación que se ofertan en el Programa de Doctorado en Matemáticas de la Universidad de Valladolid. Alternativamente conseguir competencias que le permitan la colaboración en proyectos interdisciplinares en los que el uso de las técnicas y el pensamiento matemáticos resultan fundamentales.
E4.- Capacidad y destrezas para la gestión de las fuentes bibliográficas de la investigación. Buscar y gestionar documentación y bibliografía especializada, en el ámbito específico de la especialización que le sea propia; usar ésta de modo racional y crítico para determinar el estado del arte en un determinado problema, y dominar los recursos bibliográficos pertinentes.
E5.- Capacidad de aplicar y adaptar los modelos teóricos y las técnicas específicas tanto a problemas abiertos en su línea de especialización, como a problemas provenientes de otros ámbitos ya sean científicos o técnicos. Adaptar los modelos teóricos propios de cada una de las disciplinas de las Matemáticas para el estudio de problemas abiertos relacionados o para el análisis de otros problemas provenientes de los ámbitos científicos, sociales o tecnológicos.
E6.- Capacidad de analizar problemas, detectando el posible uso de modelos matemáticos para contribuir a su comprensión y resolución. Analizar nuevas situaciones para identificar la aplicación de modelos matemáticos, existentes o de nuevo diseño, que contribuyan a la comprensión y solución de los problemas planteados.
E7.- Capacidad de exponer y defender proyectos y trabajos de investigación en el ámbito de sus líneas de especialización, así como de mantener debates científicos sobre los mismos, ya sean estos propios o adquiridos. Exponer y defender proyectos y trabajos de investigación en el ámbito propio de la especialización adquirida, tanto para defender las tesis propias como para debatir con juicio crítico con terceros.
E8.- Discernir entre las diferentes orientaciones de las técnicas específicas que concurren en la comprensión y resolución de un problema, comprendiendo la oportunidad y el uso de cada una de ellas individualmente, así como la cooperación entre ellas de cara a la resolución global del problema.
E9.- Capacidad de comprender nuevos avances y perspectivas científicas en el ámbito de la investigación en las líneas de su especialización. Comprender la formulación de nuevos avances y las perspectivas que éstos abren.
E10.- Capacidad de detectar líneas de trabajo emergentes en el ámbito de las Matemáticas o de sus aplicaciones, identificando la relación, origen e influencia con el estado de conocimiento propio de cada una de las especializaciones de las Matemáticas. Reconocer líneas de trabajo emergentes en el ámbito de las Matemáticas o de sus aplicaciones, identificando las interrelaciones existentes con cada una de las especialidades.
E11.- Capacidad para modelar matemáticamente fenómenos de la realidad y describir, en el ámbito de esos fenómenos, la relevancia de los resultados matemáticos. Proponer y ajustar modelos matemáticos en el estudio de problemas concretos, estudiando sus propiedades y la teoría matemática que sustenta su uso.

E12.- Capacidad para el ajuste de modelos matemáticos. Valorar la idoneidad de un modelo matemático en un problema concreto, estudiando sus propiedades y manejando las herramientas de ajuste y diagnóstico necesarias.
E13.- Capacidad para la utilización de las nuevas tecnologías en el ámbito de las Matemáticas y de sus aplicaciones. Utilizar métodos computacionales, según el ámbito de estudio de su especialidad, para explorar la frontera del conocimiento en las distintas disciplinas de las Matemáticas, así como en sus aplicaciones.
E14.- Conocimiento con carácter general del software matemático de carácter profesional en las distintas disciplinas de las Matemáticas, y capacidad para orientar su aplicación según las situaciones y comprender sus limitaciones. Conocer el software matemático profesional propio de cada especialidad para dirigir su aplicación en una variedad de situaciones, comprendiendo sus limitaciones, y adaptándolo cuando sea necesario.
E15.- Competencia para el diseño de técnicas computacionales y su análisis en los distintos ámbitos de las Matemáticas. Diseñar y analizar métodos computacionales en el ámbito de la Información y la Criptografía, y utilizarlos en las diversas aplicaciones en que son relevantes.

