ANX-PR/CL/001-01
GUÍA DE APRENDIZAJE

ASIGNATURA

305000151 - Introducción A La Codificación De La Información

PLAN DE ESTUDIOS

30GM - Grado En Matematicas

CURSO ACADÉMICO Y SEMESTRE

2024/25 - Primer semestre

Índice

Guía de Aprendizaje

1. Datos descriptivos

1.1. Datos de la asignatura

Nombre de la asignatura	305000151 - Introducción a la Codificación de la Información
No de créditos	6 ECTS
Carácter	Optativa
Curso	Cuarto curso
Semestre	Séptimo semestre
Período de impartición	Septiembre-Enero
Idioma de impartición	Castellano
Titulación	30GM - Grado en Matematicas
Centro responsable de la titulación	30 - Escuela Politecnica De Enseñanza Superior
Curso académico	2024-25

2. Profesorado

2.1. Profesorado implicado en la docencia

Nombre	Despacho	Correo electrónico	Horario de tutorías *
Vicente Jara Vera (Coordinador/a)	ETSIT-A-315	vicente.jara@upm.es	Sin horario.

* Las horas de tutoría son orientativas y pueden sufrir modificaciones. Se deberá confirmar los horarios de tutorías con el profesorado.

3. Conocimientos previos recomendados

3.1. Asignaturas previas que se recomienda haber cursado

- Fundamentos De MatemÁticas

- MatemÁtica Discreta

- AnÁlisis Real

- Probabilidad

- Ecuaciones Algebraicas

- Álgebra Lineal

- ModelizaciÓn Y SimulaciÓn I

- ProgramaciÓn

- Estructuras Algebraicas

- Ecuaciones En Derivadas Parciales

3.2. Otros conocimientos previos recomendados para cursar la asignatura

El plan de estudios Grado en Matematicas no tiene definidos otros conocimientos previos para esta asignatura.

4. Competencias y resultados de aprendizaje

4.1. Competencias

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

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

CE1 - Comprender y utilizar el lenguaje matemático. Adquirir la capacidad para enunciar propiedades en distintos campos de la Matemática, para construir argumentaciones, elaborar cálculos y para transmitir los conocimientos matemáticos adquiridos.

CE2 - Conocer y comprender demostraciones rigurosas de los principales teoremas de cada área de la Matemática y extraer de ellos corolarios mediante la particularización a casos concretos.

CE3 - Asimilar la definición de un nuevo objeto matemático, en términos de otros ya conocidos, y ser capaz de utilizar este objeto en diferentes contextos.

CE7 - Resolver problemas de Matemáticas, mediante habilidades de cálculo básico y tecnologías de computación, planificando su resolución en función de las herramientas de que se disponga y de las restricciones de tiempo y recursos.

CG1 - Identificar la naturaleza, métodos y fines de los distintos campos de la Matemática y asociarlos con cierta perspectiva histórica de su desarrollo.

CG3 - Utilizar las capacidades analíticas y de abstracción, la intuición y el pensamiento lógico y riguroso desarrolladas a través del estudio de la Matemática en contextos tanto matemáticos como no matemáticos.

CG4 - Utilizar los conocimientos teóricos y prácticos adquiridos en la definición y planteamiento de problemas y en la búsqueda de sus soluciones tanto en contextos académicos como profesionales.

4.2. Resultados del aprendizaje

RA259 - Comprender y operar con soltura diversos sistemas criptográficos fundamentales.

RA268 - Manejar con soltura las operaciones en aritmética entera y modular, cuerpos finitos y en sus anillos de polinomios.

RA267 - Comprender y operar con los sistemas fundamentales de codificación: instantáneos, compactos, perfectos, correctores, lineales, cíclicos.

RA260 - Comprender y manejar primitivas y esquemas básicos de mantenimiento de la integridad (funciones hash) y de autenticación (firmas digitales) de la información.

