Universidad Carlos III de Madrid
www.uc3m.es

DENOMINACIÓN ASIGNATURA: Fundamentos de Seguridad en Comunicaciones		
GRADO: Grado en Ingeniería de Tecnologías de Telecomunicación	CURSO: 4º	CUATRIMESTRE: 1º

La asignatura tiene 29 sesiones que se distribuyen a lo largo de 14 semanas. Los laboratorios pueden situarse en cualquiera de estas ellas. Semanalmente el alumnos tendrá dos sesiones, excepto en un caso que serán tres.

PLANIFICACIÓN SEMANAL DE LA ASIGNATURA

SEMANA	SESIÓN	DESCRIPCIÓN DEL CONTENIDO DE LA SESIÓN	GRUPO (marcar X)		Indicar espacio distinto de aula (aula informática, audiovisual, etc.)	Indicar SI/NO es una sesión con 2 profesores	TRABAJO SEMANAL DEL ALUMNO		
			GRANDE	PEQUEÑO			DESCRIPCIÓN	HORAS PRESENCIALES	HORAS TRABAJO (Max. 7h semana)
1	1	Introducción a la asignatura e introducción a la seguridad en red	X				Principales conceptos. Seguridad informática y seguridad en redes. Ataques informáticos: tipos y medidas de defensa. Servicios criptográficos y técnicas para la protección de la información.	1,66	
1	2	Cifrado simétrico – cifrado clásico		X			Principales técnicas para el cifrado de la información usadas a lo largo de la historia pre-computacional. Análisis y criptoanálisis de sistemas.	1,66	7
2	3	Cifrado simétrico – cifrado clásico	X				Principales técnicas para el cifrado de la información usadas a lo largo de la historia	1,66	7

							pre-computacional. Análisis y criptoanálisis de sistemas.		
2	4	Ejercicios prácticos		X			Ejercicios prácticos	1,66	
3	5	Cifrado simétrico – algoritmos de cifrado modernos	X				Principales técnicas para el cifrado de la información moderna (DES, AES). Análisis y criptoanálisis de sistemas.	1,66	
3	6	Ejercicios prácticos		X			Ejercicios prácticos	1,66	7
4	7	Cifrado simétrico – algoritmos de cifrado modernos	X				Principales técnicas para el cifrado de la información moderna (DES, AES). Análisis y criptoanálisis de sistemas.	1,66	
4	8	Ejercicios prácticos		X			Ejercicios prácticos	1,66	7
5	9	Cifrado simétrico – modos de operación	X				Mecanismos para el cifrado de cadenas de longitud arbitraria mediante técnicas de concatenación de cifradores en bloque.	1,66	
5	10	Laboratorio 1 - cifrado		X	Aula informática 4.1.B01 o 4.1.B02	SI	Laboratorio	1,66	7
6	11	Cifrado simétrico – Distribución de claves	X				Mecanismos para el intercambio de claves de sesión y generación de claves de sesión a partir de claves maestras.	1,66	
6	12	Laboratorio 2 – modos de operación		X	Aula informática 4.1.B01 o 4.1.B02	SI	Laboratorio	1,66	7
7	13	Cifrado asimétrico – Base matemática previa e introducción a RSA	X				Base de la matemática discreta. Aritmética modular. Exponenciación rápida. Base matemática de RSA.	1,66	
7	14	Ejercicios prácticos		X			Ejercicios prácticos	1,66	7
8	15	Cifrado asimétrico – Algoritmos, curvas elípticas	X				Algoritmo de ElGamal. Cuerpos de Galois. Concepto y usos de las curvas elípticas y uso en criptografía.	1,66	
8	16	Ejercicios prácticos		X			Ejercicios prácticos	1,66	7
9	17	Funciones de hash	X				Generación de huellas digitales. Propiedades y técnicas. Principales funciones de hash.		
9	18	Ejercicios prácticos		X			Ejercicios prácticos	1,66	7

10	19	Firma digital	X				Concepto, formatos y algorítmica para la generación y validación de firmas digitales.	1,66	
10	20	Ejercicios prácticos		X			Ejercicios prácticos	1,66	7
11	21	Certificados de identidad, Certificados de atributos y distribución de claves usando criptografía asimétrica	X				Comprensión de los formatos, propiedades y mecanismos criptográficos para la generación de certificados digitales, tanto de identidad (autenticación) como de atributos (autorización).	1,66	
11	22	Ejercicios prácticos		X			Ejercicios prácticos	1,66	7
12	23	IPSEC	X				Aplicación de las técnicas criptográficas para comprender el funcionamiento y la seguridad aportada por IPSEC. Negociación. Distribución de claves maestras. Generación de claves de sesión. Cifrado de datos. Generación de huellas digitales.	1,66	
12	24	Ejercicios prácticos		X			Ejercicios prácticos	1,66	7
13	25	SSL	X				Aplicación de las técnicas criptográficas para comprender el funcionamiento y la seguridad aportada por SSL. Negociación. Distribución de claves maestras. Generación de claves de sesión. Cifrado de datos. Generación de huellas digitales.	1,66	
13	26	Ejercicios prácticos		X			Ejercicios prácticos	1,66	7
14	27	Laboratorio 3 – Open SSL y criptografía asimétrica		X	Aula informática 4.1.B01 o 4.1.B02	SI	Laboratorio	1,66	
14	28	Laboratorio 4 – PGP y seguridad en red (IPSEC)		X	Aula informática 4.1.B01 o 4.1.B02	SI	Laboratorio	1,66	7
	29	Ejercicios prácticos		X			Ejercicios prácticos	1,66	
							Subtotal 1	**48**	**98**
		Total 1 *(Horas presenciales y de trabajo del alumno entre las semanas 1-14)*						146	
15		Recuperaciones, tutorías, entrega de trabajos, etc						10	
16		Preparación de evaluación y evaluación						24	

17									
18									
							Subtotal 2	**34**	
						Total 2 *(Horas presenciales y de trabajo del alumno entre las semanas 15-18)*			
TOTAL *(Total 1 + Total 2. <u>Máximo 180 horas</u>)*								**180**	