UNIVERSIDAD DE CASTILLA - LA MANCHA

GUÍA DOCENTE

1. DATOS GENERALES

Asignatura:	CRIPTOGRAFÍA	**Código:**	42364
Tipología:	OPTATIVA	**Créditos ECTS:**	6
Grado:	346 - GRADO EN INGENIERÍA INFORMÁTICA (AB)	**Curso académico:**	2018-19
Centro:	604 - ESCUELA SUPERIOR DE INGENIERIA INFORMATICA (AB)	**Grupo(s):**	17
Curso:	4	**Duración:**	C2
Lengua principal de impartición:	Español	**Segunda lengua:**	Inglés
Uso docente de otras lenguas:	Inglés (bibliografía)	**English Friendly:**	N
Página web:		**Bilingüe:**	N

Profesor: **GUILLERMO MANJABACAS TENDERO** - Grupo(s): **17**

Edificio/Despacho	Departamento	Teléfono	Correo electrónico	Horario de tutoría
	MATEMÁTICAS		CristinaRGonzalez@uclm.es	

2. REQUISITOS PREVIOS

No se considera necesario ningún requisito previo ya que se presentarán los temas de forma autocontenida. Es aconsejable haber cursado los módulos de Formación Básica y el módulo común a la rama Informátíca, ya que estos proporcionan la base necesaria para poder comprender íntegramente todos los contenidos de esta asignatura.

3. JUSTIFICACIÓN EN EL PLAN DE ESTUDIOS, RELACIÓN CON OTRAS ASIGNATURAS Y CON LA PROFESIÓN

La seguridad, entendida en el sentido de conseguir que determinada información sólo sea accesible al grupo de personas al que va dirigida, es una pieza clave en muchos procesos informáticos. Además, cada día es más frecuente la utilización de certificados y firmas digitales, el procedimiento de autentificación digital de documentos y, en general, los procesos que permiten una comunicación segura entre ordenadores. En esta asignatura se estudian algunas de las técnicas y algoritmos que están detrás de estos protocolos y que ayudan a conseguir esta seguridad desde el punto de vista de almacenado y transmisión de la información. Esta es una asignatura optativa encuadrada en la materia de Sistemas Inteligentes. Está relacionada principalmente con Seguridad de Sistemas Software, Seguridad en Redes y Seguridad en Sistemas Informáticos.

4. COMPETENCIAS DE LA TITULACIÓN QUE LA ASIGNATURA CONTRIBUYE A ALCANZAR

Competencias propias de la asignatura

Código	Descripción
BA1	Capacidad para la resolución de los problemas matemáticos que puedan plantearse en la ingeniería. Aptitud para aplicar los conocimientos sobre: álgebra lineal; cálculo diferencial e integral; métodos numéricos, algorítmica numérica, estadística y optimización.
IC6	Capacidad para comprender, aplicar y gestionar la garantía y seguridad de los sistemas informáticos.
INS1	Capacidad de análisis, síntesis y evaluación.
INS4	Capacidad de resolución de problemas aplicando técnicas de ingeniería.
PER5	Reconocimiento a la diversidad, la igualdad y la multiculturalidad.
SIS7	Conocimiento de otras culturas y costumbres.
SIS9	Tener motivación por la calidad.

5. OBJETIVOS O RESULTADOS DE APRENDIZAJE ESPERADOS

Resultados de aprendizaje propios de la asignatura

Descripción

Conocer las técnicas de cifrado y criptoanálisis.

Conocer las metodologías para garantizar el secreto en las comunicaciones.

Resultados adicionales

Conocer el esquema general de un sistema criptográfico.
Conocer las bases teóricas más importantes de la Criptografía.
Saber diferenciar entre cifrado simétrico y asimétrico, y conocer algunos algoritmos importantes de cada tipo.
Conocer algunas técnicas criptográficas que se
utilizan en aplicaciones: comunicación segura, firmas digitales, certificados, etc.

6. TEMARIO

Tema 1: Conceptos básicos

- **Tema 1.1** Terminología básica
- **Tema 1.2** Breve historia de la Criptografía
- **Tema 1.3** La criptografía digital moderna. Seguridad en sistemas informáticos

Tema 2: Fundamentos matemáticos de la Criptografía

- **Tema 2.1** Aritmética modular

Tema 2.2 Números primos
Tema 2.3 Algoritmos de factorización
Tema 2.4 Algoritmos de primalidad
Tema 2.5 El problema del logaritmo discreto

Tema 3: Algoritmos criptográficos

Tema 3.1 Algunas técnicas clásicas
Tema 3.2 Cifrados en flujo
Tema 3.3 Cifrado en bloque simétrico con clave secreta
Tema 3.4 DES y algunas variantes
Tema 3.5 AES
Tema 3.6 Cifrado en bloque asimétrico con clave pública
Tema 3.7 RSA
Tema 3.8 Otros algoritmos asimétricos
Tema 3.9 Algoritmos con curvas elípticas

Tema 4: Aplicaciones criptográficas

Tema 4.1 Firmas digitales
Tema 4.2 Funciones resumen
Tema 4.3 Certificados digitales
Tema 4.4 Autentificación
Tema 4.5 Transacciones electrónicas
Tema 4.6 Comunicaciones inalámbricas
Tema 4.7 Otras aplicaciones

7. ACTIVIDADES O BLOQUES DE ACTIVIDAD Y METODOLOGÍA

Actividad formativa	Metodología	Competencias relacionadas	ECTS	Horas	Ev	Ob	Rec	Descripción
Enseñanza presencial (Teoría) [PRESENCIAL]	Combinación de métodos	BA1 IC6 INS1 INS4 PER5 SIS7	1.04	26	N	-	-	Las clases teóricas se organizan en sesiones de entre y 1.5 horas y 2 horas, dependiendo de la planificación de horarios oficial. Se incluyen: clases magistrales, lectura de artículos, resolución de ejercicios y problemas, presentación de trabajos o temas.
Resolución de problemas o casos [PRESENCIAL]	Combinación de métodos	BA1 IC6 INS1 INS4 SIS9	0.48	12	N	-	-	Resolución de problemas en el laboratorio, donde se podrá hacer uso del ordenador.
Prácticas en aulas de ordenadores [PRESENCIAL]	Prácticas	BA1 IC6 INS1 INS4 SIS9	0.64	16	S	N	N	Realización de prácticas con uso de software adecuado en el laboratorio. Las clases prácticas se organizan en sesiones de entre 1.5 y 2 horas, según el horario oficial.
Presentación de trabajos o temas [PRESENCIAL]		BA1 IC6 INS1 INS4 SIS9	0.04	1	S	N	N	Presentación oral de un trabajo original relacionado con los contenidos de la asignatura.
Elaboración de informes o trabajos [AUTÓNOMA]	Trabajo dirigido o tutorizado	BA1 IC6 INS1 INS4 PER5 SIS7 SIS9	0.8	20	S	S	S	Presentación escrita de dos trabajos relacionados con la asignatura. Uno de ellos se expondrá de forma oral.
Elaboración de memorias de Prácticas [AUTÓNOMA]	Trabajo autónomo	BA1 IC6 INS1 INS4 SIS9	0.72	18	S	S	S	Presentación escrita de un informe con la resolución de los ejercicios propuestos en prácticas.
Estudio o preparación de pruebas [AUTÓNOMA]	Combinación de métodos	BA1 IC6 INS1 INS4	2.08	52	N	-	-	Estudio autónomo.
Tutorías individuales [PRESENCIAL]		INS1 INS4	0.2	5	N	-	-	
		Total:	**6**	**150**				
Créditos totales de trabajo presencial: 2.4					**Horas totales de trabajo presencial: 60**			
Créditos totales de trabajo autónomo: 3.6					**Horas totales de trabajo autónomo: 90**			

Ev: Actividad formativa evaluable
Ob: Actividad formativa de superación obligatoria
Rec: Actividad formativa recuperable

8. CRITERIOS DE EVALUACIÓN Y VALORACIONES

	Valoraciones		
Sistema de evaluación	**Estudiante presencial**	**Estud. semipres.**	**Descripción**
Prueba	40.00%	0.00%	ESC] Actividad individual. Se considerarán dos pruebas escritas que consistirán en la realización de dos trabajos, uno a mitad de curso y otro al final, donde se valorará la aplicación de los contenidos estudiados a algún caso concreto. Ambos trabajos tendrán el mismo

			peso en la calificación final. Cada alumno podrá orientar sus trabajos a los aspectos de la asignatura que sean de su interés, entre los propuestos por el profesor.
Resolución de problemas o casos	20.00%	0.00%	[INF] Actividad individual. A lo largo del curso, se propondrá la resolución de algunos problemas relacionados con la materia, que serán entregados por escrito para su valoración.
Elaboración de memorias de prácticas	30.00%	0.00%	[LAB] Actividad individual. Se presentará un informe de prácticas con la resolución de los ejercicios propuestos en las mismas.
Presentación oral de temas	10.00%	0.00%	[PRES] Actividad individual. Uno de los trabajos escritos será presentado de forma oral, en horario de clase.
Total:	**100.00%**	**0.00%**	

Criterios de evaluación de la convocatoria ordinaria:

En la convocatoria ordinaria, la calificación final será la media ponderada de las notas parciales obtenidas en los trabajos, ejercicios y prácticas presentados en su momento (se anunciará con antelación la fecha para cada uno). Para aprobar la asignatura, no se necesita obtener una nota mínima en ninguna de las tareas.

Particularidades de la convocatoria extraordinaria:

Si un alumno no ha aprobado en la convocatoria ordinaria, se le guardarán las notas parciales obtenidas para la convocatoria ordinaria y, además, podrá presentar antes de la fecha del examen previsto por la Subdirección de Ordenación Académica, los trabajos, ejercicios y prácticas no presentados con anterioridad, o bien presentar de nuevo aquellas tareas en las que pueda obtener una nota superior. La calificación final seguirá los mismos criterios que en la convocatoria ordinaria.

Particularidades de la convocatoria especial de finalización:

El alumno realizará un examen final sobre los contenidos de la asignatura que podrá incluir teoría, problemas y cuestiones relacionadas tanto con los temas expuestos en clase como con las prácticas.

9. SECUENCIA DE TRABAJO, CALENDARIO, HITOS IMPORTANTES E INVERSIÓN TEMPORAL

No asignables a temas

Horas	**Suma horas**

Tema 1 (de 4): Conceptos básicos

Actividades formativas	**Horas**
Enseñanza presencial (Teoría) [PRESENCIAL][Combinación de métodos]	3
Prácticas en aulas de ordenadores [PRESENCIAL][Prácticas]	1.5
Elaboración de memorias de Prácticas [AUTÓNOMA][Trabajo autónomo]	2
Estudio o preparación de pruebas [AUTÓNOMA][Combinación de métodos]	2

Tema 2 (de 4): Fundamentos matemáticos de la Criptografía

Actividades formativas	**Horas**
Enseñanza presencial (Teoría) [PRESENCIAL][Combinación de métodos]	6
Resolución de problemas o casos [PRESENCIAL][Combinación de métodos]	4.5
Prácticas en aulas de ordenadores [PRESENCIAL][Prácticas]	3
Elaboración de memorias de Prácticas [AUTÓNOMA][Trabajo autónomo]	6
Estudio o preparación de pruebas [AUTÓNOMA][Combinación de métodos]	12

Tema 3 (de 4): Algoritmos criptográficos

Actividades formativas	**Horas**
Enseñanza presencial (Teoría) [PRESENCIAL][Combinación de métodos]	9
Resolución de problemas o casos [PRESENCIAL][Combinación de métodos]	6
Prácticas en aulas de ordenadores [PRESENCIAL][Prácticas]	7.5
Elaboración de memorias de Prácticas [AUTÓNOMA][Trabajo autónomo]	4
Estudio o preparación de pruebas [AUTÓNOMA][Combinación de métodos]	20

Tema 4 (de 4): Aplicaciones criptográficas

Actividades formativas	**Horas**
Enseñanza presencial (Teoría) [PRESENCIAL][Combinación de métodos]	7.5
Resolución de problemas o casos [PRESENCIAL][Combinación de métodos]	1.5
Prácticas en aulas de ordenadores [PRESENCIAL][Prácticas]	4.5
Elaboración de memorias de Prácticas [AUTÓNOMA][Trabajo autónomo]	6
Estudio o preparación de pruebas [AUTÓNOMA][Combinación de métodos]	18

Actividad global

Actividades formativas	**Suma horas**
Enseñanza presencial (Teoría) [PRESENCIAL][Combinación de métodos]	25.5
Prácticas en aulas de ordenadores [PRESENCIAL][Prácticas]	16.5
Estudio o preparación de pruebas [AUTÓNOMA][Combinación de métodos]	52
Elaboración de memorias de Prácticas [AUTÓNOMA][Trabajo autónomo]	18
Resolución de problemas o casos [PRESENCIAL][Combinación de métodos]	12
Total horas:	124

10. BIBLIOGRAFÍA, RECURSOS

Autor/es	**Título/Enlace Web**	**Editorial**	**Población**	**ISBN**	**Año**	**Descripción**
Vaudenay, S.	A classical introduction to cryptography. Applications for	Springer		978-0387254647	2006	

	communications security			
Trappe, W.	Introduction to cryptography with coding theory 2nd. ed.)	Pearson Education	0-13-198199-4	2006
Paar, C. y Pelzl, J.	Understanding cryptography : a textbook for students and practitioners	Springer	978-3-642-44649-8	2010
Fuster, A. y otros	Técnicas criptográficas de protección de datos (3ª ed.)	Ra-Ma	978-84-7897-594-5	2004
Gómez Pardo, José L.	Introduction to cryptography with Maple	Springer	978-3-642-32165-8	2013
Katz, J. y Lindell, Y.	Introduction to modern cryptography (2nd. ed.)	Chapman & Hall/CRC	978-1-4665-7026-9	2014
Stallings, W.	Cryptography and network security : principles and practice (6th. ed.)	Prentice-Hall Pearson Education	978-0-13-705632-3	2013