Guía docente de la asignatura

Asignatura	CÓDIGOS Y CRIPTOGRAFÍA		
Materia	COMPLEMENTOS DE COMPUTACIÓN		
Módulo	(vacío)		
Titulación	GRADO EN INGENIERÍA INFORMÁTICA (463)		
Plan	463	**Código**	45217
Periodo de impartición	1er. CUATRIMESTRE	**Tipo/Carácter**	OPTATIVA
Nivel/Ciclo	GRADO	**Curso**	4º
Créditos ECTS	6 ECTS		
Lengua en que se imparte	CASTELLANO		
Profesor/es responsable/s	José Enrique Marcos Naveira		
Datos de contacto (E-mail, teléfono…)	TELÉFONO: 983 423000 ext. 5002 E-MAIL: marcosje@agt.uva.es		
Horario de tutorías	En despacho A308 del edificio blanco que está enfrente de la Escuela de informática. Lunes de 18 a 20 horas. Martes de 16 a 18 horas. Miércoles de 16 a 18 horas. Y en cualquier momento en que el profesor se encuentre en dicho despacho.		
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. Todo ello es obvio.

1.2 Relación con otras materias

Muy relacionado con aritmética modular.

1.3 Prerrequisitos

Matemática discreta (NO es obligatorio tenerla aprobada).

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)	38	Estudio y trabajo autónomo individual	90
Clases prácticas de aula (A)		Estudio y trabajo autónomo grupal	
Laboratorios (L)	**20**		
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: El Nombre del Primer Bloque CRIPTOGRAFIA

Carga de trabajo en créditos ECTS: 6

a. Contextualización y justificación

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. Todo ello es obvio.

b. Objetivos de aprendizaje

Los que se deducen obviamente de los contenidos.

c. Contenidos

1. Aritmética modular. Nuevos trucos matemáticos para operar más eficientemente.
2. Cuerpos finitos. Logaritmo discreto.
3. Funciones hash. SHA1. MD5.
4. Criptografía de clave pública. Criptosistema RSA. PKCS # 1. Public-Key Cryptography Standards.
5. Firma digital. sha1 RSA. Autentificación de mensajes.
6. Advanced encryption Standard. AES.
7. Criptosistemas tipo ElGamal.
8. Cifrado en flujo. Registros lineales retroalimentados, Lineal Feedback Shift Registers, LFSR. Criptosistema RC4. Criptografía (débil) del Bluetooth.
9. Algunos sistemas criptográficos clásicos o rudimentarios. Vistazo a otros criptosistemas de menor aceptación.
10. La seguridad de criptosistemas (Vistazo).
11. Cámaras temporales criptográficas.
12. Secretos compartidos. Varias personas comparten una información crítica sin que ninguno individualmente tenga acceso ni a una mínima parte de dicha información.
13. Funciones de único sentido. One-way functions.
14. Códigos compresores sin pérdida.

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
- Recopilación de información en la Red.
- Descarga de programas ya elaborados de librerías comunes para entender y verificar su funcionamiento

e. Plan de trabajo

- Estudio de la teoría y conocimientos matemáticos prácticos que son de inmediata aplicación en criptografía. Nada de teoría pura matemática. Se va al grano, a lo que se aplica tal cual. Esto no debería presentar ninguna seria.
- 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 y resuelta por el profesor. El alumno tiene la tarea de programar, y que su programa funcione.

- Un pequeño conocimiento práctico del sistema MAPLE, con el que se solventan las dificultades matemáticas.
- Descarga, desde librerías usuales, de programas ya elaborados sobre stándares de criptografía, para entenderlos y comprobar su funcionamiento.

f. Evaluación

Ver punto 7 de esta guía.

g. Bibliografía básica

- Menezes, Oorschot, Vanstone, Handbook of Applied Cryptography, CRC Press. ISBN 0-8493-8523-7
- 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
- Latif, Simulation of Rijndael, Mars and RC6 of AES. ISBN 3639225457 / 3-639-22545-7. Libro del tipo “print on demand”. Se puede adquirir en www.abebooks.com
- http://eprint.iacr.org/
- http://www.infosyssec.net/infosyssec/security/cry2.htm
- http://www.criptored.upm.es/
- http://csrc.nist.gov/groups/ST/toolkit/index.html

h. Bibliografía complementaria

i. Recursos necesarios

MAPLE (proporcionado por la Universidad de Valladolid). Este programa solo funciona dentro del campus de la universidad, puesto que tenemos una licencia de campus. No funciona en casa.

6. Temporalización (por bloques temáticos)

BLOQUE TEMÁTICO	CARGA ECTS	PERIODO PREVISTO DE DESARROLLO
Bloque 1: Criptografía	6 ECTS	Semanas 1 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 30 minutos de duración cada uno.	10%	Aproximadamente en semanas 5 y 8. Si no se obtiene la calificación deseada, se puede renunciar a ella, y obtener la nota en el examen final.
Apreciación subjetiva de aplicación en laboratorio.	7%	Asistir al laboratorio, habiendo estudiado previamente algo de la parte teórica correspondiente a ese día.
Descarga de programas cortos de librerías, comprobar y entender su funcionamiento.	10%	Dos veces: Aproximadamente desde semana 4 hasta semana 10.
Entrega práctica programa informático realizado por el alumno [solo o en dúo].	23%	Aproximadamente semana 13. Es obligatorio para aprobar en primera convocatoria.
Examen final escrito	50%	Periodo de exámenes. Puede llegar hasta el 60% si se ha de recuperar la nota de los microexámenes.

CRITERIOS DE CALIFICACIÓN

• **Convocatoria ordinaria**: **Tal y como se indica en la tabla anterior. La fórmula de la nota es la suma ordinaria. Se procurará adaptar, individualmente, a necesidades específicas que tuviese el alumno.**
• **Convocatoria extraordinaria:**
  o **La entrega del programa elaborado por el alumno, deja de ser obligatoria para aprobar, si bien, sigue contando un 23% para la calificación.**
  o **Examen escrito, cuyo peso varía del 50% al 77%, según el alumno quiera incluir o no los otros ítems de calificación indicados en el cuadro previo que se deberían haber obtenido a lo largo del cuatrimestre. 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 MAPLE, para tenerlo como herramienta en ciertas comprobaciones y cálculos previos a la programación práctica. Así como para ilustra ciertas operaciones aritméticas complejas y algebraicas que están presentes en ciertos criptosistemas.

9. Anexo: Cronograma de actividades previstas

Nota: Las actividades previstas se solapan respecto de las semanas, ya que no se hacen en forma de compartimentos estancos.

- Semanas primera a quinta: exposición de los fundamentos matemáticos necesarios en criptografía: aritmética modular, cuerpos finitos, sucesiones lineales recurrentes sobre cuerpos finitos, logaritmo discreto, etc…
- Semanas tercera a séptima: exposición de funciones hashs, funciones de un único sentido y criptosistema RSA.
- Semanas cuarta a octava: estudio práctico del sistema MAPLE. Comprobación de su utilidad en los aspectos matemáticos de la criptografía.
- Semanas quinta a décimocuarta: realización en laboratorio informático de diversas prácticas relativas a los criptosistemas a medida que se vayan explicando.
- Semanas séptima a decimoquinta: elaboración por parte del alumno de una práctica consistente en un criptosistema sugerido por el profesor.