Proyecto/Guía docente de la asignatura Códigos y Criptografía

Asignatura	Códigos y Criptografía		
Materia	Computación		
Módulo	Tecnologías específicas		
Titulación	Grado en ingeniería informática		
Plan	545	**Código**	46948
Periodo de impartición	Primer cuatrimestre	**Tipo/Carácter**	Optativa
Nivel/Ciclo	Grado	**Curso**	Tercero
Créditos ECTS	6		
Lengua en que se imparte	Castellano		
Profesor/es responsable/s	Diego Ruano Benito		
Datos de contacto (E-mail, teléfono…)	Email: diego.ruano@uva.es. Teléfono: 983185084. Despacho: A313 de la Facultad de Ciencias		
Departamento	Álgebra, Análisis Matemático, Geometría y Topología		

1. Situación / Sentido de la Asignatura

1.1 Contextualización

Los datos transmitidos a través de sistemas de comunicación digital pueden corromperse, lo que resulta en un desajuste entre los símbolos enviados y recibidos. Los códigos correctores de errores garantizan una transmisión fiable y rápida de información en dichos sistemas agregando símbolos adicionales a la información enviada. De esta forma, aunque algunos símbolos sean corrompidos, se puede recrear la información original gracias a la redundancia introducida. El desafío es construir códigos que, además de corregir muchos errores utilizando la menor cantidad de símbolos adicionales posible, también vengan acompañados de algoritmos rápidos de codificación y descodificación.

Además, normalmente se requiere que la información digital que se transmite o almacena esté protegida frente a terceros no autorizados. Históricamente, la criptografía ha ido evolucionando desde sistemas de clave privada, en la que el emisor y el receptor comparten una clave, a implementar también el uso de sistemas de clave privada, donde hay una clave pública para cifrar y una privada para descifrar. La irrupción del ordenador cuántico está modificando los estándares usados actualmente (criptografía postcuántica). Además, hoy es necesario disponer métodos criptográficos adicionales como la firma digital.

Ambas disciplinas están fuertemente basadas en métodos matemáticos.

1.2 Relación con otras materias

Fundamentos Básicos de Matemáticas (Álgebra lineal y Matemática discreta)

1.3 Prerrequisitos

Recomendable: conocimiento de Fundamentos Básicos de Matemáticas

2. Competencias

2.1 Generales

G16- Capacidad de aplicar los conocimientos en la práctica.
G18- Capacidad de aprender.

2.2 Específicas

CC6- Capacidad para desarrollar y evaluar sistemas interactivos y de presentación de información compleja y su aplicación a la resolución de problemas de diseño de interacción persona computadora.
IC6- Capacidad para comprender, aplicar y gestionar la garantía y seguridad de los sistemas informáticos.

3. Objetivos

CC6.1-Conocer y comprender los principios básicos de la codificación y de la teoría de la información y conocer y manejar con soltura los principios de la codificación orientada a la compresión de datos, a la corrección de errores y a la seguridad.
IC6.1- Conocer el estado actual de las técnicas criptográficas y su evolución histórica y manejar con soltura los principales algoritmos de cifrado tanto de clave privada como de clave pública.
IC6.2-Conocer y manejar los principales protocolos criptográficos, sus objetivos y sus técnicas.
IC6.3- Implementar y programar algunos protocolos criptográficos sencillos.

4. Contenidos y/o bloques temáticos

Bloque 1: "Códigos correctores de errores"

Carga de trabajo en créditos ECTS: 3

a. Contextualización y justificación

Como se ha descrito en el apartado 1.1 de esta guía, los códigos correctores de errores son necesarios para la comunicación y almacenamiento de información digital. Además, veremos cómo esta disciplina está fuertemente basada en métodos matemáticos.

b. Objetivos de aprendizaje

Conocer y comprender la construcción y descodificación de códigos correctores de errores. Desde la teoría matemática en la que están basados, hasta su implementación práctica.

c. Contenidos

Fundamentos de la teoría de la información. Códigos correctores, parámetros y cotas. Códigos lineales. Códigos Reed-Solomon. Breve introducción a otras familias de códigos. Código compresor de Huffman.

d. Métodos docentes

Lecciones magistrales. Clases prácticas en el aula y con ordenador. Trabajos propuestos a los alumnos.

e. Plan de trabajo

Lecciones teóricas y prácticas. Resolución de problemas usando SAGE (software matemático basado en Python).

f. Evaluación

Ver apartado 7 de esta guía

g Material docente

g.1 Bibliografía básica

-J. Justensen, T. Høholdt. A course in error-correcting codes. Second Edition. Textbooks in Mathematics. Second Edition. European Mathematical Society (2017)
-C. Munuera, J. Tena. Codificación de la Información. Pub. Universidad de Valladolid (1997)

g.2 Bibliografía complementaria

-W.C. Huffman, V. Pless. Fundamentals of Error-Correcting Codes. Cambridge University Press (2003)
-J.H. van Lint. Introduction to Coding Theory. Graduate Texts in Mathematics 86. Springer (1999)
-R. Pellikaan, X.W. Wu, S. Bulygin, R. Jurrius. Codes, Cryptology and Curves with Computer Algebra. Cambridge University Press (1997).

g.3 Otros recursos telemáticos (píldoras de conocimiento, blogs, videos, revistas digitales, cursos masivos (MOOC), …)

