ANX-PR/CL/001-01

GUÍA DE APRENDIZAJE

ASIGNATURA

95000277 - Criptografía

PLAN DE ESTUDIOS

09TT - Grado En Ingenieria De Tecnologias Y Servicios De Telecomunicacion

CURSO ACADÉMICO Y SEMESTRE

2023/24 - Primer semestre

Índice

Guía de Aprendizaje

1. Datos descriptivos

1.1. Datos de la asignatura

Nombre de la asignatura	95000277 - Criptografía
No de créditos	4.5 ECTS
Carácter	Optativa
Curso	Tercero curso
Semestre	Quinto semestre
Período de impartición	Septiembre-Enero
Idioma de impartición	Castellano
Titulación	09TT - Grado en Ingenieria de Tecnologias y Servicios de Telecomunicacion
Centro responsable de la titulación	09 - Escuela Tecnica Superior De Ingenieros De Telecomunicacion
Curso académico	2023-24

2. Profesorado

2.1. Profesorado implicado en la docencia

Nombre	Despacho	Correo electrónico	Horario de tutorías *
Lorenzo Javier Martin Garcia (Coordinador/a)	A-307	lorenzojavier.martin@upm.es	Sin horario. Previa solicitud
Vicente Jara Vera	A-315	vicente.jara@upm.es	Sin horario. Previa solicitud

Maria Del Carmen Sanchez Avila	A-305	carmen.sanchez.avila@upm.es	Sin horario. Previa solicitud

* Las horas de tutoría son orientativas y pueden sufrir modificaciones. Se deberá confirmar los horarios de tutorías con el profesorado.

3. Requisitos previos obligatorios

3.1. Asignaturas previas requeridas para cursar la asignatura

- Algebra

3.2. Otros requisitos previos para cursar la asignatura

El plan de estudios Grado En Ingenieria De Tecnologias Y Servicios De Telecomunicacion no tiene definidos requisitos para esta asignatura.

4. Competencias y resultados de aprendizaje

4.1. Competencias

CEB1 - Capacidad para la resolución de los problemas matemáticos que puedan plantearse en la ingeniería. Aptitud para aplicar los conocimientos sobre: álgebra lineal; geometría; geometría diferencial; cálculo diferencial e integral; ecuaciones diferenciales y en derivadas parciales; métodos numéricos; algorítmica numérica; estadística y optimización

CEB2 - Conocimientos básicos sobre el uso y programación de los ordenadores, sistemas operativos, bases de datos y programas informáticos con aplicación en ingeniería

CG10 - Creatividad

CG5 - Que los estudiantes hayan desarrollado aquellas habilidades de aprendizaje necesarias para emprender estudios posteriores con un alto grado de autonomía

CG9 - Uso de Tecnologías de la Información y de las Comunicaciones

4.2. Resultados del aprendizaje

RA725 - Comprender y operar con soltura diversos sistemas criptográficos fundamentales

RA727 - Comprender la diversa fundamentación de la criptografía no cuántica frente a la variante cuántica y algunos sistemas post-cuánticos

RA726 - Comprender y manejar primitivas y esquemas básicos de mantenimiento de la integridad (funciones hash) y de autenticación (firmas digitales) de la información

RA45 - Conocimientos y habilidades de las temáticas científico tecnológicas desarrolladas en las asignaturas ofertadas

RA722 - Comprender, interpretar y aplicar teoremas, propiedades y técnicas de la teoría de números, principalmente los relacionados con los números primos

RA728 - Comprender e interpretar la utilización y necesidad de la criptografía en de la tecnología blockchain

RA723 - Manejar con soltura las operaciones en cuerpos finitos y en sus anillos de polinomios

RA724 - Operar fluidamente en la aritmética entera y modular

5. Descripción de la asignatura y temario

5.1. Descripción de la asignatura

La asignatura comienza con una breve introducción a la Matemática discreta, la teoría de números y los cuerpos finitos donde se exponen los conceptos y resultados necesarios para comprender y manejar las técnicas y estrategias propias de la Criptografía actual.

A continuación se estudian los sistemas criptográficos simétricos y asimétricos basados en el conocimiento o desconocimiento público de las claves. Se hace especial mención a la seguridad de las firmas digitales y se concluye analizando la situación actual de la criptografía post-cuántica y a los métodos criptográficos utilizados en blockchain.

