

**Guía docente de la asignatura**

Asignatura	PROTOCOLOS CRIPTOGRAFICOS		
Materia	AUDITORIA, CALIDAD Y SEGURIDAD		
Módulo	(vacío)		
Titulación	MASTER EN INGENIERIA INFORMATICA		
Plan		Código	2.1.3
Periodo de impartición	2º CUATRIMESTRE	Tipo/Carácter	OPTATIVA
Nivel/Ciclo	MASTER	Curso	
Créditos ECTS	3 ECTS		
Lengua en que se imparte	CASTELLANO		
Profesor/es responsable/s	Juan TENA AYUSO		
Datos de contacto (E-mail, teléfono...)	TELÉFONO: 983 423000 ext. 3045 E-MAIL: tena@agt.uva.es ,		
Horario de tutorías	Véase www.uva.es → Centros → Campus de Valladolid → Escuela Técnica Superior de Ingeniería Informática → Tutorías		
Departamento	Algebra, Análisis Matemático, Geometría y Topología		



1. Situación / Sentido de la Asignatura

1.1 Contextualización

La asignatura pretende dar a conocer el estado actual de las técnicas criptográficas y los principales protocolos derivados de las mismas, las herramientas matemáticas y criptográficas subyacentes así como su uso en diferentes contextos de interés tecnológico y social como firma electrónica, computación multipartita, comercio electrónico, votaciones electrónicas, etc.

1.2 Relación con otras materias

1.3 Prerrequisitos

La asignatura no requiere prerrequisitos específicos aunque se considera deseable la formación básica correspondiente a un grado en Ingeniería Informática o similar.





2. Competencias

2.1 Generales

Código	Descripción
CG1	Capacidad para proyectar, calcular y diseñar productos, procesos e instalaciones en todos los ámbitos de la ingeniería informática.
CG2	Capacidad para la dirección de obras e instalaciones de sistemas informáticos, cumpliendo la normativa vigente y asegurando la calidad del servicio
CG4	Capacidad para el modelado matemático, cálculo y simulación en centros tecnológicos y de ingeniería de empresa, particularmente en tareas de investigación, desarrollo e innovación en todos los ámbitos relacionados con la Ingeniería en Informática.
CG7	Capacidad para la puesta en marcha, dirección y gestión de procesos de fabricación de equipos informáticos, con garantía de la seguridad para las personas y bienes, la calidad final de los productos y su homologación.
CG8	Capacidad para la aplicación de los conocimientos adquiridos y de resolver problemas en entornos nuevos o poco conocidos dentro de contextos más amplios y multidisciplinarios, siendo capaces de integrar estos conocimientos.
CG9	Capacidad para comprender y aplicar la responsabilidad ética, la legislación y la deontología profesional de la actividad de la profesión de Ingeniero en Informática.
CG10	Capacidad para aplicar los principios de la economía y de la gestión de recursos humanos y proyectos, así como la legislación, regulación y normalización de la informática

2.2 Específicas

Código	Descripción
CET3	Capacidad para asegurar, gestionar, auditar y certificar la calidad de los desarrollos, procesos, sistemas, servicios, aplicaciones y productos informáticos
CET4	Capacidad para diseñar, desarrollar, gestionar y evaluar mecanismos de certificación y garantía de seguridad en el tratamiento y acceso a la información en un sistema de procesamiento local o distribuido



3. Objetivos

Código	Descripción
CET3, CET4	Conocer el estado actual de las técnicas criptográficas.
CET3, CET4	Implementar los principales criptosistemas discriminando en función de su uso concreto.
CET3, CET4	Capacidad de adaptar los sistemas criptográficos a situaciones concretas.
CET3, CET4	Conocer y manejar los principales protocolos criptográficos, sus objetivos y sus técnicas
CET3, CET4	Analizar la seguridad y los posibles ataques a los protocolos estudiados





4. Tabla de dedicación del estudiante a la asignatura

ACTIVIDADES PRESENCIALES	HORAS	ACTIVIDADES NO PRESENCIALES	HORAS
Clases teórico-prácticas (T/M)	12	Estudio y trabajo autónomo individual	
Clases prácticas de aula (A)		Estudio y trabajo autónomo grupal	
Laboratorios (L)	8		
Prácticas externas, clínicas o de campo			
Presentación Trabajos	4		
Tutorías grupales o individuales	4		
Evaluación (fuera del periodo oficial de exámenes)	2		
Total presencial	30	Total no presencial	45



5. Programa

Carga de trabajo en créditos ECTS:

a. Contextualización y justificación

Ver Punto 1.

b. Objetivos de aprendizaje

Ver tabla apartado 3.

c. Contenidos

TEMA 1: Conceptos y métodos de la Criptografía. Protocolos criptográficos. Criptografía de clave privada y de clave pública.

TEMA 2: Principales esquemas criptográficos de clave pública.

TEMA 3: Protocolos de acuerdo y transporte de claves.

TEMA 4: Protocolos de autenticación.

TEMA 5: Protocolos de firma digital.

TEMA 6: Computación multipartita. Esquemas de reparto de secretos.

TEMA 7: Otros Protocolos: elecciones electrónicas, comercio electrónico, etc.

d. Métodos docentes

- Clase magistral participativa
- Implementación en laboratorio de algunos protocolos
- Resolución de problemas
- Aprendizaje colaborativo
- Preparación y presentación de trabajos

e. Plan de trabajo

Se combinarán las clases teórico-prácticas con la implementación en laboratorio de alguno de los esquemas y protocolos estudiados. Se realizará un examen/control aproximadamente en la quinta semana del curso. Asimismo los alumnos en grupos de dos o tres prepararán y expondrán públicamente (en las últimas clases del curso) un tema complementario a los desarrollados en clase.

f. Evaluación

Ver punto 7.



g. Bibliografía básica

- J. A. Buchmann, *Introduction to Cryptography*, Second Edition, Springer, 2001, ISBN 0-387-21156-X
- A. J. Menezes; P. C. van Oorschot, S. A. Vanstone, *Applied Cryptography*, CRC Press, 1997, ISBN 0-8493-8523-7

h. Bibliografía complementaria

- J. Gutierrez; J. Tena (Eds), *Protocolos Criptográficos y Seguridad en Redes*, Servicio de Publicaciones de la Universidad de Cantabria, 2003, ISBN 84-8102-345-0
- B. Schneider, *Applied Cryptography*, John Wiley, Second Edition, 1996, ISBN 0-471-11709-7
- W. Stalling, *Network and Internetwork Security*, IEEE Press, 1995, 0-02-415483-0
- J. R. Ramio, *Seguridad Informática y Criptografía*, 2006, Edición electrónica, Criptored <http://www.criptored.upm.es>

7. Sistema de calificaciones – Tabla resumen

INSTRUMENTO/PROCEDIMIENTO	PESO EN LA NOTA FINAL	OBSERVACIONES
Examen Final escrito (versara sobre los conceptos fundamentales del curso y su aplicación a un caso concreto)	50%	Periodo de Exámenes
Prácticas de Laboratorio	20%	Horario a establecer
Presentación y entrega de trabajos	15%	Entrega anterior al examen
Examen/control	15%	

CRITERIOS DE CALIFICACIÓN

- **Convocatoria ordinaria:**
La ponderación será la establecida en la tabla anterior. Será necesaria la obtención de una nota igual o superior a dos puntos (sobre 10) en el examen final.
- **Convocatoria extraordinaria:**
Se tomara la opción más favorable entre: la establecida para la convocatoria ordinaria y la nota obtenida en el examen escrito correspondiente a esta convocatoria.