Universitat Autònoma de Barcelona

**2022/2023**

# Información y Seguridad

Código: 104418
Créditos ECTS: 6

| Titulación | Tipo | Curso | Semestre |
|---|---|---|---|
| 2503740 Matemática Computacional y Analítica de Datos | OT | 4 | 2 |

## Contacto

Nombre: Carlos Borrego Iglesias
Correo electrónico: carlos.borrego@uab.cat

## Uso de idiomas

Lengua vehicular mayoritaria: español (spa)
Algún grupo íntegramente en inglés: No
Algún grupo íntegramente en catalán: No
Algún grupo íntegramente en español: Sí

## Equipo docente

Carlos Borrego Iglesias

## Prerequisitos

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

## Objetivos y contextualización

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.

## Competencias

- Aplicar el espíritu crítico y el rigor para validar o refutar argumentos tanto propios como de otros.
- Diseñar, desarrollar y evaluar soluciones algorítmicas eficientes para problemas computacionales de acuerdo con los requisitos establecidos.
- Evaluar de manera crítica y con criterios de calidad el trabajo realizado.
- Formular hipótesis e imaginar estrategias para confirmarlas o refutarlas.
- Que los estudiantes hayan demostrado poseer y comprender conocimientos en un área de estudio que parte de la base de la educación secundaria general, y se suele encontrar a un nivel que, si bien se apoya en libros de texto avanzados, incluye también algunos aspectos que implican conocimientos procedentes de la vanguardia de su campo de estudio.
- Que los estudiantes hayan desarrollado aquellas habilidades de aprendizaje necesarias para emprender estudios posteriores con un alto grado de autonomía.
- Que los estudiantes sepan aplicar sus conocimientos a su trabajo o vocación de una forma profesional y posean las competencias que suelen demostrarse por medio de la elaboración y defensa de argumentos y la resolución de problemas dentro de su área de estudio.
- Que los estudiantes tengan la capacidad de reunir e interpretar datos relevantes (normalmente dentro de su área de estudio) para emitir juicios que incluyan una reflexión sobre temas relevantes de índole social, científica o ética.
- Relacionar objetos matemáticos nuevos con otros conocidos y deducir sus propiedades.

- Trabajar cooperativamente en un contexto multidisciplinar asumiendo y respetando el rol de los diferentes miembros del equipo.
- Utilizar eficazmente bibliografía y recursos electrónicos para obtener información.

## Resultados de aprendizaje

1. Aplicar el espíritu crítico y el rigor para validar o refutar argumentos tanto propios como de otros.
2. Conocer los resultados básicos de la seguridad en la información y la criptografía.
3. Evaluar de manera crítica y con criterios de calidad el trabajo realizado.
4. Identificar los parámetros que determinan el funcionamiento de un sistema.
5. Que los estudiantes hayan demostrado poseer y comprender conocimientos en un área de estudio que parte de la base de la educación secundaria general, y se suele encontrar a un nivel que, si bien se apoya en libros de texto avanzados, incluye también algunos aspectos que implican conocimientos procedentes de la vanguardia de su campo de estudio.
6. Que los estudiantes hayan desarrollado aquellas habilidades de aprendizaje necesarias para emprender estudios posteriores con un alto grado de autonomía.
7. Que los estudiantes sepan aplicar sus conocimientos a su trabajo o vocación de una forma profesional y posean las competencias que suelen demostrarse por medio de la elaboración y defensa de argumentos y la resolución de problemas dentro de su área de estudio.
8. Que los estudiantes tengan la capacidad de reunir e interpretar datos relevantes (normalmente dentro de su área de estudio) para emitir juicios que incluyan una reflexión sobre temas relevantes de índole social, científica o ética.
9. Trabajar cooperativamente en un contexto multidisciplinar asumiendo y respetando el rol de los diferentes miembros del equipo.
10. Utilizar eficazmente bibliografía y recursos electrónicos para obtener información.
11. Utilizar métodos numéricos para resolver problemas en criptografía y seguridad.

## Contenido

- Introducción a la criptografia.
- Fundamentos matemáticos de la criptografia.
- Criptografia de clave simétrica.
- Funciones hash.
- Criptografia de clave pública.
- Infrastructuras de clave pública.
- Comunicación y transmisión de datos seguros.
- Analisis de datos cifrados.

## Metodología

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.

## Actividades

| Título | Horas | ECTS | Resultados de aprendizaje |
|---|---|---|---|
| Tipo: Dirigidas | | | |
| Seminarios / prácticas | 15 | 0,6 | |
| Sesiones de problemas | 15 | 0,6 | |
| Sesiones de teoria | 30 | 1,2 | |
| Tipo: Supervisadas | | | |
| Preparación de sesions | 15 | 0,6 | |
| Tutorias | 15 | 0,6 | |
| Tipo: Autónomas | | | |
| Estudio / preparación examen | 22,5 | 0,9 | |
| Trabajo personal | 30 | 1,2 | |

## Evaluación

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 4.5.
- 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 algún caso práctico o práctica durante el curso. Nota mínima de cada práctica por separado: 4.5.

Para poder aprobar la asignatura es necesario que la evaluación de cada una de las partes supere el mínimo exigido y que la evaluación total supere los 5 puntos sobre 10.

En caso de no superar la asignatura debidoa que alguna de las actividades de evaluación no alcanza la nota mínima requerida, la nota numérica del expediente será el valor menor 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 porseparado. 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 sístensis 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 possibles incidencias. Siempre se informará en el campus virtual sobre estos cambios ya que se entiende es el mecanismo habitual de intercambio deinformación entre el profesorado y el alumnado.

Así mismo, se detallarán con suficiente tiempo de antelación los mecanismos de evaluación, metodología o funcionamiento general de la asignatura que no se hayan concretado en esta guía.

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).

## Actividades de evaluación

| Título | Peso | Horas | ECTS | Resultados de aprendizaje |
|---|---|---|---|---|
| Examenes parciales | 45 | 3 | 0,12 | 1, 3, 2, 4, 5, 6, 7, 8, 10, 11 |
| Problemas y ejercicios | 15 | 1,5 | 0,06 | 1, 3, 2, 4, 5, 6, 7, 8, 9, 10, 11 |
| Prácticas / seminarios | 40 | 3 | 0,12 | 1, 3, 2, 4, 5, 6, 7, 8, 9, 10, 11 |

## Bibliografía


- Jordi Herrera-Joancomartí, Cristina Pérez-Solà, (2021) Criptografia.
- 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://cataleg.uab.cat/iii/encore/record/C__Rb1956470
- Smart, N. P., *Cryptography Made Simple*. Springer International Publishing, 2016. https://doi.org/10.1007/978-3-319-21936-3. Biblioteca UAB: https://cataleg.uab.cat/iii/encore/record/C__Rb1980662


## 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.