Guía docente de CÓDIGOS y CRIPTOGRAFÍA

Asignatura	CÓDIGOS Y CRIPTOGRAFÍA		
Materia	COMPUTACIÓN		
Módulo	Tecnologías Específicas		
Titulación	GRADO EN INGENIERÍA INFORMÁTICA (454)		
Plan	545	**Código**	46948
Periodo de impartición	1er. CUATRIMESTRE	**Tipo/Carácter**	OPTATIVA
Nivel/Ciclo	GRADO	**Curso**	3º
Créditos ECTS	6 ECTS		
Lengua en que se imparte	CASTELLANO		
Profesor/es responsable/s	Manuel M. Carnicer Arribas		
Datos de contacto (E-mail, teléfono…)	TELÉFONO: 983 423029 E-MAIL: carnicer@agt.uva.es		
Departamento	Álgebra, Análisis Matemático, Geometría y Topología		

1. Situación / Sentido de la Asignatura

1.1 Contextualización

La criptografía es imprescindible para el comercio electrónico, la privacidad en la red, la autentificación del usuario, el acceso restringido y la seguridad informática. Aparte de usos militares, diplomáticos, espionaje.

1.2 Relación con otras materias

Muy relacionado con aritmética modular y álgebra.

1.3 Prerrequisitos

Matemática discreta. Buena disposición hacia las matemáticas.

2. Competencias

2.1 Generales

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

2.2 Específicas

Código	Descripción
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

Código	Descripción
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. Tabla de dedicación del estudiante a la asignatura

ACTIVIDADES PRESENCIALES	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**		
Prácticas 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**

5. Bloques temáticos

Bloque 1: Fundamentos Matemáticos

Carga de trabajo en créditos ECTS: 1

a. Contextualización y justificación

Esta asignatura tiene un alto contenido matemático, de álgebra y teoría de números.

Hay que presentar la base matemática a los alumnos

b. Objetivos de aprendizaje

Es necesario aprender y saber contenidos elevados de álgebra y teoría de números.

Así mismo, es necesaria la presentación de cuerpos finitos y algo de álgebra lineal sobre ellos.

c. Contenidos

1. Aritmética modular.
2. Álgebra y aritmética de los cuerpos finitos.
3. Logaritmo discreto.
4. La importancia de los números primos.
5. Espacios vectoriales y subespacios en cuerpos finitos..

d. Métodos docentes

- Clase tradicional. Parece que las nuevas tecnologías no han superado a una buena comunicación personal y directa entre docente y alumnos.
- Estudio de casos en aula y en laboratorio
- Resolución de problemas

e. Plan de trabajo

- Estudio de la teoría y conocimientos matemáticos prácticos que son de inmediata aplicación en códigos y criptografía.

f. Evaluación

Ver punto 7 de esta guía.

g. Bibliografía básica

C. Munuera, J. Tena: Codificación de la Información, U. de Valladolid, 1997.

h. Bibliografía complementaria

i. Recursos necesarios

Bloque 2: Códigos correctores y compresores

Carga de trabajo en créditos ECTS: 2

a. Contextualización y justificación

Esta asignatura tiene un alto contenido matemático, de álgebra y teoría de números.

Los códigos compresores y correctores son fundamentales en el almacenamiento y la transmisión de datos digitales.

b. Objetivos de aprendizaje

Los objetivos que se deducen obviamente de los contenidos.

c. Contenidos

6. Fundamentos de teoría de la información
7. Códigos compresores y óptimos.
8. Códigos correctores.
9. Códigos Lineales

d. Métodos docentes

- Clase tradicional. Parece que las nuevas tecnologías no han superado a una buena comunicación personal y directa entre docente y alumnos.
- Estudio de casos en aula y en laboratorio
- Resolución de problemas
- Desarrollo de proyectos (programas informáticos).
- Recopilación de información en la Red.

e. Plan de trabajo

- Estudio de la teoría y conocimientos matemáticos prácticos que son de inmediata aplicación en códigos.
- Conocimiento de ciertos estándares de codificación. En ningún caso se exige aprender de memoria de forma exacta.
- El alumno debe elaborar~programar un usando códigos correctores, a escoger entre varios modelos propuestos por el profesor y con su asesoramiento. La dificultad matemática será siempre asesorada por el profesor.
- Un pequeño conocimiento práctico del sistema wxMaxima, con el que se solventan algunas dificultades matemáticas.

f. Evaluación

Ver punto 7 de esta guía.

g. Bibliografía básica

C. Munuera, J. Tena: Codificación de la Información, U. de Valladolid, 1997.

h. Bibliografía complementaria

i. Recursos necesarios

El programa wxMaxima, de libre distribución, es un auxiliar adecuado.

Bloque 3: Criptografía

Carga de trabajo en créditos ECTS: 3

a. Contextualización y justificación

Esta asignatura tiene un alto contenido matemático, de álgebra y teoría de números.

