

DATOS BÁSICOS DE LA GUÍA DOCENTE:

Materia:	CRIPTOGRAFIA		
Identificador:	30082		
Titulación:	GRADUADO EN INGENIERÍA INFORMÁTICA. PLAN 2008 (BOE 15/12/2008)		
Módulo:	GESTION DE LA INFORMACION Y EL CONOCIMIENTO		
Tipo:	OPTATIVA		
Curso:	4	Periodo lectivo:	Primer Cuatrimestre
Créditos:	3	Horas totales:	75
Actividades Presenciales:	36	Trabajo Autónomo:	39
Idioma Principal:	Inglés	Idioma Secundario:	Inglés
Profesor:	BALLARIN USIETO, PABLO (T)	Correo electrónico:	pballarinu@usj.es

PRESENTACIÓN:

Perspectiva histórica. Algoritmos criptográficos. Criptografía de clave privada. Criptografía de clave pública. Firma digital. Protocolos de seguridad. Otras aplicaciones de la criptografía.

COMPETENCIAS PROFESIONALES A DESARROLLAR EN LA MATERIA:

Competencias Generales de la titulación	G02	Capacidad innovadora para proponer y encontrar formas nuevas y eficaces de realizar cualquier tarea y/ o función dentro de su entorno profesional con una elevada motivación por la calidad
	G03	Capacidad para trabajar dentro de equipos multidisciplinares para conseguir metas comunes, anteponiendo los intereses colectivos a los personales
	G10	Capacidad crítica y analítica en la evaluación de información, datos y líneas de actuación
	G12	Capacidad para desarrollar las actividades profesionales con integridad respetando normas sociales, organizacionales y éticas
	G13	Capacidad para utilizar estrategias de aprendizaje individuales orientadas a la mejora continua en el ejercicio profesional y para emprender estudios posteriores de forma autónoma
	G14	Capacidad de abstracción para manejar diferentes modelos complejos de conocimiento y aplicarlos al planteamiento y resolución de problemas
	G15	Capacidad para estructurar la realidad relacionando objetos, situaciones y conceptos a través del razonamiento lógico matemático
Competencias Específicas de la titulación	E01	Capacidad para comprender la profesión de la ingeniería y compromiso para servir a la sociedad de acuerdo al código de conducta profesional correspondiente
	E02	Capacidad para aplicar los principios intrínsecos de la ingeniería basados en las matemáticas y en una combinación de disciplinas científicas
	E03	Capacidad para reconocer los principios teóricos y aplicar satisfactoriamente los métodos prácticos apropiados para el análisis y la resolución de problemas de ingeniería
	E08	Capacidad para comunicarse productivamente con clientes, usuarios y colegas, tanto de modo oral como por escrito, con el fin de transmitir ideas, resolver conflictos y alcanzar consensos
	E10	Capacidad para comprender y evaluar el impacto de la tecnología en los individuos, las organizaciones, la sociedad y el medioambiente, incluyendo aspectos éticos, legales y políticos, reconociendo y aplicando los estándares y regulaciones oportunos
	E12	Capacidad para gestionar la complejidad a través de la abstracción, el modelado, las "best practices", los patrones, los estándares y el uso de herramientas apropiadas
	E13	Capacidad para identificar, evaluar y usar tecnologías actuales y emergentes, considerando su aplicabilidad en función de las necesidades de individuos y organizaciones
Resultados de Aprendizaje	E17	Capacidad para identificar y analizar las necesidades de los usuarios con el objetivo de diseñar soluciones IT efectivas y usables que puedan integrarse en el entorno operativo del usuario.
	R01	Evaluar las fortalezas y debilidades de seguridad de diferentes aplicaciones a través de distintos métodos criptográficos
	R02	Implementar un algoritmo criptográfico completo.
	R03	Entender los conceptos matemáticos sobre los que se apoyan los distintos métodos criptográficos
	R04	Distinguir y utilizar los conceptos principales de la criptografía.
R05	Comparar las diferentes herramientas criptográficas	

R06 Conocer los diferentes problemas de seguridad de la sociedad de la información

PROGRAMACIÓN DE LA MATERIA:

Contenidos de la materia:

BIBLIOGRAFÍA Y DOCUMENTACIÓN:

Bibliografía recomendada:

Bibliografía básica:

Páginas web recomendadas: