



Curso 2011-2012

CENTROS

Planes Estudio

PLANES

ASIGNATURAS

v. 2.11

Criptografía y seguridad en comunicaciones

CÓDIGO:18186

 Ingeniero de Telecomunicación (en extinción)
 Escuela de Ingeniería y Arquitectura, Zaragoza

Departamentos:
 Ingeniería Electrónica y Comunicaciones

Áreas:
 Ingeniería Telemática

Curso: 5
Duración: 2º cuatrimestre
Carácter: Optativa
Tipo: Teórica Práctica
Idioma: Español

Horas teóricas: 3
Horas prácticas: 15
Créditos UZ: 6
Créditos ECTS: 4,9

 Oferta de plazas de libre elección:
Propia Titulación:
Otras Titulaciones: S/L
y/u:
Otros Centros: S/L
Nº Plazas optativas: S/L

Objetivos y Programa

Profesores y Bibliografía

Horario / Observaciones

Objetivos

El objetivo principal de la asignatura es plantear una visión general de la Criptografía, y de la Seguridad en redes, todo ello desde un punto de vista eminentemente práctico y aplicado a las necesidades reales.

Programa

La parte de Criptografía cubre todos los tipos de criptografía y algoritmos modernos, pasando a continuación a las aplicaciones de dichos algoritmos y protocolos.

La parte de Seguridad intenta dar una perspectiva descriptiva (aunque se profundice en algunos aspectos) de todos los temas importantes de la seguridad de redes de comunicaciones.

Teoría - Criptografía

- " Tema 1: Introducción a la Criptografía
- " Tema 2: Cifrado en flujo
- " Tema 3: Criptografía de clave secreta
- " Tema 4: Criptografía de clave pública
- " Tema 5: Funciones HASH y firmas digitales
- " Tema 6: Certificados digitales y PKI
- " Tema 7: Esteganografía - Marcas de agua
- " Tema 8: Sistemas de voto electrónico
- " Tema 9: Protocolos y aplicaciones de la criptografía
- " Tema 10 : Ejercicios y dudas

Teoría - Seguridad en Redes

- " Tema 1 : Conceptos básicos de seguridad (2h)
- " Tema 2 : Seguridad en Sistemas Operativos (2h)
- " Tema 3 : Sistemas Redundantes (1h)
- " Tema 4 : Virus & Malware (1h)
- " Tema 5 : Seguridad de equipos de comunicaciones(1h)
- " Tema 6 : Seguridad de servicios internet (1h)
- " Tema 7 : SPAM (1h)
- " Tema 8 : Seguridad de redes WLAN (1h)
- " Tema 9 : Protocolos de Seguridad en redes de comunicaciones (1h)
- " Tema 10 : Cortafuegos y Seguridad perimetral (1h)
- " Tema 11 : Sistemas de detección y prevención de intrusos (1h)
- " Tema 12 : Programación segura (1h)
- " Tema 13 : Seguridad en aplicaciones web (1h)
- " Tema 14 : Auditorias de Seguridad y Peritajes (1h)
- " Tema 15 : Delitos informáticos e Informática Forense (1h)
- " Tema 16 : Respuesta ante incidentes de seguridad (1h)
- " Tema 17 : Gestión de la Seguridad : SGSI (2h)
- " Tema 18 : LOPD : SGSI (1h)
- " Tema 19 : Ejercicios (2h)

Prácticas

- " Práctica 1 : Correo seguro mediante GPG + Thunderbird
- " Práctica 2 : Infraestructuras de clave pública con OpenSSL
- " Práctica 3 : Seguridad de Sistemas Operativos: Windows XP y Fedora Linux
- " Práctica 4 : Análisis de Seguridad de Redes: LCP, nmap, Nessus, WireShark
- " Práctica 5 : Seguridad web: Inyección SQL, XSS y mod_security
- " Práctica 6 : Cortafuegos : Outpost Firewall + iptables

Evaluación

La nota de la asignatura dependerá tanto de un examen (80%) como del proyecto de comercio electrónico desarrollado a lo largo de la misma (20%). Será condición necesaria el obtener una nota mínima de 4.0 en las dos partes para que se realice el promedio final.

Nota importante : Es imprescindible entregar el informe de las prácticas como muy tarde el mismo día del examen de la

convocatoria en la que se pretenda aprobar la asignatura.

