UNIVERSIDAD DE LAS PALMAS DE GRAN CANARIA

GUÍA DOCENTE *CURSO: 2009/10*

14116 - PROTOCOLOS Y SERVICIOS

ASIGNATURA: *14116 - PROTOCOLOS Y SERVICIOS*
CENTRO: *Escuela de Ingeniería de Telecomunicación y Electrónica*
TITULACIÓN: *Ingeniero de Telecomunicación*
DEPARTAMENTO: *INGENIERÍA TELEMÁTICA*
ÁREA: *Ingeniería Telemática*
PLAN: *13 - Año 200* **ESPECIALIDAD:**
CURSO: *Quinto curso* **IMPARTIDA:** *Primer semestre* **TIPO:** *Troncal*
CRÉDITOS: *6* **TEÓRICOS:** *3* **PRÁCTICOS:** *3*

Información ECTS

Créditos ECTS:4,8
Horas presenciales: 60,0
- Horas teóricas (HT): 27,0
- Horas prácticas (HP): 22,5
- Horas de clases tutorizadas (HCT): 12,0
- Horas de evaluación: 1,5
- otras: 0,0

Horas no presenciales: 60,0
- trabajos tutorizados (HTT): 30,0
- actividad independiente (HAI): 30,0

Idioma en que se imparte: Español

Horas de trabajo del alumno: 121,5

Descriptores B.O.E.

Planificación y gestión de redes y servicios. Normalización y política de telecomunicaciones. Codificación y cifrado de información.

Temario

PROGRAMA TEÓRICO:

Tema 1. Presentación de la asignatura (2 horas)
- 1.1. Proyecto docente.
- 1.3. Introducción los bloques temáticos
- 1.2. Herramientas utilizadas
- 1.3. Creación de grupos de trabajo

Tema 2. Gestión de red (8 horas)
- 2.1. Conceptos de gestión de red (1 hora)
- 2.2. ASN.1 (1 hora)
- 2.3. SMI y MIB II (2 horas)
- 2.2. SNMP (2 horas)
- 2.4. CMIP y TMN (2 horas)

Tema 3: Seguridad de Red (12 horas)
2.1. Conceptos de seguridad (2 horas)
2.2. Algoritmos y protocolos (6 horas)
2.3. Seguridad en Internet (4 horas)

Tema 4: Política de Telecomunicaciones (8 horas)
3.1. Política de Telecomunicaciones en Europa (2 horas)
3.2. Proceso de la Liberalización de las Telecomunicaciones (2 horas)
3.3. Política de Telecomunicaciones en España(4 horas)

Objetivos

1.Objetivos conceptuales:
1.1.Introducir conceptos, herramientas y procedimientos utilizados en la asignatura.
1.2.Conocer los conceptos básicos de la gestión de red.
1.3.Conocer y comprender diversas herramientas para gestionar la MIB.
1.4.Saber y conocer el protocolo de gestión de red SNMP.
1.5.Saber y comprender los aspectos matemáticos básicos asociados a la criptografía.
1.6.Conocer los principales algoritmos de cifrado por sustitución.
1.7.Saber y comprender los principales cifradores clásicos existentes.
1.8.Conocer y analizar el cifrado simétrico y asimétrico.
1.9.Conocer y comprender los aspectos principales de la firma digital y la gestión de claves.
1.10.Conocer la política de las telecomunicaciones en Europa.
1.11.Analizar el proceso de liberalización de las Telecomunicaciones en España.
1.12.Conocer la política de las telecomunicaciones en España.

2.Objetivos procedimentales:
2.1.Experimentar con las herramientas de laboratorio.
2.2.Manejar y elaborar diferentes configuraciones del servidor SNMP.
2.3.Utilizar aplicaciones gráficas para gestionar la MIB.
2.4.Ejecutar aplicaciones de consola para comunicación entre cliente y servidor SNMP.
2.5.Aplicar los conceptos matemáticos básicos asociados con la criptografía y manejar aplicaciones que permiten realizar estos cálculos.
2.6.Manejar los principales algoritmos de sustitución y ejecutar aplicaciones que permiten aplicar estos algoritmos.
2.7.Utilizar los principales cifradores clásicos y probar aplicaciones que los usan.
2.8.Manejar algoritmos de cifrado simétrico y asimétrico y ejecutar aplicaciones que permiten aplicar estos algoritmos.
2.9.Ejecutar aplicaciones que permiten la firma digital y la gestión de claves.
2.10.Aplicar las leyes de Telecomunicación a diferentes supuestos.

