UAB
Universitat Autònoma de Barcelona

Seguridad y Privacidad de Datos

Código: 106568
Créditos ECTS: 6

2024/2025

Titulación	Tipo	Curso
2504392 Inteligencia Artificial / Artificial Intelligence	OT	3
2504392 Inteligencia Artificial / Artificial Intelligence	OT	4

Contacto

Nombre: Cristina Perez Sola

Correo electrónico: cristina.perez@uab.cat

Equipo docente

Guillermo Navarro Arribas

Idiomas de los grupos

Puede consultar esta información al final del documento.

Prerrequisitos

Para un mejor seguimiento del curso, se recomienda tener habilidades básicas de programación adquiridas en los cursos previos de "Fundamentos de Programación".

Objetivos y contextualización

Este curso cubre los principios fundamentales de la seguridad de los datos y la privacidad mediante la criptografía, proporcionando una comprensión exhaustiva tanto de los métodos criptográficos clásicos como de los modernos, y cómo aplicarlos para proteger los datos en diferentes escenarios del mundo real.

Competencias

Inteligencia Artificial / Artificial Intelligence

- Analizar y resolver problemas de forma efectiva, generando propuestas innovadoras y creativas para alcanzar los objetivos.
- Conocer y utilizar de forma eficiente las técnicas y herramientas de representación, manipulación, análisis y gestión de datos a gran escala.

Resultados de aprendizaje

1. Analizar y resolver problemas de forma efectiva, generando propuestas innovadoras y creativas para alcanzar los objetivos.
2. Comprender como funciona una infraestructura de clave pública.
3. Conocer el funcionamiento de la criptografía simétrica y asimétrica.
4. Conocer los principales modelos de privacidad de datos, sus limitaciones y su aplicación a la publicación y tratamiento de datos.
5. Conocer los riesgos de las comunicaciones en Internet.

Contenido

- Unidad 1: Introducción a la Criptografía y Fundamentos Matemáticos
- Unidad 2: Criptosistemas Clásicos
- Unidad 3: Criptografía de Clave Simétrica
- Unidad 4: Funciones Hash
- Unidad 5: Criptografía de Clave Pública
- Unidad 6: Infraestructura de Clave Pública
- Unidad 7: Seguridad y Privacidad en el Aprendizaje Automático

Actividades formativas y Metodología

Título	Horas	ECTS	Resultados de aprendizaje
Tipo: Dirigidas			
Actividades prácticas / laboratorios	12	0,48	1, 2, 3, 4, 5
Clases de problemas	12	0,48	1, 2, 3, 4, 5
Clases de teoria	26	1,04	2, 3, 4
Tipo: Supervisadas			
Tutorías y consultas	14	0,56	1, 2, 3, 4, 5
Tipo: Autónomas			
Preparación de exámenes	25	1	1, 2, 3, 4, 5
Preparación de problemas y prácticas	25	1	1, 2, 3, 4, 5
Trabajo personal	25	1	1, 2, 3, 4, 5

El canal oficial de comunicación entre estudiantado y profesorado es el Campus Virtual de la UAB.

Las clases teóricas se basarán en lecciones magistrales, aunque se fomentará la participación del estudiantado en la resolución de ejemplos, etc. En las clases de resolución de problemas, se seguirá una lista de ejercicios para que el estudiantado intente resolverlos por su cuenta. Se fomentará que el estudiantado presente sus enfoques de resolución de problemas. Las sesiones prácticas profundizarán en temas relacionados: escenarios del mundo real, ampliación de temas específicos con técnicas y algoritmos alternativos a los ya tratados.

