Universidad Carlos III de Madrid
www.uc3m.es

Subject Name: Basis for secure communication		
Study: Bachelor in Telecommunication Technology Engineering	**COURSE: 4**	**SEMESTER: 1º**

The course has 29 sessions distributed over 14 weeks. Laboratories can be located in any of these.
Weekly students will have two sessions, except in one case that will be three.

PLANIFICACIÓN SEMANAL DE LA ASIGNATURA

WEEK	SESSION	CONTENT DESCRIPTION	GROUP		ROOM	2 INSTRUCTORS	STUDENTS' WORKING LOAD AND CONTENT SPECIFICATION		
			"MAGISTRAL"	REDUCED			DESCRIPTION	CLASS HOURS	PERSONAL WORK HOURS
1	1	Topic 1: Introduction to the course. Topic 2: Introduction to network security	X				Main concepts. Information security and Network security. Cyberattacks and countermeasures.Cryptographic services and techniques for information protection.	1,66	
1	2	Introduction to network security		X			Exercises	1,66	7
2	3	Topic 3: Information Theory	X				Information Theory. Entropy. Unicity Distance	1,66	
2	4	Information Theory		X			Exercises	1,66	7
3	5	Topic 4: Classical Ciphers	X				Historical cryptographic techniques used for encryption. Cryptoanalysis.	1,66	7

3	6	Classical Ciphers		X			Exercises	1,66	
4	7	Topic 5: Symmetric Encryption –modern encryption algorithms	X				Modern encryption algorithms (DES, AES). Cryptoanalysis	1,66	
4	8	Symmetric Encryption		X			Exercises	1,66	7
5	9	Topic 6: symmetric Encryption – Modes of operation	X				Mechanisms for the encryption of chains of arbitrary length by techniques of concatenation of block ciphers.	1,66	
5	10	Lab 1 - Encryption		X	Computer room 4.1.B01 o 4.1.B02	YES	Password cracking lab	1,66	7
6	11	Topic 7: Key Distribution	X				Mechanisms for exchanging sesión keys	1,66	
6	12	Lab 2 – Operation modes		X	Computer room 4.1.B01 o 4.1.B02	YES	Analysing how different block sizes and modes of opperation work together.	1,66	7
7	13	Topic 8: Asymmetric encryption – Mathematical Basis, introduction to RSA	X				Discrete mathematics. Modular Arithmetic. Fast exponentiation. Mathematical basis of RSA.	1,66	
7	14	Asymmetric encryption		X			Exercises	1,66	7
8	15	Topic 8: Asymmetric encryption – Algorithms, Elliptic curves	X				ElGamal. Galois representations. Usage of elliptic curves in cryptography.	1,66	
8	16	Asymmetric encryption		X			Exercises	1,66	7
9	17	Topic 9: Authentication and Digital signatures – Hash functions	X				Hash functions and underlying concepts.		
9	18	Hash functions		X			Exercises	1,66	7
10	19	Topic 9: Authentication and Digital signatures - Digital signatures	X				Concept, format and algorithms for generating and validating digital signatures.	1,66	
10	20	Digital signatures		X			Exercises	1,66	7
11	21	Topic 9: Authentication and Digital signatures – Digital certificates	X				Concept, formats and cryptographic mechanisms for generating digital certificates.	1,66	
11	22	Digital certificates		X			Exercises	1,66	7
12	23	Topic 10: IPSEC	X				IPSEC. Negotiation, key distribution. Key generation. Encryption and authentication.	1,66	
12	24	IPSEC		X			Exercises	1,66	7

13	25	Topic 11: Transport Level Security	X				TLS/SSL. Negotiation, key distribution. Key generation. Encryption and authentication .	1,66	
13	26	Transport Level Security		X			Exercises	1,66	7
14	27	Lab 3 – Open SSL and asymmetric cryptography		X	Computer room 4.1.B01 o 4.1.B02	YES	Using OpenSSL to generate certfificates, encrypt and sign documents.	1,66	
14	28	Lab 4 – PGP and IPSEC)		X	Computer room 4.1.B01 o 4.1.B02	YES	Understanding PGP	1,66	7
	29	Review		X			Final review	1,66	
							Subtotal 1	**48**	**98**
		Total 1 *(total hours of student work 1-14)*						146	
15		Catch up hours						10	
16		Exam preparation and realization						24	
17									
18									
							Subtotal 2	**34**	
		Total 2 *(total hours of student work 15-18)*							
TOTAL *(Total 1 + Total 2. Up to 180 hours)*								**180**	