La criptografía es imprescindible para el comercio electrónico, la privacidad en la red, la autentificación del usuario, el acceso restringido y la seguridad informática. Aparte de usos militares, diplomáticos, espionaje.

b. Objetivos de aprendizaje

Los objetivos que se deducen obviamente de los contenidos.

c. Contenidos

10. Criptografía de clave pública. Criptosistemas tipo ElGamal.
11. Criptosistema RSA. PKCS # 1. Public-Key Cryptography Standards.
12. Cifrado en flujo. Criptosistema RC4.
13. Funciones hash. SHA1. MD5. One-way functions.
14. Firma digital. Sha1 RSA. Autentificación de mensajes.
15. Advanced encryption Standard. AES.
16. El cifrador Salsa 20.
17. Secretos compartidos. Varias personas comparten una información crítica sin que ninguno individualmente tenga acceso ni a una mínima parte de dicha información.

d. Métodos docentes

- Clase tradicional. Parece que las nuevas tecnologías no han superado a una buena comunicación personal y directa entre docente y alumnos.
- Estudio de casos en aula y en laboratorio
- Resolución de problemas
- Desarrollo de proyectos (programas informáticos).
- Recopilación de información en la Red.

e. Plan de trabajo

- Estudio de la teoría y conocimientos matemáticos prácticos que son de inmediata aplicación en criptografía.
- Conocimiento de ciertos estándares de criptografía. En ningún caso se exige aprender de memoria de forma exacta.
- El alumno debe elaborar~programar un encriptador-desencriptador, a escoger entre varios modelos propuestos por el profesor y con su asesoramiento. La dificultad matemática será siempre asesorada por el profesor.
- Un pequeño conocimiento práctico del sistema wxMaxima, con el que se solventan algunas dificultades matemáticas.

f. Evaluación

Ver punto 7 de esta guía.

g. Bibliografía básica

- C. Munuera, J. Tena: Codificación de la Información, U. de Valladolid, 1997.
- Menezes, Oorschot, Vanstone, Handbook of Applied Cryptography, CRC Press. ISBN 0-8493-8523-7

h. Bibliografía complementaria

- en.wikipedia.org
- http://www.aescrypt.com/
- http://techheap.packetizer.com/cryptography/
- Buchmann, Introduction to cryptography. ISBN 0-387-95034-6
- Rijmen, The Design of Rijndael Aes - the Advanced Encryption Standard, Editorial Springer. ISBN 3540425802 / 3-540-42580-2
- http://www.infosyssec.net/infosyssec/security/cry2.htm
- http://www.criptored.upm.es/
- http://csrc.nist.gov/groups/ST/toolkit/index.html

i. Recursos necesarios

El programa wxMaxima, de libre distribución, es un auxiliar adecuado.

6. Temporalización (por bloques temáticos)

BLOQUE TEMÁTICO	CARGA ECTS	PERIODO PREVISTO DE DESARROLLO
Bloque 1: Fundamentos matemáticos	1 ECTS	Semanas 1 a 3
Bloque 2: Códigos compresores y correctores	2 ECTS	Semanas 4 a 8
Bloque 3: Criptografía	3 ECTS	Semanas 9 a 15

7. Sistema de calificaciones – Tabla resumen

INSTRUMENTO/PROCEDIMIENTO	PESO EN LA NOTA FINAL	OBSERVACIONES
Dos pequeños microexámenes de teoría a lo largo del cuatrimestre. De unos 40 minutos de duración cada uno.	20%	Aproximadamente en semanas 5 y 8.
Entrega prácticas: dos programas informáticos realizados por el alumno [solo o en dúo].	15%	Aproximadamente semanas 6 y 13.
Examen final escrito	65%	Periodo de exámenes

CRITERIOS DE CALIFICACIÓN
• **Convocatoria ordinaria**: **Tal y como se indica en la tabla anterior. La fórmula de la nota es la suma ordinaria.** • **Convocatoria extraordinaria: Examen escrito, cuyo peso varía del 65% al 100%, según el alumno quiera incluir o no los otros ítems de calificación indicados en el cuadro previo. La nota de esos ítems es guardada para esta convocatoria, si el alumno quiere. Cada alumno decide libremente.**

8. Anexo: Métodos docentes

Se imparte clase en el aula con pizarra, explicando especialmente los fundamentos matemáticos y aritméticos de la criptografía.

Se visitan desde el aula varias de las páginas destinadas a fijar protocolos informáticos y a explicar los mismos. Se procura aprender en qué contextos se usan.

Visualización de criptosistemas utilizados por las diversas páginas web, según se navega por ellas.

En el laboratorio se realizarán algunos programas que implementan criptosismetas sencillos. O alguna de las partes de algún criptosistema más complejo.

En laboratorio se estudia el sistema algebraico wxMaxima, para tenerlo como herramienta en ciertas comprobaciones y cálculos previos a la programación práctica. Así como para ilustrar ciertas operaciones aritméticas complejas y algebraicas que están presentes en ciertos criptosistemas.