3.Objetivos actitudinales
3.1.Interesarse por los objetivos que se quieren cubrir.
3.2.Valorar la importancia de una buena gestión de red.
3.3.Apreciar que la seguridad es fundamental en la Sociedad de la Información.
3.4.Respectar el marco legal por el que se rigen las Telecomunicaciones.

Metodología

La asignatura consta de dos partes claramente diferenciadas: teoría y prácticas de laboratorio.
TEORÍA
La teoría se desarrollara combinando las clases de teoría con ejercicios escritos, prácticos y de exposición por parte del alumno.

* Clases de teoría:
-Actividad del profesor: Clases expositivas combinadas con la presentación de casos de uso. Se combinará el uso de presentaciones y documentos en vídeo en el cañón, y el uso de la pizarra, todo en el aula.
- Actividad del estudiante:
o Presencial: Tomar apuntes, participar en clase planteando dudas, hacer presentaciones e intervenir en debates sobre las presentaciones de los compañeros.
o No presencial: Preparar apuntes, estudiar la materia, recopilar información sobre los trabajos asignados y preparar las presentaciones de estos trabajos.

PRACTICAS DE LABORATORIO
-Actividad del profesor: Asesorar al alumno para que el alumno realice todos los pasos de la práctica.
-Actividad de los alumnos:
o No presencial: Recopilar información sobre la práctica y desarrollar la estratégia de trabajo que va a seguir en el laboratorio.
o Presencial: Realizar todos los paso de la práctica, responder a las preguntas del profesor sobre el trabajo realizado y hacer una memoria con las respuestas.

Criterios de Evaluación

Actividades que liberan materia:
- Sólo en la convocatoria ordinaria de este curso académico, prueba objetiva al final del tema 2 que puntúa el 15% de la nota final de la asignatura.
- Sólo en la convocatoria ordinaria de este curso académico, prueba objetiva al final del tema 3 que puntúa el 20% de la nota final de la asignatura.
- Sólo en la convocatoria ordinaria de este curso académico, prueba objetiva al final del tema 4 que puntúa el 15% de la nota final de la asignatura.
- Realización de las 2 prácticas, que libera un 20% de la nota final de la asignatura.
- Análisis, exposición y defensa en clase de un trabajo de teoría relacionado con el temario de la asignatura, que libera un 10%.
- Sólo en la convocatoria ordinaria de este curso académico, los alumnos que hagan y aprueben el trabajo de teoría y asistan al menos al 80% de las exposiciones de los trabajos de los compañeros liberan el 20%.

Actividades que no liberan materia:
- Trabajo práctico de gestión de red (1 punto)
- Trabajo práctico de seguridad de red (1 punto)
- Trabajo práctico de política de Telecomunicación (1 punto)

Otras consideraciones:
- La asignatura se puede aprobar mediante evaluación continua: teoría (pruebas objetivas y asistencia a exposiciones de trabajos), trabajo de teoría y prácticas.
- La parte de teoría está formada por la materia explicada por el profesor (50% de la nota final de la asignatura) y la materia de los trabajos de teoría que los alumnos presentan los alumnos (20% de la nota final de la asignatura).
- Los alumnos que hagan y aprueben el trabajo de teoría y asistan al menos al 80% de las exposiciones de los trabajos de los compañeros obtinen los dos puntos asociados a las preguntas que sobre trabajos hay en el examen de teoría de la convocatoria ordinaria de este curso académico (es decir, no tienen que responder a las preguntas del apartado asociado a trabajos de teoría).
- La práctica 1 puntúa con el 40% de la nota final de prácticas.
- La práctica 2 puntúa con el 60% de la nota final de prácticas.
- Para aprobar las pruebas objetivas de teoría es necesario sacar al menos 50% de la nota la prueba