A lo largo del curso, se llevarán a cabo las siguientes actividades:

- Clases teóricas: Se presentará la teoría con varios ejemplos de ejercicios, y se hará un esfuerzo por fomentar la participación del estudiantado en su resolución.
- Clases de resolución de problemas: Estas son sesiones con todo el grupo o grupos pequeños orientadas a aplicar la teoría a la resolución de problemas. El estudiantado dispondrá de una lista de problemas para resolver. En algunos casos, el profesorado puede solicitar soluciones a los ejercicios antes del seminario y discutir su resolución durante estas sesiones. Estas sesiones pretenden promover habilidades analíticas y sintéticas, razonamiento crítico, resolución de problemas y trabajo en equipo.
- Sesiones prácticas: Profundizarán en los temas relacionados con los tratados en teoría. Se hará hincapié en los escenarios del mundo real, ampliando temas específicos con técnicas y algoritmos alternativos.
- Sesiones de presentación de proyectos: Durante el curso, el estudiantado realizará un proyecto en grupo sobre el tema final de la asignatura. En las sesiones de presentación de proyectos, una parte del estudiantado presentará su trabajo mientras otros escucharán y harán preguntas. Los temas presentados durante las sesiones de presentación de proyectos también serán evaluados en los exámenes de la asignatura.

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
Actividades prácticas / laboratorios	3	2	0,08	1, 2, 3, 4, 5
Exámenes	5	3	0,12	1, 2, 3, 4, 5
Resolución de ejercicios	1	4	0,16	1, 2, 3, 4, 5
Trabajo final	1	2	0,08	1, 2, 3, 4, 5

Las fechas para las actividades de evaluación continua se publicarán en el campus virtual y en las diapositivas de presentación del curso. Estas fechas pueden estar sujetas a reprogramación debido a posibles incidentes. Cualquier cambio siempre se comunicará a través del campus virtual de la UAB, ya que se entiende que es la plataforma habitual de intercambio de información entre el profesorado y el estudiantado.

La evaluación del curso, sobre 10 puntos, se llevará a cabo de la siguiente manera:

- Exámenes (5 puntos): Dos exámenes parciales individuales para un total de 5 puntos (2,5 puntos cada uno). Como parte de la evaluación continua, estas pruebas se realizarán durante las sesiones de clase. Cada prueba evaluará una parte del temario, y la nota final será la media aritmética de las dos pruebas. Cada prueba solo se promediará si se califica con más de 4 sobre 10. Si alguna de las pruebas no obtiene más de 4, los exámenes parciales se considerarán suspendidos.
- Ejercicios (1 punto): Como parte de la evaluación continua, el estudiantado deberá entregar las soluciones a las actividades o ejercicios propuestos a lo largo del curso.
- Actividades de laboratorio (3 puntos): Como parte de la evaluación continua, algunas actividades de laboratorio deberán completarse en el Laboratorio Integrado. Cada actividad de laboratorio solo se

promediará si se califica con más de 4 sobre 10. Si alguna de las actividades de laboratorio no obtiene más de 4, las actividades de laboratorio se considerarán suspendidas. El promedio de las calificaciones de las actividades de laboratorio debe ser superior a 5 sobre 10 para aprobar el curso.
- Proyecto final (1 punto): Se deberá hacer un informe escrito y una presentación oral y defensa del proyecto final.

El estudiantado que haya suspendido la parte teórica del curso tendrá la opción de realizar el examen final, que cubrirá todo el temario del curso, independientemente de las puntuaciones obtenidas en los exámenes parciales. La calificación de este examen de recuperación se considerará como la nota de los exámenes para el cálculo de la nota final del curso, representando el 50% de la nota final del curso. Para aprobar el curso, la calificación del examen de recuperación debe ser superior a 5 sobre 10. El estudiantado que desee mejorar sus calificaciones de los exámenes parciales puede realizar el examen final para la mejora de la nota. En este caso, presentar el examen y que este sea calificado por el profesorado sustituirá las calificaciones de exámenes anteriores.

La entrega de ejercicios, actividades de laboratorio y el proyecto final no se pueden recuperar.

