UNIVERSIDAD DE CASTILLA - LA MANCHA

GUÍA DOCENTE

1. DATOS GENERALES

Asignatura: CRIPTOGRAFÍA
Código: 42364
Tipología: OPTATIVA
Créditos ECTS: 6
Grado: 406 - GRADO EN INGENIERÍA INFORMÁTICA (AB)_20
Curso académico: 2021-22
Centro: 604 - E.S. DE INGENIERÍA INFORMÁTICA ALBACETE
Grupo(s): 17
Curso: 4
Duración: C2
Lengua principal de impartición: Español
Segunda lengua:
Uso docente de otras lenguas: Inglés para bibliografía y material de consulta.
English Friendly: N
Página web:
Bilingüe: N

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

Edificio/Despacho	Departamento	Teléfono	Correo electrónico	Horario de tutoría
Infante Don Juan Manuel. Despacho 1.B.4	MATEMÁTICAS	2172	guillermo.manjabacas@uclm.es	Consultar en www.esiiab.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 todas las asignaturas de los módulos de Formación Básica así como las del módulo común a la rama Informática, ya que estas proporcionan la base necesaria para poder comprender integramente todos los contenidos de esta asignatura.

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

La criptografía puede considerarse una herramienta fundamental para conseguir que determinada información sea solo accesible al grupo de personas a las que va dirigida, especialmente cuando se considera que esa información puede estar al alcance de otras personas. Entre sus posibilidades comprende el proceso de cifrado y descifrado de la información, el uso de certificados y firmas digitales, el procedimiento de autentificación digital de documentos y, en general, cualquier proceso en el que se pretende 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 la seguridad desde el punto de visto de almacenado y transmisión de la información. Esta asignatura 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
BA01	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.
IC06	Capacidad para comprender, aplicar y gestionar la garantía y seguridad de los sistemas informáticos.
INS01	Capacidad de análisis, síntesis y evaluación.
INS04	Capacidad de resolución de problemas aplicando técnicas de ingeniería.
SIS03	Aprendizaje autónomo.

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 los distintos sistemas criptográficos.

Saber diferenciar entre sistema criptográfica simétrico o asimétrico y conocer algunos algoritmos importantes de cada tipo.

Conocer algunas técnicas criptográficas muy utilizadas en aplicaciones: comunicación segura, firmas digitales, certificados, etc.

Conocer las bases teóricas usadas en criptografía.

6. TEMARIO

Tema 1: Conceptos básicos

- **Tema 1.1** Terminología
- **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	Descripción
Enseñanza presencial (Teoría) [PRESENCIAL]	Combinación de métodos	BA01 IC06 INS01 INS04	1.04	26	N	-	Se incluyen: clases magistrales, lectura de artículos, resolución de ejercicios y problemas.
Resolución de problemas o casos [PRESENCIAL]	Combinación de métodos	BA01 IC06 INS01 INS04	0.48	12	N	-	Resolución de problemas en el laboratorio, con la posibilidad de hacer uso del ordenador.
Prácticas en aulas de ordenadores [PRESENCIAL]	Prácticas	BA01 IC06 INS01 INS04	0.64	16	N	-	Realización de prácticas con uso de software adecuado en el laboratorio.
Presentación de trabajos o temas [PRESENCIAL]		BA01 IC06 INS01 INS04 SIS03	0.04	1	S	S	Presentación oral de un trabajo original relacionado con los contenidos de la asignatura.
Elaboración de informes o trabajos [AUTÓNOMA]	Trabajo dirigido o tutorizado	BA01 IC06 INS01 INS04 SIS03	0.8	20	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	BA01 IC06 INS01 INS04 SIS03	0.72	18	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	BA01 IC06 INS01 INS04 SIS03	2.08	52	N	-	Estudio autónomo.
Tutorías individuales [PRESENCIAL]			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 (Será imprescindible su superación tanto en evaluación continua como no continua)

8. CRITERIOS DE EVALUACIÓN Y VALORACIONES

Sistema de evaluación	Evaluacion continua	Evaluación no continua*	Descripción
Presentación oral de temas	10.00%	10.00%	[PRES] Actividad individual. Uno de los trabajos escritos será presentado de forma oral, preferentemente en horario de clase.
Prueba	40.00%	40.00%	[ESC] Actividad individual, aunque puede considerarse en algún caso la realización en grupo. Se considerarán dos pruebas escritas que consisten 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.
Elaboración de memorias de prácticas	30.00%	30.00%	[LAB] Actividad individual. Se presentará un informe de prácticas con la resolución de los problemas propuestos en las mismas.
Resolución de problemas o casos	20.00%	20.00%	[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.
Total:	**100.00%**	**100.00%**	

** En **Evaluación no continua** se deben definir los porcentajes de evaluación según lo dispuesto en el art. 6 del Reglamento de Evaluación del Estudiante de la UCLM, que establece que debe facilitarse a los estudiantes que no puedan asistir regularmente a las actividades formativas presenciales la superación de la*

asignatura, teniendo derecho (art. 13.2) a ser calificado globalmente, en 2 convocatorias anuales por asignatura, una ordinaria y otra extraordinaria (evaluándose el 100% de las competencias).