RA94 - Aplicar la teoría de grupos, anillos y cuerpos para resolver problemas prácticos de áreas como la criptografía y la teoría de códigos.

RA269 - Comprender e interpretar la utilización y necesidad de la criptografía en la tecnología blockchain.

RA266 - Comprender e interpretar los principales elementos de la codificación.

RA263 - Comprender la diversa fundamentación de la criptografía no cuántica frente a la variante cuántica y algunos sistemas post-cuánticos.

5. Descripción de la asignatura y temario

5.1. Descripción de la asignatura

La asignatura recoge los conocimientos fundamentales y necesarios relativos a los métodos de protección de la información, tanto para asegurar que el receptor sea capaz de recuperar la información enviada por el emisor (Codificación) como para asegurar la confidencialidad, integridad y autenticación de la misma (Criptografía).

Se inicia el temario con el Modelo del sistema de comunicación y los conceptos de información, incertidumbre (entropía) y capacidad del canal. Se estudian conceptos básicos de protección de la información frente a errores del canal, presentando los códigos fundamentales (lineales y cíclicos).

Seguidamente se hace un recorrido por la Criptografía clásica y moderna. Se exponen los sistemas simétricos y asimétricos, profundizando en los principales esquemas criptológicos. Siguen bloques relativos a las funciones hash y los esquemas de firmas digitales y certificados. Finalmente, se expone la situación actual de la Criptografía postcuántica, y la intrínseca relación de la Criptografía con la Blockchain.

5.2. Temario de la asignatura

1. Modelo del sistema de comunicación
    1.1. Fuente y codificación
    1.2. Entropía e información
    1.3. Capacidad de canal
2. Codificación
    2.1. Fuentes con memoria y sin memoria
    2.2. Canal con ruido y sin ruido
    2.3. Códigos instantáneos y de decodificación única
    2.4. Códigos compactos: algoritmo de Huffman
    2.5. Teoremas de Shannon
    2.6. Códigos correctores (Hadamard, Reed-Muller)
    2.7. Códigos perfectos
3. Códigos lineales
    3.1. Definición y propiedades
    3.2. Matriz generadora y de paridad
    3.3. Decodificación
    3.4. Probabilidad de error
    3.5. Código Hamming
4. Códigos cíclicos
    4.1. Definición y propiedades
    4.2. Estructura matricial
    4.3. Circuitos codificadores
    4.4. Detección de errores
    4.5. Decodificación
    4.6. Códigos BCH (Bose-Chaudhuri-Hocquenghem)

4.7. Códigos Reed-Solomon

5. Historia de la Criptografía

5.1. Cifrados de transposición y de sustitución monográmicos, poligrámicos, monoalfabéticos, polialfabéticos y homofónicos