3. OBJETIVOS

O1.- Comprender como las matemáticas permiten la comunicación de información fiable y segura entre los usuarios de una red de comunicaciones.
O2.- Comprender el propósito de la codificación de la información y sus diferentes tipos.
O3.- Conocer los principales tipos de códigos compresores, correctores y criptográficos; ser capaz de implementar alguno de ellos en un sistema de álgebra computacional.
O4.- Que los estudiantes desarrollen las habilidades necesarias para emprender estudios posteriores con un alto grado de autonomía.

4. TABLA DE DEDICACIÓN DEL ESTUDIANTE A LA ASIGNATURA

ACTIVIDADES PRESENCIALES	Metodología docente	HORAS
Clases teóricas	Lección expositiva.	13
Clases prácticas en aula	Aprendizaje cooperativo. Estudio de ejemplos. Realización de prácticas orientadas en el aula.	13
Sesiones de evaluación		1
	Total presencial	**27**

ACTIVIDADES NO PRESENCIALES		HORAS
Estudio	Estudio autónomo	25
Realización de trabajos	Realización de trabajos y ejercicios planteados. Trabajos con ordenador.	18
Investigación bibliográfica	Búsqueda de materiales y documentación bibliográfica o por internet	5
	Total no presencial	**48**

5. BLOQUES TEMÁTICOS

Bloque 1. Teoría de la Información

Carga de trabajo en créditos ECTS: 0,6

a. Contextualización y justificación

Tratar cuantitativamente la información requiere poder manipularla y medirla. En este bloque abordamos los conceptos básicos de la información y su manejo, y las principales características de la transmisión de información.

b. Objetivos de aprendizaje

Entender qué es una información digital, su medida de la información y sus propiedades. Entender los principales factores que describen las características de la transmisión de la información. Entender los principios en que se basan los códigos compresores, correctores y secretos.

c. Contenidos

La Transmisión de Información. Codificación. Descodificación. Fuentes de Información. Medida de la Información. La Entropía. Compresión de la Información. Códigos Óptimos. Construcción de Códigos Óptimos. Métodos de Huffman y de Lempel-Ziv. Algunos códigos criptográficos. El ruido. Detección y corrección de errores. Teorema de Shannon.

d. Métodos docentes

Lección magistral, práctica de aula y práctica con ordenador. Trabajos propuestos a los alumnos.

e. Plan de trabajo

Semanas 1 a 4. Lecciones teóricas (3 horas), prácticas de aula (3 horas).

f. Evaluación

Se realizará la evaluación en base al siguiente criterio: Trabajo final: 50%; Evaluación continua: 50%.

g. Bibliografía

J. Adamek: *Foundations of Coding: Theory and Applications of Error-Correcting Codes with an Introduction to Cryptography and Information Theory*, Ed Wiley, 1991**.**

C. Munuera, J. Tena: *Codificación de la Información*, Pub. Universidad de Valladolid, 1997.

h. Recursos necesarios

Aula de clases, computadora.

Bloque 2. Códigos correctores y algunas de sus aplicaciones

Carga de trabajo en créditos ECTS: 1,4

a. Contextualización y justificación

En este bloque se estudian los canales con ruido, en el que los mensajes transmitidos pueden sufrir alteraciones. Se estudia el papel del ruido desde un punto de vista teórico, su efecto en la capacidad de un canal, y el teorema de Shannon. Tras esto se ofrecen métodos efectivos para combatir este problema, mediante los códigos correctores de errores, que trataremos con cierta profundidad. También se estudiarán sus aplicaciones en diversas áreas de las comunicaciones.