objetiva.
- Para aprobar las prácticas es necesario sacar al menos el 50% de la nota de prácticas.
- Para aprobar el trabajo de teoría es necesario sacar al menos el 50% de la nota del trabajo.
- Para aprobar la asignatura es necesario aprobar las tres partes en que se divide la asignatura: parte de teoría, parte de trabajo de teoría y parte de prácticas.
- Los exámenes de convocatoria son para recuperar cualquiera de las partes de la asignatura: la parte de teoría, la parte de trabajo de teoría o la parte de práctica.
- Cuando un alumno se presenta al examen de convocatoria ordinaria, renuncia a la nota obtenida en la evaluación continua de las partes a las que se presente (teoría, trabajo o práctica).
- Cuando un alumno se presenta a un examen de convocatoria no ordinaria, debe hacer siempre la parte de teoría y si se presenta a otra parte renuncia a la nota obtenida en la evaluación continua de esa parte (trabajo o práctica).
- El alumno debe superar el 50% de la nota final para aprobar la asignatura.

Descripción de las Prácticas

Las prácticas serán realizadas en el Laboratorio de Redes de Área Local, Extensa y RDSI del Departamento de Ingeniería Telemática.

Práctica 1: Gestión de Red con SNMP

1.1 Introducción a SNMP.
Duración: 2 horas
En esta práctica se pretende dar una visión general sobre la gestión de red con SNMP. Para ello, vamos a tomar el primer contacto con el entorno de trabajo y con el agente SNMP. En este último caso, veremos algunos aspectos básicos de su configuración así como la manera que tenemos para interactuar con él.

1.2 Cómo configurar y usar SNMP.
Duración: 4 horas
En esta práctica se pretende profundizar en la configuración del agente SNMP. También, profundizaremos en la manera que tenemos para interactuar con él incluyendo la posibilidad de modificar valores de la MIB.

1.3 Cliente y servidor SNMP.
Duración: 4 horas
En esta práctica se aplicar las opciones no vistan aún en la configuración del agente SNMP. También, profundizaremos en la manera que tenemos para interactuar con él desde otros ordenadores de la red.

1.4 Traps y MIB Browser.
Duración: 2 horas
En esta práctica vamos a configurar el agente SNMP para permitir el envío y recepción de traps (notificaciones).

Práctica 2: Seguridad en Redes

2.1 Fundamentos Teóricos de la critografía
Duración: 2 horas
Esta práctica tiene como objetivo comprobar la entropía de los mensajes y de las claves, así como estudiar y comprobar el comportamiento característico del lenguaje y su redundancia, aspectos que permitirán el criptoanálisis de sistemas de cifra clásicos.

2.2 Cifradores por sustitución monográfica monoalfabeto
Duración: 2 horas
En esta práctica veremos los cifradores por sustitución monográmica monoalfabeto donde el cifrado se realiza mediante un algoritmo que hace corresponder una letra del texto en claro a una única letra del criptograma, es decir, cifra monogramas.

2.3 Cifra por sustitución polialfabética monográfica
Duración: 2 horas
En esta práctica utilizaremos los algoritmos de sustitución polialfabética que tienen por objeto producir una distribución plana de la frecuencia relativa de los caracteres en el criptograma. Para ello utilizan sustituciones múltiples de forma que en un texto largo se combinan las altas frecuencias de algunos caracteres con otros de menor frecuencia. La técnica anterior consiste en aplicar dos o más alfabetos de cifrado de forma que cada uno de ellos sirva para cifrar los caracteres del texto en claro, dependiendo de la posición
relativa de éstos en dicho texto.

2.4 Cifradores clásicos
Duración: 4 horas
En esta práctica veremos otro método clásico utilizado para cifrar mensajes: la transposición o permutación de caracteres. Esto consiste en reordenar los caracteres del texto. El resultado de tal acción es la de difuminar la información del texto en claro y provocar, por tanto, la difusión propuesta por Shannon para la protección de la misma.

2.5 Cifrado asimétrico por bloques y asimétrico
Duración: 4 horas
Este tipo de cifradores utiliza una única clave que debe guardarse en secreto ya que en ella reside la seguridad de los mismos. Por esta razón se les denomina también simétricos puesto que usan la misma clave para cifrar en emisión y descifrar en recepción. Los cifradores de exponenciación que usan el problema matemático de la factorización de números grandes basan su seguridad en que, para el propietario del par de claves asiméticas es fácil deducir la clave privada de la clave pública.

2.6 Funciones resumen y gestión de claves
Duración: 4 horas
Las funciones hash, tienen su principal aplicación en los sistemas de cifra actuales generalmente bajo dos términos: como parte principal de algoritmos de autenticación o como funciones resumen para reducir el tamaño de un bloque de texto en claro a un valor constante de sólo unas centenas de bits y con ello permitir la firma digital.