Criterios de evaluación de la convocatoria ordinaria:

Evaluación continua:

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 establece ninguna nota mínima para ninguna tarea.

Evaluación no continua:

En caso de no haber sido evaluado de las tareas que corresponden al menos a un 50% de la nota final en las fechas previstas en la evaluación continua, el alumno podrá realizar las tareas no evaluadas hasta el momento en una fecha próxima a la del examen previsto por la Subdirección de Ordenación Académica, que se indicará con suficiente antelación. En este caso, se conservarán las notas obtenidas en la evaluación continua.

Particularidades de la convocatoria extraordinaria:

Si un alumno no ha aprobado en la convocatoria ordinaria, se le guardarán las notas parciales obtenidas en dicha convocatoria 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 será de nuevo la media ponderada de las notas parciales obtenidas en todas las tareas, al igual 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
Tutorías individuales [PRESENCIAL][]	5

Comentarios generales sobre la planificación: La asignatura se imparte en tres sesiones semanales de 1h20m. La planificación es orientativa, pudiendo variar a lo largo del curso en función de las necesidades docentes, festividades o por cualquier otra causa imprevista. Aparecerá una planificación actualizada en la plataforma Campus Virtual.

Tema 1 (de 4): Conceptos básicos

Actividades formativas	Horas
Enseñanza presencial (Teoría) [PRESENCIAL][Combinación de métodos]	2.5
Prácticas en aulas de ordenadores [PRESENCIAL][Prácticas]	1.5
Elaboración de memorias de Prácticas [AUTÓNOMA][Trabajo autónomo]	1.5

Periodo temporal: Semana 1

Comentario: Periodo aproximado, dependiendo de la dinámica del curso.

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

Actividades formativas	Horas
Enseñanza presencial (Teoría) [PRESENCIAL][Combinación de métodos]	7.5
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

Periodo temporal: 4 semanas

Comentario: Periodo aproximado, dependiendo de la dinámica del curso.

Tema 3 (de 4): Algoritmos criptográficos

Actividades formativas	Horas
Enseñanza presencial (Teoría) [PRESENCIAL][Combinación de métodos]	8
Resolución de problemas o casos [PRESENCIAL][Combinación de métodos]	4.5
Prácticas en aulas de ordenadores [PRESENCIAL][Prácticas]	4.5
Presentación de trabajos o temas [PRESENCIAL][]	1
Elaboración de informes o trabajos [AUTÓNOMA][Trabajo dirigido o tutorizado]	10
Elaboración de memorias de Prácticas [AUTÓNOMA][Trabajo autónomo]	5.5
Estudio o preparación de pruebas [AUTÓNOMA][Combinación de métodos]	25

Periodo temporal: 5 semanas

Comentario: Periodo aproximado, dependiendo de la dinámica del curso.

Tema 4 (de 4): Aplicaciones criptográficas

Actividades formativas	Horas
Enseñanza presencial (Teoría) [PRESENCIAL][Combinación de métodos]	8
Resolución de problemas o casos [PRESENCIAL][Combinación de métodos]	3
Prácticas en aulas de ordenadores [PRESENCIAL][Prácticas]	7
Elaboración de informes o trabajos [AUTÓNOMA][Trabajo dirigido o tutorizado]	10
Elaboración de memorias de Prácticas [AUTÓNOMA][Trabajo autónomo]	5
Estudio o preparación de pruebas [AUTÓNOMA][Combinación de métodos]	15

Periodo temporal: 5 semanas

Comentario: Periodo aproximado, dependiendo de la dinámica del curso.

Actividad global

Actividades formativas	Suma horas
Elaboración de informes o trabajos [AUTÓNOMA][Trabajo dirigido o tutorizado]	20
Elaboración de memorias de Prácticas [AUTÓNOMA][Trabajo autónomo]	18
Presentación de trabajos o temas [PRESENCIAL][]	1
Enseñanza presencial (Teoría) [PRESENCIAL][Combinación de métodos]	26
Estudio o preparación de pruebas [AUTÓNOMA][Combinación de métodos]	52
Resolución de problemas o casos [PRESENCIAL][Combinación de métodos]	12

Prácticas en aulas de ordenadores [PRESENCIAL][Prácticas]	16
Tutorías individuales [PRESENCIAL][]	5
Total horas:	150

10. BIBLIOGRAFÍA, RECURSOS

Autor/es	Título/Enlace Web	Editorial	Población	ISBN	Año	Descripción
C. Paar, J. Pezl	Understanding cryptography: a textbook for students and practitioners	Springer		978-3-642-44649-8	2010	
J.L. Gómez Pardo	Introduction to cryptography with Maple	Springer		978-3-642-32165-8	2013	
A. Fúster y otros	Técnicas criptográficas de protección de datos (3ª ed)	Ra-Ma		978-84-7897-594-5	2004	
J.J. Ortega, M.Á. López y Eugenio C. García	Introducción a la criptografía: historia y actualidad	Ediciones de la Universidad de Castilla-La Mancha		84-8427-441-1	2006	
J. Katz y Y. Lindell	Introduction to modern cryptography (2nd. ed)	Chapman & Hall/CRC		978-1-4665-7026-9	2015	