

Titulación	Tipo	Curso
Matemática Computacional y Analítica de Datos	OP	4

Profesor/a de contacto

Nombre : Carlos Garrigues Olivella

Correo electrónico : carlos.garrigues@uab.cat

Equipo docente

Jordi Herrera Joancomarti

Cristina Fernandez Cordoba

Cristina Perez Sola

Idiomas de los grupos

Puede consultar esta información al [final](#) del documento.

Prerrequisitos

No hay requisitos obligatorios aunque se recomienda haber adquirido los conocimientos sobre álgebra, probabilidad, teoría de la información y programación de cursos anteriores.

Objetivos

En esta asignatura se dará una introducción a la criptografía. El objetivo es que el alumnado aprenda los principios fundamentales y herramientas que se utilizan en criptografía en la actualidad.

Resultados de aprendizaje

- KM33 (Identificar los resultados básicos de la seguridad en la información y la criptografía.) Identificar los resultados básicos de la seguridad en la información y la criptografía.
- KM34 (Identificar los parámetros que determinan la seguridad en el funcionamiento de un sistema.) Identificar los parámetros que determinan la seguridad en el funcionamiento de un sistema.
- SM40 (Utilizar métodos numéricos para resolver problemas en criptografía y seguridad.) Utilizar métodos numéricos para resolver problemas en criptografía y seguridad.
- SM42 (Distinguir, entre las distintas herramientas matemáticas, las que son factibles de cara a su implementación de las que no lo son.) Distinguir, entre las distintas herramientas matemáticas, las que son factibles de cara a su implementación de las que no lo son.

Contenidos

2. Introducción a la criptografía.
4. Fundamentos matemáticos de la criptografía.
6. Criptografía de clave simétrica.
8. Funciones hash.
10. Criptografía de clave pública.
12. Infraestructuras de clave pública.
14. Protocolos criptográficos.

Actividades formativas y Metodología

Título	Horas	ECTS	Resultados de aprendizaje
Preparación de sesiones	15	0,6	
Trabajo personal	30	1,2	
Tutorías	15	0,6	
Sesiones de teoría	30	1,2	
Estudio / preparación examen	22,5	0,9	
Sesiones de problemas	15	0,6	
Seminarios / prácticas	15	0,6	

La asignatura se imparte en dos sesiones semanales de 2 horas cada una. las sesiones se harán en una única aula con ordenadores o posibilidad de enchufar los portátiles de los alumnos. No hay una clara distinción entre sesiones de teoría, problemas y prácticas en el laboratorio. Estas se irán alternando durante el curso según convenga al seguimiento de la asignatura. En general, y para cada tema a tratar, se introducirán conceptos teóricos y se realizarán actividades más aplicadas como la resolución de problemas o seminarios. se recomienda que el alumno revise los materiales correspondientes a cada sesión con anterioridad. Se fomentará la participación activa en la resolución de problemas participando en su resolución, exposición y debate en el aula. Durante el curso se realizarán algunas prácticas de laboratorio o seminarios de trabajo práctico, donde se planteará uno o más problemas que requerirán el diseño y implementación de una solución completa.

De forma más específica, durante el curso se irán alternando:

- Sesiones de teoría: clases de tipo magistral donde el objetivo es introducir los conceptos básicos que permitan al alumnado obtener una visión general y una buena base a partir de la que desarrollar los contenidos y competencias de la asignatura. Se fomentará la interactividad y participación activa de del alumnado.
- Sesiones de problemas: sesiones en las que se plantean problemas o ejercicios concretos principalmente de carácter práctico y de seguimiento. Estos ejercicios tienen el objetivo de ayudar al alumnado a alcanzar y practicar los conceptos y competencias relacionadas con la asignatura. Los problemas se realizan en el caso general de forma individual.

- Prácticas / seminarios: se planteará algún problema más amplio que los tratados en las sesiones de problemas como un proyecto o práctica de laboratorio. Este se realizará y se evaluará en grupo. El número de prácticas a realizar dependerá de su dificultad y longitud y puede cambiar en cada curso.