5.2. Temario de la asignatura

1. Nociones de Matemática discreta

   1.1. Técnicas de recuento

   1.2. Teoría de números

   1.3. Aritmética modular. Congruencias

2. Criptografía

   2.1. Historia de la Criptografía

   2.2. Criptografía de clave secreta (DES, AES)

   2.3. Criptografía de clave pública (RSA, ElGamal, ECC)

   2.4. Funciones hash

   2.5. Firma digital (Firmas RSA y ElGamal, ECDSA)

   2.6. Estado actual de la criptografía post-cuántica (Shor, Grover, McElliece, candidatos NIST a estándares post-cuánticos)

   2.7. Métodos criptográficos en blockchain

6. Cronograma

6.1. Cronograma de la asignatura *

Sem	Actividad en aula	Actividad en laboratorio	Tele-enseñanza	Actividades de evaluación
1	**Técnicas de recuento** Duración: 02:00 LM: Actividad del tipo Lección Magistral **Teoría de números** Duración: 01:00 LM: Actividad del tipo Lección Magistral			
2	**Aritmética modular. Cuerpos finitos** Duración: 02:00 LM: Actividad del tipo Lección Magistral **Técnicas de recuento y Teoría de números** Duración: 01:00 PR: Actividad del tipo Clase de Problemas			
3	**Aritmética modular. Congruencias** Duración: 02:00 LM: Actividad del tipo Lección Magistral **Aritmética modular. Congruencias. Cuerpos finitos** Duración: 01:00 PR: Actividad del tipo Clase de Problemas			
4	**Matemática discreta** Duración: 01:00 OT: Otras actividades formativas **Historia de la Criptografía** Duración: 02:00 LM: Actividad del tipo Lección Magistral			**Examen presencial sobre Matemática discreta** EX: Técnica del tipo Examen Escrito Evaluación continua y sólo prueba final Presencial Duración: 03:00
5	**Historia de la Criptografía** Duración: 02:00 LM: Actividad del tipo Lección Magistral **Historia de la Criptografía, Práctica Maple** Duración: 01:00 PL: Actividad del tipo Prácticas de Laboratorio			
6	**Criptografia secreta** Duración: 03:00 LM: Actividad del tipo Lección Magistral			

7	**Criptografia secreta** Duración: 02:00 PR: Actividad del tipo Clase de Problemas **Criptografia secreta. Práctica Maple** Duración: 01:00 PL: Actividad del tipo Prácticas de Laboratorio			
8	**Criptografia pública** Duración: 03:00 LM: Actividad del tipo Lección Magistral			
9	**Criptografia pública** Duración: 02:00 PR: Actividad del tipo Clase de Problemas **Criptografia pública. Práctica Maple** Duración: 01:00 PL: Actividad del tipo Prácticas de Laboratorio			
10	**Funciones hash** Duración: 01:00 LM: Actividad del tipo Lección Magistral **Funciones hash** Duración: 01:00 PR: Actividad del tipo Clase de Problemas **Firma digital y certificados** Duración: 01:00 LM: Actividad del tipo Lección Magistral			
11	**Firma digital y certificados** Duración: 01:00 LM: Actividad del tipo Lección Magistral **Firma digital y certificados** Duración: 01:00 PR: Actividad del tipo Clase de Problemas **Firma digital y certificados. Práctica Maple y lenguaje de alto nivel (Python, Java, C...)** Duración: 01:00 PL: Actividad del tipo Prácticas de Laboratorio			
12	**Criptografia post-cuántica** Duración: 03:00 LM: Actividad del tipo Lección Magistral			
13	**Criptografia post-cuántica** Duración: 02:00 LM: Actividad del tipo Lección Magistral **Criptografia post-cuántica. Práctica Maple y Qiskit** Duración: 01:00 PL: Actividad del tipo Prácticas de Laboratorio			

14	**Blockchain** Duración: 02:00 LM: Actividad del tipo Lección Magistral **Blockchain** Duración: 01:00 PR: Actividad del tipo Clase de Problemas			
15				
16				
17				**Examen presencial sobre Criptografía** EX: Técnica del tipo Examen Escrito Evaluación continua y sólo prueba final Presencial Duración: 03:00 **Entrega trabajo en grupo** TG: Técnica del tipo Trabajo en Grupo Evaluación continua y sólo prueba final Presencial Duración: 00:00

Para el cálculo de los valores totales, se estima que por cada crédito ECTS el alumno dedicará dependiendo del plan de estudios, entre 26 y 27 horas de trabajo presencial y no presencial.

* El cronograma sigue una planificación teórica de la asignatura y puede sufrir modificaciones durante el curso derivadas de la situación creada por la COVID-19.

7. Actividades y criterios de evaluación

7.1. Actividades de evaluación de la asignatura

7.1.1. Evaluación (progresiva)

Sem.	Descripción	Modalidad	Tipo	Duración	Peso en la nota	Nota mínima	Competencias evaluadas
4	Examen presencial sobre Matemática discreta	EX: Técnica del tipo Examen Escrito	Presencial	03:00	20%	0 / 10	CG10 CEB1 CG5
17	Examen presencial sobre Criptografía	EX: Técnica del tipo Examen Escrito	Presencial	03:00	60%	0 / 10	CG10 CEB1 CEB2 CG5
17	Entrega trabajo en grupo	TG: Técnica del tipo Trabajo en Grupo	Presencial	00:00	20%	0 / 10	CG9 CG10 CEB1 CEB2 CG5

7.1.2. Prueba evaluación global

Sem	Descripción	Modalidad	Tipo	Duración	Peso en la nota	Nota mínima	Competencias evaluadas
4	Examen presencial sobre Matemática discreta	EX: Técnica del tipo Examen Escrito	Presencial	03:00	20%	0 / 10	CG10 CEB1 CG5
17	Examen presencial sobre Criptografía	EX: Técnica del tipo Examen Escrito	Presencial	03:00	60%	0 / 10	CG10 CEB1 CEB2 CG5
17	Entrega trabajo en grupo	TG: Técnica del tipo Trabajo en Grupo	Presencial	00:00	20%	0 / 10	CG9 CG10 CEB1 CEB2 CG5

7.1.3. Evaluación convocatoria extraordinaria

Descripción	Modalidad	Tipo	Duración	Peso en la nota	Nota mínima	Competencias evaluadas
Examen presencial sobre todo el temario	EX: Técnica del tipo Examen Escrito	Presencial	03:00	80%	0 / 10	CG10 CEB1 CEB2 CG5
Entrega trabajo en grupo	TG: Técnica del tipo Trabajo en Grupo	Presencial	00:00	20%	0 / 10	CG9 CG10 CEB1 CEB2 CG5

7.2. Criterios de evaluación

La asignatura se superará al obtener 5 o más puntos de los 10 posibles en las actividades de evaluación.

Se considera **Actividad Obligatoria** para la evaluación de esta asignatura, la entrega de un trabajo durante el periodo docente que podrá aportar hasta 2 puntos de la nota total del curso. La oferta de trabajos se publicará a lo largo del periodo docente especificándose las características de redacción y los plazos de entrega.

Convocatoria ordinaria. Evaluación progresiva y evaluación global

- Actividad obligatoria: entrega de un trabajo por un valor máximo de 2 puntos de la nota final.
- Examen (primer parcial) presencial al finalizar los contenidos de Matemática discreta que tendrá un valor máximo de 2 puntos.
- Examen (final) presencial en el que todos los alumnos realizarán una prueba (segundo parcial) sobre los contenidos de Criptografía que tendrá un valor máximo de 6 puntos y quienes lo deseen realizarán una prueba adicional sobre Matemática discreta con un peso de 2 puntos renunciando con su presentación a la calificación obtenida en el Examen (primer parcial) realizado a mitad de curso.

Convocatoria extraordinaria. Evaluación global no progresiva

- Actividad obligatoria: entrega de un trabajo por un valor máximo de 2 puntos de la nota final. Si el alumno ya ha realizado un trabajo en la evaluación progresiva o global, se mantendrá la nota obtenida salvo que el alumno realice un nuevo trabajo siguiendo los plazos y condiciones que se establezcan.
- Examen presencial sobre el temario completo de la asignatura y que supondrá 8 puntos de la nota final.

8. Recursos didácticos

8.1. Recursos didácticos de la asignatura

Nombre	Tipo	Observaciones
Kenneth H. Rosen. Matemática Discreta y sus aplicaciones. McGraw-Hill, Madrid, quinta edición, 2004.	Bibliografía	
Juan de Burgos Román. Matemática Discreta. 21 problemas útiles. García-Maroto Editores, S.L., Madrid, primera edición, 2011.	Bibliografía	
A. J. Menezes, P. C. van Oorschot, S. A. Vanstone, Handbook of Applied Cryptography, CRC Press, Boca Raton, Florida, 1996.	Bibliografía	
D. J. Bernstein, J. Buchmann, E. Dahmen, Post-Quantum cryptography, Springer, Berlin, 2009.	Bibliografía	
A. Bolfing, Cryptographic Primitives in Blockchain Technology, Oxford University Press, Oxford, 2020.	Bibliografía	
V. Jara Vera, C. Sánchez Ávila, "Problemas resueltos de Criptografía", Paraninfo, Madrid, 2019.	Bibliografía	
Material de trabajo de la asignatura, elaborado por el profesorado y diisponible en Moodle	Otros	

9. Otra información

9.1. Otra información sobre la asignatura

La asignatura se relaciona directamente con los ODS 11 y 12: "Lograr que las ciudades y los asentamientos humanos sean inclusivos, seguros, resilientes y sostenibles" y "Garantizar modalidades de consumo y producción sostenibles" porque las técnicas que en ella se presentan sirven para preservar la privacidad y asegurar que cualquier tipo de transacciones informáticas pueda realizarse de forma segura y eficiente.