Resumen

DESCRIPCIÓN GENERAL DE LA ASIGNATURA

Los objetivos de esta asignatura se centran en entender el funcionamiento tanto de los sistemas criptográficos simétricos o de clave secreta, como de los asimétricos o de clave pública, así como de distintos esquemas de firma digital, con el objetivo de ser utilizados como mecanismos de seguridad para proveer servicios criptográficos. Asimismo, se estudian distintos protocolos y aplicaciones criptográficas que se emplean en la actualidad y previsiblemente en el futuro.

OBJETIVOS, COMPETENCIAS Y DESTREZAS

CONOCIMIENTOS RECOMENDADOS

Previos

Titulación	Asignatura
MÁSTER UNIVERSITARIO EN TECNOLOGÍAS, SISTEMAS Y REDES DE COMUNICACIONES	(31069) COMUNICACIÓN DE DATOS

SELECCIÓN Y ESTRUCTACIÓN LAS UNIDADES DIDÁCTICAS

1. Introducción
    1. Introducción a la Criptografía
2. Criptografía simétrica o de clave secreta
    1. Criptografía simétrica o de clave secreta
3. Criptografía asimétrica o de clave pública
    1. Criptografía asimétrica o de clave pública
4. Firmas digitales
    1. Firmas digitales
5. Protocolos y aplicaciones criptográficas
    1. Protocolos y aplicaciones criptográficas

DISTRIBUCIÓN DE LAS UNIDADES DIDÁCTICAS

Unidad didáctica	Trab. Presencial	Trab.no Presencial
Introducción	2,00	3,00
Criptografía simétrica o de clave secreta	8,00	12,00
Criptografía asimétrica o de clave pública	8,00	12,00
Firmas digitales	4,00	6,00
Protocolos y aplicaciones criptográficas	8,00	12,00
Total:	**30,00**	**45,00**

METODOLOGIA DE ENSEÑANZA-APRENDIZAJE

Autónomas

Nombre	Descripción	Horas
Trabajos prácticos	Preparación de actividades para exponer o entregar en las clases prácticas.	15
Estudio teórico	Estudio de contenidos relacionados con las "clases teóricas": Incluye cualquier actividad de estudio que no se haya computado en el apartado anterior (estudiar exámenes, trabajo en biblioteca, lecturas complementarias, hacer problemas y ejercicios, etc.).	20
Estudio práctico	Relacionado con las "clases prácticas".	10
	Total:	**45,00**

METODOLOGIA DE ENSEÑANZA-APRENDIZAJE

Presenciales

Nombre	Descripción	Horas
Acrividades de evaluación	Conjunto de pruebas escritas, orales, prácticas, proyectos, trabajos, etc. utilizados en la evaluación del progreso del estudiante.	1
Clase magistral	Exposición de contenidos mediante presentación o explicación por parte de un profesor (posiblemente incluyendo demostraciones).	29
	Total:	**30,00**

EVALUACIÓN

Nombre	Descripción
Pruebas objetivas (tipo test)	Examen escrito estructurado con diversas preguntas o ítems en los que el alumno no elabora la respuesta; sólo ha de señalarla o completarla con elementos muy precisos.

RECURSOS

apuntes
copia de las transparencias
exámenes resueltos
laboratorio (especificar tipo en observaciones)
materiales multimedia
pizarra
software informático(especificar en observaciones)
transparencias

Laboratorio: PC. Software: Java

BIBLIOGRAFÍA

· *Fundamentos de seguridad en redes : aplicaciones y stándares (Stallings, William)*
· *Criptografía digital : fundamentos y aplicaciones (Pastor Franco, José)*
· *Handbook of applied criptography (Menezes, Alfred J.)*
· *A course in number theory and cryptography (Koblitz, Neal)*
· *Applied criptography : protocols, algorithms, and source code in C (Schneier, Bruce)*