Durante todo el curso se utilizará el aula Moodle del Campus Virtual de la UAB como medio principal de comunicación entre el profesorado y el alumnado. esto incluye la publicación de materiales, publicación de notas parciales, foro de discusión, entrega de trabajos, etc.

Nota: se reservarán 15 minutos de una clase dentro del calendario establecido por el centro o por la titulación para que el alumnado rellene las encuestas de evaluación de la actuación del profesorado y de evaluación de la asignatura o módulo.

Evaluación

Actividades de evaluación continuada

Título	Peso	Horas	ECTS	Resultados de aprendizaje
Problemas y ejercicios	15	1,5	0,06	KM33, KM34, SM40, SM42
Exámenes parciales	45	3	0,12	KM33, KM34, SM40, SM42
Prácticas / seminarios	40	3	0,12	KM33, KM34, SM40, SM42

La evaluación de la asignatura consta de las siguientes partes:

- Exámenes parciales: constan de preguntas teóricas y/o prácticas. El primero se realizará aproximadamente a mitad de curso y el segundo al final de curso. La nota mínima de cada parcial por separado es de 5.
- Ejercicios y problemas: resolución de problemas y ejercicios durante las sesiones de problemas. Pueden ser actividades de tipo práctico o teórico. No requiere nota mínima.
- Prácticas/seminarios: resolución en grupo de tres casos prácticos.

El resultado de las actividades prácticas / seminarios deberá entregarse a través del campus virtual, pero estas entregas no tendrán ninguna nota asociada.

- La evaluación de las prácticas se realizará únicamente mediante exámenes en papel que se realizarán en las fechas de los exámenes parciales.
- Si bien las prácticas se resuelven en grupo, los exámenes de prácticas son pruebas de carácter individual.
- En estas pruebas, se evaluará la asimilación tanto de los conceptos teóricos como prácticos asociados a cada actividad.
- Cada una de las 3 prácticas deberá aprobarse por separado con una nota mínima de 4,5.

Para aprobar la asignatura, será necesario que la evaluación de cada una de las partes (teoría y prácticas) supere el mínimo exigido. Además, la nota final calculada con la ponderación anteriormente indicada deberá superar los 5 puntos sobre 10.

En caso de no superar la asignatura porque alguna de las actividades de evaluación no llega a la nota mínima requerida, la nota numérica del expediente será el menor valor entre 4,5 y la media ponderada de las notas.

La calificación de "no evaluable" se otorgará al alumnado que no participe en ninguna de las actividades de evaluación.

La calificación de "matrícula de honor" se otorgará al alumnado con nota igual o superior a 9 por orden de mejor nota final.

Puede darse el caso de alguna pequeña variación en la ponderación de cada parte de la asignatura. Si esto fuera así, se comunicaría a principio de curso.

Recuperación de notas de la evaluación continua:

Se realizará un examen final de recuperación que permitirá recuperar los exámenes parciales por separado.

Asimismo se permitirá una entrega final para recuperar aquellas prácticas suspendidas (esta entrega adicional conllevará una penalización en la nota final de la práctica).

La parte de problemas y o actividades que no requiere nota mínima no se podrá recuperar.

Convalidaciones parciales al alumnado repetidor:

Inicialmente, no se plantea la posibilidad de convalidar partes de la asignatura, ni la realización de pruebas de síntesis especiales al alumnado repetidor. Sin embargo, este hecho se puede reconsiderar a comienzo de curso en función de los contenidos de cada parte.

Fechas de actividades de evaluación:

Las fechas de evaluación continua y entrega de trabajos y prácticas se publicarán en el campus virtual y pueden estar sujetas a cambios de programación por motivos de adaptación a posibles incidencias. Siempre se informará en el campus virtual sobre estos cambios ya que se entiende es el mecanismo habitual de intercambio de información entre el profesorado y el alumnado.

También se ofrecerá la posibilidad de recuperar los exámenes de prácticas suspendidos. Estas recuperaciones se realizarán conjuntamente con el examen final de recuperación de la asignatura.

Para cada actividad de evaluación, se indicará un lugar, fecha y hora de revisión en la que el estudiante podrá revisar la actividad con el profesor. En este contexto, se podrán hacer reclamaciones sobre la nota de la actividad, que serán evaluadas por el profesorado responsable de la asignatura. Si el estudiante no se presenta a esta revisión, no se revisará posteriormente esta actividad.

Compromiso ético:

Sin perjuicio de otras medidas disciplinarias que se estimen oportunas, y de acuerdo con la normativa académica vigente, las irregularidades cometidas por el alumnado que puedan conducir a una variación de la calificación, se calificarán con un cero (0). Las actividades de evaluación calificadas de esta forma y por este procedimiento no serán recuperables. Si es necesario superar cualquiera de estas actividades de evaluación para aprobar la asignatura, esta asignatura quedará suspendida directamente, sin oportunidad de recuperarla en el mismo curso. Estas irregularidades incluyen, entre otros:

- la copia total o parcial de una práctica, informe, o cualquier otra actividad de evaluación;
- dejar copiar;
- presentar un trabajo de grupo no hecho íntegramente por los miembros del grupo;
- presentar como propios materiales elaborados por un tercero, aunque sean traducciones o adaptaciones, y en general trabajos con elementos no originales y exclusivos del estudiante;
- tener dispositivos de comunicación (como teléfonos móviles, smart watches, etc.) accesibles durante las pruebas de evaluación teórico-prácticas individuales (exámenes).

La nota numérica del expediente será el valor menor entre 3.0 y la media ponderada de las notas en caso de que el estudiante haya cometido irregularidades en un acto de evaluación (y por tanto no será posible aprobar la asignatura por compensación).

Uso de una base de inteligencia artificial:

Esta asignatura establece una política de uso restringido de las tecnologías de inteligencia artificial (IA). Está permitido el uso de tecnologías de Inteligencia Artificial (IA) exclusivamente en tareas de soporte, como la búsqueda bibliográfica o de información, la corrección de textos, las traducciones, o la consulta de documentación sobre funciones o librerías de programas. Además, no está permitido utilizar la IA para generar íntegramente la solución de una práctica, ni para escribir funciones completas o fragmentos de código sustanciales. El estudiantado debe identificar claramente cuáles son los fragmentos que se han generado con esta tecnología y especificar las herramientas utilizadas. La no transparencia del uso de la IA en una actividad evaluable se considerará una falta de honestidad académica y puede comportar una penalización parcial o total en la nota de la actividad, o sanciones mayores en casos de gravedad.

Evaluación única:

La asignatura no da la posibilidad de realizar evaluación única.

Bibliografía

- Herrera Joancomartí, Jordi; Pérez Solà, Cristina. La criptografía que et cal saber. (2023) Disponible on-line: <https://criptografia.cat/>
- Paar, C., Pelzl, J., Understanding Cryptography: A Textbook for Students and Practitioners. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010. <https://doi.org/10.1007/978-3-642-04101-3>. Biblioteca UAB: https://bibcercador.uab.cat/permalink/34CSUC_UAB/1eqfv2p/alma991010489805006709
- Smart, N. P., Cryptography Made Simple. Springer International Publishing, 2016. <https://doi.org/10.1007/978-3-319-21936-3>. Biblioteca UAB: https://bibcercador.uab.cat/permalink/34CSUC_UAB/1eqfv2p/alma991006792939706709

Software

Durante el curso se utilizará software diverso en función de la actividad concreta que se lleve a cabo. Se prevé el uso del lenguaje de programación Python con lenguaje principal para la resolución de ejercicios y prácticas, y el uso de herramientas del sistema Linux como OpenSSL para alguna actividad concreta.

Grupos e idiomas de la asignatura

La información proporcionada es provisional hasta el 30 de noviembre. A partir de esta fecha, podrá consultar el idioma de cada grupo a través de este [enlace](#). Para acceder a la información, será necesario introducir el CÓDIGO de la asignatura