5.2. Cifrados mixtos y máquinas de rotores (ENIGMA)

5.3. Cifrado perfecto

5.4. Conceptos fundamentales y sistematización

6. Criptografía simétrica

6.1. Principios y tipología de la criptografía de clave secreta o simétrica

6.2. DES (Data Encryption Standard) y T-DES (Triple DES)

6.3. AES (Advanced Encryption Standard)

6.4. Modos de funcionamiento

6.5. Cifrados de flujo

7. Criptografía asimétrica

7.1. Principios de la criptografía de clave pública o asimétrica

7.2. Protocolo de Intercambio de clave de Diffie-Hellman

7.3. RSA y el Problema de la Factorización de Enteros

7.4. ElGamal y el Problema del Logaritmo Discreto

7.5. Curvas Elípticas y el Problema del Logaritmo Discreto en Curva Elíptica

8. Funciones Hash

8.1. Definición y propiedades

8.2. Familias SHA-1 y SHA-2

8.3. SHA-3 (Keccak)

9. Firma digital y certificados

9.1. Principales características

9.2. Algoritmos de firma digital

10. Criptografía cuántica

10.1. Conceptos básicos de Mecánica cuántica

10.2. Qubit, puertas lógicas cuánticas y ordenadores cuánticos

10.3. Algoritmo de Shor (Problemas de Factorización de Enteros y del Logaritmo Discreto)

10.4. Cifrados resistentes a ataques cuánticos

11. Blockchain

11.1. Definiciones, historia, estructura y tipología

11.2. Bitcoin y otras criptomonedas

11.3. Cadena de bloques y criptografía

11.4. Identidad autosoberana

12. Criptografía y programación

12.1. Lenguajes de programación criptográfica

12.2. Simuladores cuánticos

6. Cronograma

6.1. Cronograma de la asignatura *

Sem	Actividad tipo 1	Actividad tipo 2	Tele-enseñanza	Actividades de evaluación
1	**Presentación** Duración: 00:30 LM: Actividad del tipo Lección Magistral **Tema 1: Teoría** Duración: 03:30 LM: Actividad del tipo Lección Magistral **Tema 1: Ejercicios** Duración: 01:00 PR: Actividad del tipo Clase de Problemas			
2	**Tema 2: Teoría** Duración: 04:00 LM: Actividad del tipo Lección Magistral **Tema 2: Ejercicios** Duración: 01:00 PR: Actividad del tipo Clase de Problemas			
3	**Tema 2: Teoría** Duración: 02:00 LM: Actividad del tipo Lección Magistral **Tema 2: Ejercicios** Duración: 00:30 PR: Actividad del tipo Clase de Problemas **Tema 3: Teoría** Duración: 02:00 LM: Actividad del tipo Lección Magistral **Tema 3: Ejercicios** Duración: 00:30 PR: Actividad del tipo Clase de Problemas			
4	**Tema 3: Teoría** Duración: 04:00 LM: Actividad del tipo Lección Magistral **Tema 3: Ejercicios** Duración: 00:30 PR: Actividad del tipo Clase de Problemas **Ejercicio breve** Duración: 00:30 OT: Otras actividades formativas / Evaluación			**Ejercicio breve** EX: Técnica del tipo Examen Escrito Evaluación Progresiva Presencial Duración: 00:30

5	**Tema 4: Teoría** Duración: 04:00 LM: Actividad del tipo Lección Magistral **Tema 4: Ejercicios** Duración: 00:30 PR: Actividad del tipo Clase de Problemas **Ejercicio breve** Duración: 00:30 OT: Otras actividades formativas / Evaluación			**Ejercicio breve** EX: Técnica del tipo Examen Escrito Evaluación Progresiva Presencial Duración: 00:30
6	**Tema 5: Teoría** Duración: 03:00 LM: Actividad del tipo Lección Magistral **Tema 5: Ejercicios** Duración: 00:30 PR: Actividad del tipo Clase de Problemas **Primera prueba (temas 1 al 4, inclusive)** Duración: 01:30 OT: Otras actividades formativas / Evaluación			**Primera prueba (temas 1 al 4, inclusive)** EX: Técnica del tipo Examen Escrito Evaluación Progresiva Presencial Duración: 01:30
7	**Tema 5: Teoría** Duración: 04:00 LM: Actividad del tipo Lección Magistral **Tema 5: Ejercicios** Duración: 01:00 PR: Actividad del tipo Clase de Problemas			
8	**Tema 6: Teoría** Duración: 04:00 LM: Actividad del tipo Lección Magistral **Tema 6: Ejercicios** Duración: 00:30 PR: Actividad del tipo Clase de Problemas **Ejercicio breve** Duración: 00:30 OT: Otras actividades formativas / Evaluación			**Ejercicio breve** EX: Técnica del tipo Examen Escrito Evaluación Progresiva Presencial Duración: 00:30
9	**Tema 6: Teoría** Duración: 02:00 LM: Actividad del tipo Lección Magistral **Tema 6: Ejercicios** Duración: 00:30 PR: Actividad del tipo Clase de Problemas **Tema 7: Teoría** Duración: 02:00 LM: Actividad del tipo Lección Magistral **Tema 7: Ejercicios** Duración: 00:30 PR: Actividad del tipo Clase de Problemas			

10	**Tema 7: Teoría** Duración: 04:00 LM: Actividad del tipo Lección Magistral **Tema 7: Ejercicios** Duración: 00:30 PR: Actividad del tipo Clase de Problemas **Ejercicio breve** Duración: 00:30 OT: Otras actividades formativas / Evaluación			**Ejercicio breve** EX: Técnica del tipo Examen Escrito Evaluación Progresiva Presencial Duración: 00:30
11	**Tema 7: Teoría** Duración: 02:00 LM: Actividad del tipo Lección Magistral **Tema 7: Ejercicios** Duración: 00:30 PR: Actividad del tipo Clase de Problemas **Tema 8: Teoría** Duración: 02:00 LM: Actividad del tipo Lección Magistral **Tema 8: Ejercicios** Duración: 00:30 PR: Actividad del tipo Clase de Problemas			
12	**Tema 9: Teoría** Duración: 02:00 LM: Actividad del tipo Lección Magistral **Tema 9: Ejercicios** Duración: 00:30 PR: Actividad del tipo Clase de Problemas **Tema 10: Teoría** Duración: 01:30 LM: Actividad del tipo Lección Magistral **Tema 10: Ejercicios** Duración: 00:30 PR: Actividad del tipo Clase de Problemas **Ejercicio breve** Duración: 00:30 OT: Otras actividades formativas / Evaluación			**Ejercicio breve** EX: Técnica del tipo Examen Escrito Evaluación Progresiva Presencial Duración: 00:30
13	**Tema 10: Teoría** Duración: 02:00 LM: Actividad del tipo Lección Magistral **Tema 10: Ejercicios** Duración: 00:30 PR: Actividad del tipo Clase de Problemas **Tema 11: Teoría** Duración: 02:30 LM: Actividad del tipo Lección Magistral			

14	**Tema 11: Teoría** Duración: 02:00 LM: Actividad del tipo Lección Magistral **Tema 12: Teoría** Duración: 02:30 LM: Actividad del tipo Lección Magistral **Ejercicio breve** Duración: 00:30 OT: Otras actividades formativas / Evaluación			**Ejercicio breve** EX: Técnica del tipo Examen Escrito Evaluación Progresiva Presencial Duración: 00:30
15	**Tema 12: Teoría** Duración: 01:00 LM: Actividad del tipo Lección Magistral **Ejercicios** Duración: 01:00 PR: Actividad del tipo Clase de Problemas			
16				**Segunda prueba (temas 5 al 12, inclusive)** EX: Técnica del tipo Examen Escrito Evaluación Progresiva Presencial Duración: 01:30
17				**Prueba global (temas 1 al 12, inclusive)** EX: Técnica del tipo Examen Escrito Evaluación Global Presencial Duración: 03:00

Para el cálculo de los valores totales, se estima que por cada crédito ECTS el alumno dedicará dependiendo del plan de estudios, entre 26 y 27 horas de trabajo presencial y no presencial.

7. Actividades y criterios de evaluación

7.1. Actividades de evaluación de la asignatura

7.1.1. Evaluación (progresiva)

Sem.	Descripción	Modalidad	Tipo	Duración	Peso en la nota	Nota mínima	Competencias evaluadas
4	Ejercicio breve	EX: Técnica del tipo Examen Escrito	Presencial	00:30	5%	0 / 10	CB2 CE7 CB4 CE1 CE2 CE3 CG1 CG4 CG3 CB5
5	Ejercicio breve	EX: Técnica del tipo Examen Escrito	Presencial	00:30	5%	0 / 10	CB2 CE7 CB4 CE1 CE2 CE3 CG1 CG4 CG3 CB5
6	Primera prueba (temas 1 al 4, inclusive)	EX: Técnica del tipo Examen Escrito	Presencial	01:30	30%	1 / 10	CB2 CE7 CB4 CE1 CE2 CE3 CG1 CG4 CG3 CB5
8	Ejercicio breve	EX: Técnica del tipo Examen Escrito	Presencial	00:30	5%	0 / 10	CB2 CE7 CB4 CE1 CE2 CE3 CG1 CG4 CG3

							CB5
10	Ejercicio breve	EX: Técnica del tipo Examen Escrito	Presencial	00:30	5%	0 / 10	CB2 CE7 CB4 CE1 CE2 CE3 CG1 CG4 CG3 CB5
12	Ejercicio breve	EX: Técnica del tipo Examen Escrito	Presencial	00:30	5%	0 / 10	CB2 CE7 CB4 CE1 CE2 CE3 CG1 CG4 CG3 CB5
14	Ejercicio breve	EX: Técnica del tipo Examen Escrito	Presencial	00:30	5%	0 / 10	CB2 CE7 CB4 CE1 CE2 CE3 CG1 CG4 CG3 CB5
16	Segunda prueba (temas 5 al 12, inclusive)	EX: Técnica del tipo Examen Escrito	Presencial	01:30	40%	1 / 10	CB2 CE7 CB4 CE1 CE2 CE3 CG1 CG4 CG3 CB5

7.1.2. Prueba evaluación global

Sem	Descripción	Modalidad	Tipo	Duración	Peso en la nota	Nota mínima	Competencias evaluadas
17	Prueba global (temas 1 al 12, inclusive)	EX: Técnica del tipo Examen Escrito	Presencial	03:00	100%	0 / 10	CB2 CE7 CB4 CE1 CE2 CE3 CG1 CG4

							CG3 CB5

7.1.3. Evaluación convocatoria extraordinaria

Descripción	Modalidad	Tipo	Duración	Peso en la nota	Nota mínima	Competencias evaluadas
Examen convocatoria extraordinaria	EX: Técnica del tipo Examen Escrito	Presencial	03:00	100%	0 / 10	CB2 CE7 CB4 CE1 CE2 CE3 CG1 CG4 CG3 CB5

7.2. Criterios de evaluación

La evaluación tiene dos convocatorias durante el curso: ordinaria y extraordinaria.

A) Convocatoria ordinaria

Presenta dos modalidades: progresiva y global.

A.1) Progresiva. Es la modalidad de evaluación continuada o progresiva en el tiempo.

La asignatura puede dividirse en dos partes o secciones: la codificación (temas 1-4) y la criptografía (temas 5-12).

- Habrá un examen escrito presencial sin libros al final del bloque de codificación (temas 1-4). Su peso es del 30% del total de la nota de la asignatura. Tiene una nota mínima de 1 sobre 10.

- Habrá un examen escrito presencial sin libros al final del bloque de criptografía (temas 5-12). Su peso es del 40% del total de la nota de la asignatura. Tiene una nota mínima de 1 sobre 10.

- Durante la parte del bloque de codificación habrá dos pruebas breves escritas presenciales con ayuda de apuntes, realizadas en clase, cada una de las cuales tendrá un peso del 5% del total de la asignatura. Ocurrirán en torno a las semanas 4 y 5. No tienen nota mínima.

- Durante la parte del bloque de criptografía habrá cuatro pruebas breves escritas presenciales con ayuda de apuntes, realizadas en clase, cada una de las cuales tendrá un peso del 5% del total de la asignatura. Ocurrirán en torno a las semanas 8, 10, 12 y 14. No tienen nota mínima.

+ La asignatura se considerará superada si se obtiene una puntuación igual o mayor que un 50% de la nota total y además se alcanzan las notas mínimas de los dos exámenes mencionados.

A.2) Global. Es la modalidad de evaluación con una única prueba total o global.

- Habrá un examen escrito presencial sin libros de toda la asignatura (temas 1-12). Su peso es del 100% del total de la nota de la asignatura. No tiene nota mínima en ninguna de sus partes o secciones.

+ La asignatura se considerará superada si se obtiene una puntuación igual o mayor que un 50% de la nota total.

* Los alumnos que se presenten a la prueba de la modalidad progresiva (A.1) de la parte del bloque de criptografía no podrán presentarse a la modalidad de evaluación global. Los alumnos que no se presenten a dicha parte (temas 5-12), aunque lo hicieran al bloque de codificación (temas 1-4) de la modalidad progresiva, podrán renunciar a la modalidad de evaluación progresiva que estuvieran llevando, presentándose al examen de la modalidad global, siendo su nota final la que aquí, en la global, obtengan.

B) Convocatoria extraordinaria

Los alumnos que no se hayan presentado o no hayan superado la convocatoria ordinaria podrán presentarse a la extraordinaria.

- Habrá un examen escrito presencial sin libros de toda la asignatura (temas 1-12). Su peso es del 100% del total de la nota de la asignatura. No tiene nota mínima en ninguna de sus partes o secciones.

+ La asignatura se considerará superada si se obtiene una puntuación igual o mayor que un 50% de la nota total.

8. Recursos didácticos

8.1. Recursos didácticos de la asignatura

Nombre	Tipo	Observaciones
Dominic Welsh. "Codes and Cryptography". Oxford Science Publications, Oxford, 1988.	Bibliografía	Básica
Cándido López García, Manuel Fernández Veiga. "Teoría de la Información y Codificación". Andavira, Santiago de Compostela, 2013.	Bibliografía	Básica
Song Y. Yan. "Number Theory for Computing". Springer, Berlín, 2002.	Bibliografía	Básica
Douglas R. Stinson. "Cryptography. Theory and Practice". Chapman & Hall /CRC, Boca Raton, 2002.	Bibliografía	Complementaria
Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone. "Handbook of Applied Cryptography". CRC Press, Boca Raton, Florida, 1996.	Bibliografía	Complementaria

Daniel T. Gillespie. "Introducción a la Mecánica Cuántica". Reverté, Barcelona, 2002.	Bibliografía	Complementaria
Michael A. Nielsen, Isaac L. Chuang. "Quantum Computation and Quantum Information". Cambridge University Press, Cambridge, 2010.	Bibliografía	Complementaria
Andreas M. Antonopoulos. "Mastering Bitcoin". O'Reilly, Beijing, 2017.	Bibliografía	Complementaria
John Viega, Matt Messier. "Secure Programming Cookbook for C and C++". O'Reilly, Beijing, 2003.	Bibliografía	Complementaria
Jonathan Knudsen. "Java Cryptography". O'Reilly, Beijing, 1998.	Bibliografía	Complementaria
Seth J. Nielson, Christopher K. Monson. "Practical Cryptography in Python: Learning Correct Cryptography by Example". Apress, New York, 2019.	Bibliografía	Complementaria
Vicente Jara Vera, Carmen Sánchez Ávila. "Problemas resueltos de Criptografía". Paraninfo, Madrid, 2019.	Bibliografía	Básica
Material de trabajo de la asignatura elaborado por el profesorado y disponible en Moodle	Recursos web	Básica / Complementaria

9. Otra información

9.1. Otra información sobre la asignatura

La asignatura se relaciona directamente con los siguientes ODS, en tanto que los conocimientos y técnicas que en ella se presentan sirven para preservar la privacidad y asegurar que cualquier tipo de comunicación informática pueda realizarse de forma eficiente y segura:

ODS 9: "Construir infraestructuras resilientes, promover la industrialización sostenible y fomentar la innovación".

ODS 11: "Lograr que las ciudades sean más inclusivas, seguras, resilientes y sostenibles".

ODS 16: "Promover sociedades justas, pacíficas e inclusivas", donde en la meta 16.10 se afirma: "Garantizar el acceso público a la información y proteger las libertades fundamentales, de conformidad con las leyes nacionales y los acuerdos internacionales".