Para cada actividad de evaluación, se indicará un lugar, fecha y hora de revisión, durante la cual el estudiantado podrá revisar la actividad con el profesorado. En este contexto, se pueden hacer reclamaciones sobre la calificación de la actividad, que serán evaluadas por el profesorado del curso. Si una persona no asiste a esta revisión, la actividad no se revisará posteriormente.

Este curso no incluye un sistema de evaluación única.

Los estudiantes que hayan cursado la asignatura anteriormente y hayan aprobado las actividades de laboratorio podrán conservar sus notas de laboratorio. Sin embargo, es importante que se pongan en contacto con los profesores de laboratorio al inicio del curso (cuando se formen los grupos de prácticas) para informarles de esto. En ningún caso se conservarán las notas de los exámenes teóricos, la presentación de problemas ni el proyecto final de cursos anteriores.

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

- Copia total o parcial de una práctica, informe o cualquier otra actividad de evaluación;
- Permitir que otros copien;
- Presentar un trabajo en grupo no realizado íntegramente por los miembros del grupo;
- Uso no autorizado de IA (por ejemplo, Copilot, ChatGPT o equivalentes) para resolver ejercicios, prácticas y/o cualquier otra actividad evaluable;
- Presentar como propios materiales creados 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, relojes inteligentes, etc.) accesibles durante las pruebas de evaluación teórico-prácticas individuales (exámenes);
- Hablar con compañeros durante las pruebas de evaluación teórico-prácticas individuales (exámenes);
- Copiar o intentar copiar de otros estudiantes durante las pruebas de evaluación teórico-prácticas (exámenes);
- Utilizar o intentar utilizar escritos relacionados con la materia durante las pruebas de evaluación teórico-prácticas (exámenes), cuando estos no hayan sido explícitamente permitidos.

En futuras ediciones de este curso, los estudiantes que hayan cometido irregularidades en un acto de evaluación no tendrán ninguna de sus actividades de evaluación convalidadas. En resumen: copiar, permitir copiar o plagiar (o intentar cualquiera de estas acciones) en cualquiera de las actividades de evaluación resulta en una suspensión inmediata, no compensable, y sin convalidación de partes del curso en años posteriores.

Los estudiantes que consigan el número mínimo de puntos para aprobar la asignatura pero no alcancen la nota mínima en alguna de las actividades de evaluación serán calificados con una nota final de 4,5. Si la asignatura no se aprueba debido a una calificación de cero en una actividad por copia, la nota final del curso será de 3, lo que no permitirá compensar la asignatura.

Finalmente, los estudiantes que no asistan a ninguna prueba individual (exámenes parciales y el examen final) recibirán una calificación de "No Evaluado." La participación en cualquiera de estas actividades de evaluación resultará en una calificación diferente de "No Evaluado."

Ninguna actividad de evaluación se realizará en un momento diferente del horario establecido a menos que haya una causa justificada, previa notificación antes de la actividad, y consentimiento del profesor. En cualquier otro caso, si un estudiante no asiste a una actividad, esta no podrá ser recuperada.

Con respecto a las calificaciones de honor, estas pueden otorgarse a los estudiantes que hayan aprobado la asignatura con una nota final de 9 o superior. Dado que el número de calificaciones de honor no puede exceder el 5% de los estudiantes matriculados, se otorgarán a aquellos con las calificaciones más altas.Encaso de empate, se considerarán las soluciones propuestas en cada una de las actividades de evaluación realizadas a lo largo del curso.

Bibliografía

- Cristina Pérez-Solà and Jordi Herrera Joancomartí. *La criptografia que et cal saber*. (2023) Available on-line: https://criptografia.cat/
- Christof Paar and Jan Pelzl. *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
- Nigel P. Smart. *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

Las actividades de laboratorio del curso se desarrollarán utilizando Python.

Lista de idiomas

Nombre	Grupo	Idioma	Semestre	Turno
(PAUL) Prácticas de aula	1	Inglés	primer cuatrimestre	tarde
(TE) Teoría	1	Inglés	primer cuatrimestre	tarde