Bibliografía

[1 Básico] Computer networks /
Andrew S. Tanenbaum.
Prentice Hall,, Englewood Cliffs (New Jersey) : (2003) - (4th. ed.)
0130384887

[2 Básico] Applied cryptography: protocols,algorithms and source code in C.
Schneier, Bruce
John Wiley & Sons,, Chichester : (1996) - (2nd. ed.)
0471117099

[3 Básico] Política de Telecomunicaciones en la Unión Europea.
Ministerio de Obras Públicas, Transportes y Medio Ambiente,, Madrid : (1995)
844980146X

[4 Recomendado] Handbook of applied cryptography /

Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone.
CRC,, Boca Ratón [etc.] : (1996)
0-8493-8523-7

[5 Recomendado] Protocolos criptográficos y seguridad en redes /

Jaime Gutiérrez, Juan Tena, (eds).
Servicio de Publicaciones de la Universidad de Cantabria,, Santander : (2003)
84-8102-345-0

[6 Recomendado] Normalización y política de las telecomunicaciones /

José Andrés
Vázquez Travieso ; Gustavo Rodríguez Rodríguez, dir.
Escuela Universitaria de Ingeniería
Técnica de Telecomunicación,, Las Palmas de Gran Canaria : (2000)

[7 Recomendado] Gestión de red, SNMP /

José María Quinteiro González ; Gustavo Rodríguez Rodríguez.
Universidad de Las Palmas de Gran Canaria,, Las Palmas de Gran Canaria : (1997)

[8 Recomendado] SNMP, SNMPv2, and CMIP: the practical guide to network management standards /

William Stallings.
Addison-Wesley,, Reading, Mass. : (1993)
0201633310

Organización Docente de la Asignatura

	Horas					
Contenidos	HT	HP	HCT	HTT	HAI	Competencias y Objetivos
Tema 1. Práctica 1.1.	2,0	1,5	0,5	2,0	1,5	1.1, 2.1 y 3.1
Tema 2. Prácticas 1.2 y 1.3. Prueba objetiva de teoría.	7,0	6,0	3,0	8,0	8,5	1.2, 1.3, 1.4, 2.2, 2.3, 2.4 y 3.2
Tema 3. Prácticas 1.4, 2.1, 2.2, 2.3 y 2.4. Prueba objetiva de teoría.	11,0	9,0	4,0	10,0	12,0	1.5, 1.6, 1.7, 1.8, 1.9, 2.5, 2.6, 2.7, 2.8, 2.9, 3.3
Tema 4. Prácticas 2.5 y 2.6. Prueba objetiva de teoría.	7,0	6,0	3,0	8,0	8,0	1.10, 1.11, 1.12, 2.10 y 3.4

Equipo Docente

FRANCISCO JOSÉ GUERRA SANTANA *(COORDINADOR)*
Categoría: *TITULAR DE UNIVERSIDAD*
Departamento: *INGENIERÍA TELEMÁTICA*
Teléfono: *928451238* **Correo Electrónico:** *francisco.guerra@ulpgc.es*
WEB Personal: *http://www.dit.ulpgc.es/usuarios/profes/fguerra/index.html*

LUIS MIGUEL HERNÁNDEZ ACOSTA *(RESPONSABLE DE PRACTICAS)*
Categoría: *PROFESOR CONTRATADO DOCTOR, TIPO 1*
Departamento: *INGENIERÍA TELEMÁTICA*
Teléfono: *928451383* **Correo Electrónico:** *luismiguel.hernandez@ulpgc.es*
WEB Personal: *http://www.dit.ulpgc.es/usuarios/profes/lhdez/index.html*

Resumen en Inglés

DESCRIPTOR:
Network Management. Applied Criptography. Telcommunications Policies.

GOALS
- Study Network Management.
- Apply Criptography Algorithm.
- Analyze Telcommunications Policies in Europe Specially Spanish Policies.

METHODOLOGY
- The instructor presents in class the main concepts
- The instructor proposes exercises that help the students to understand the concepts presented in class
- In the laboratory the students will program complementary exercies
- The electronic documents containing complementary material will be available in the Campus Virtual server of the ULPGC.