Páginas web de ayuda y foros del programa SAGE.
Vídeos en Youtube de “Art of the problem”.

h. Recursos necesarios

Aula y ordenador con el programa SAGE basado en Python (libre y gratuito).

i. Temporalización

CARGA ECTS	PERIODO PREVISTO DE DESARROLLO
3	Semanas 1-8

Bloque 2: “Criptografía”

Carga de trabajo en créditos ECTS: 3

a. Contextualización y justificación

Como se ha descrito en el apartado 1.1 de esta guía, la criptografía es necesaria para preservar la privacidad en el ámbito digital. Además, veremos cómo esta disciplina está fuertemente basada en métodos matemáticos.

b. Objetivos de aprendizaje

Conocer y comprender los principales criptosistemas. Desde la teoría matemática en la que están basados, hasta su implementación práctica.

c. Contenidos

Historia de la criptografía. Criptografía de clave privada (o simétrica), en particular el criptosistema AES (Advanced encryption Standard). Criptografía de clave privada (o asimétrica) y firma digital, en particular los

criptosistemas RSA y ElGamal. Criptografía postcuántica, en particular el criptosistema de McEliece. Compartición de secretos, en particular el método de Shamir. Intercambio de claves cuántico, en particular BB84.

d. Métodos docentes

Lecciones magistrales. Clases prácticas en el aula y con ordenador. Trabajos propuestos a los alumnos.

e. Plan de trabajo

Lecciones teóricas y prácticas. Resolución de problemas usando SAGE (software matemático basado en Python).

f. Evaluación

Ver apartado 7 de esta guía.

g Material docente

g.1 Bibliografía básica

-J. Buchmann, Introduction to Cryptography. Undergraduate Texts in Mathematics, Springer (2004)
-M.I. González Vasco, A. L. Pérez del Pozo. Criptografía Esencial. Principios básicos para el diseño de esquemas y protocolos seguros. RA-MA (2021)
-C. Munuera, J. Tena. Codificación de la Información. Pub. Universidad de Valladolid (1997)

g.2 Bibliografía complementaria

-A.J. Menezes, P.C. van Oorschot, S.A. Vanstone. Handbook of Applied Cryptography. CRC Press 1996.
-P. Caballero: Introducción a la criptografía. 2ª Edición actualizada. RA-MA (2002)
-M.I. González Vasco. Las matemáticas de la criptología. Secretos demostrables y demostraciones secretas. Miradas Matemáticas. Catarata (2018)

g.3 Otros recursos telemáticos (píldoras de conocimiento, blogs, videos, revistas digitales, cursos masivos (MOOC), …)

Páginas web de ayuda y foros del programa SAGE.
Vídeos en Youtube de “Art of the problem”.

h. Recursos necesarios

Aula y ordenador con el programa SAGE basado en Python (libre y gratuito).

i. Temporalización

CARGA ECTS	PERIODO PREVISTO DE DESARROLLO
3	Semanas 8-15

5. Métodos docentes y principios metodológicos

Se combinará la clase magistral junto con el aprendizaje basado en resolución de problemas.

6. Tabla de dedicación del estudiante a la asignatura

ACTIVIDADES PRESENCIALES o PRESENCIALES A DISTANCIA(1)	HORAS	ACTIVIDADES NO PRESENCIALES	HORAS
Clases teórico-prácticas (T/M)	43	Estudio y trabajo autónomo individual	90
Clases prácticas de aula (A)		Estudio y trabajo autónomo grupal	
Laboratorios (L)	15		
Practicas externas, clínicas o de campo			
Seminarios (S)			
Tutorías grupales (TG)			
Evaluación (fuera del periodo oficial de exámenes)	2		
Total presencial	**60**	Total no presencial	**90**
		TOTAL presencial + no presencial	**150**

(1) Actividad presencial a distancia es cuando un grupo sigue una videoconferencia de forma síncrona a la clase impartida por el profesor para otro grupo presente en el aula.

7. Sistema y características de la evaluación

Criterio: cuando al menos el 50% de los días lectivos del cuatrimestre transcurran en normalidad, se asumirán como criterios de evaluación los indicados en la guía docente. Se recomienda la evaluación continua ya que implica minimizar los cambios en la adenda.

INSTRUMENTO/PROCEDIMIENTO	PESO EN LA NOTA FINAL	OBSERVACIONES
Dos pequeños exámenes a lo largo del cuatrimestre. De unos 40 minutos de duración cada uno	20%	Uno de la parte de códigos correctores y otro de la parte de criptografía
Entrega de prácticas: resolución de ejercicios en Sage, software basado en Python	20%	Una de la parte de códigos correctores y otra de la parte de criptografía
Examen final escrito	60%	En el periodo de exámenes

CRITERIOS DE CALIFICACIÓN

- **Convocatoria ordinaria:**
  - De acuerdo a la tabla anterior.
  - Exactitud, claridad, precisión en la exposición de conceptos y cálculos.
- **Convocatoria extraordinaria:**
  - El examen escrito tendrá un peso entre el 60% y el 100% dependiendo de si el alumno quiere que los otros ítems de calificación sean tenidos en cuenta.
  - Exactitud, claridad, precisión en la exposición de conceptos y cálculos.

8. Consideraciones finales