b. Objetivos de aprendizaje

Entender el papel del ruido y el concepto de capacidad de un canal. Conocer las principales propiedades de los códigos correctores de errores. Conocer los tipos más importantes de códigos correctores y sus aplicaciones en diversos aspectos del tratamiento de la información.

c. Contenidos

Cuerpos Finitos. Códigos lineales. Codificación lineal. Peso de Hamming. Dualidad. Descodificación de los códigos lineales. Códigos BCH y RS. Los códigos correctores en otros problemas de la información. Recuperación local de

información. Códigos de red. El sistema de McEliece en la criptografía post-cuántica. Reparto de secretos. Esteganografía

d. Métodos docentes

Lección magistral, práctica de aula y práctica con ordenador. Trabajos propuestos a los alumnos.

e. Plan de trabajo

Semanas 4 a 10. Lecciones teóricas (7 horas), prácticas de aula (7 horas).

f. Evaluación

Se realizará la evaluación en base al siguiente criterio: Trabajo final: 50%; Evaluación continua: 50%.

g. Bibliografía

J. Adamek, *Foundations of Coding: Theory and Applications of Error-Correcting Codes with an Introduction to Cryptography and Information Theory*, Ed Wiley, 1991**.**

C. Munuera, J. Tena, *Codificación de la Información*, Pub. Universidad de Valladolid, 1997.

h. Recursos necesarios

Aula de clases, computadora.

Bloque 3. Criptografía

Carga de trabajo en créditos ECTS: 0,6

a. Contextualización y justificación

Un aspecto fundamental de la transmisión de información es su seguridad frente a terceros. En este bloque nos ocuparemos de estudiar los códigos diseñados para garantizar la integridad y privacidad de la información.

b. Objetivos de aprendizaje

Entender el papel de los códigos criptográficos en la transmisión de la información. Conocer la diferencia entre clave pública y clave privada. Familiarizarse con algunos de los principales códigos en uso y sus aplicaciones. Incitar a los estudiantes a investigar en un tema de su elección en este área.

c. Contenidos

Criptografía simétrica o de clave privada. Cifrado en bloque. AES. Cifrado en flujo. Clave pública. El sistema criptográfico RSA. El sistema criptográfico El-Gamal. Firma digital.

d. Métodos docentes

Lección magistral, práctica de aula y práctica con ordenador. Trabajos propuestos a los alumnos.

e. Plan de trabajo

Semanas 10 a 13. Lecciones teóricas (3 horas), prácticas de aula (3 horas).

f. Evaluación

Se realizará la evaluación en base al siguiente criterio: Trabajo Final: 50%; Pruebas de Evaluación continua: 50%.

g. Bibliografía

C. Munuera, J. Tena, *Codificación de la Información*, Pub. Universidad de Valladolid, 1997.
Revistas científicas y Páginas de Internet.

h. Recursos necesarios

Aula de clases, computadora.

6. TEMPORALIZACIÓN POR BLOQUES TEMÁTICOS

BLOQUE TEMÁTICO	CARGA ECTS	PERIODO PREVISTO DE DESARROLLO
Teoría de la información	0,6	Semanas 1-4
Códigos correctores y sus aplicaciones	1,4	Semanas 4-10
Criptografía	0,6	Semanas 10-13

Esta temporalización es desiderativa, y puede variar en función del desarrollo del curso

7. SISTEMAS Y CARACTERÍSTICAS DE LA EVALUACIÓN

INSTRUMENTO/PROCEDIMIENTO	PESO EN LA NOTA FINAL	OBSERVACIONES
Evaluación continua	50%	
Realización y exposición de un trabajo final	50%	

CRITERIOS DE CALIFICACIÓN
En los trabajos propuestos, se valorarán principalmente los conocimientos y la madurez adquiridos; el manejo de los conceptos, y el rigor, limpieza y claridad en la exposición. En la evaluación continua se valorará también el trabajo desarrollado, y la actitud y el interés mostrado durante las clases.

.