UAB
Universitat Autònoma de Barcelona

# Seguretat i Privacitat de Dades

Codi: 106568
Crèdits: 6

2024/2025

| Titulació | Tipus | Curs |
|---|---|---|
| 2504392 Intel·ligència Artificial / Artificial Intelligence | OT | 3 |
| 2504392 Intel·ligència Artificial / Artificial Intelligence | OT | 4 |

## Professor/a de contacte

Nom: Cristina Perez Sola

Correu electrònic: cristina.perez@uab.cat

## Equip docent

Guillermo Navarro Arribas

## Idiomes dels grups

Podeu consultar aquesta informació al final del document.

## Prerequisits

Per a un millor seguiment del curs, es recomana tenir coneixements bàsics de programació adquirits en els cursos anteriors de "Fonaments de la Programació".

## Objectius

Aquest curs cobreix els principis fonamentals de la seguretat de les dades i la privacitat mitjançant la criptografia, proporcionant una comprensió exhaustiva tant dels mètodes criptogràfics clàssics com dels moderns, i com aplicar-los per protegir les dades en diferents escenaris del món real.

## Competències

Intel·ligència Artificial / Artificial Intelligence

- Analitzar i resoldre problemes de manera efectiva, i generar propostes innovadores i creatives per aconseguir els objectius.
- Conèixer i utilitzar de manera eficient les tècniques i eines de representació, manipulació, anàlisi i gestió de dades a gran escala.

## Resultats d'aprenentatge

1. Analitzar i resoldre problemes de manera efectiva, i generar propostes innovadores i creatives per aconseguir els objectius.
2. Comprendre com funciona una infraestructura de clau pública.
3. Conèixer el funcionament de la criptografia simètrica i asimètrica.
4. Conèixer els principals models de privacitat de dades, les seves limitacions i la seva aplicació a la publicació i tractament de dades.
5. Conèixer els riscos de les comunicacions a internet.

## Continguts

- Unitat 1: Introducció a la Criptografia i Fonaments Matemàtics
- Unitat 2: Criptosistemes Clàssics
- Unitat 3: Criptografia de Clau Simètrica
- Unitat 4: Funcions de Hash
- Unitat 5: Criptografia de Clau Pública
- Unitat 6: Infraestructura de Clau Pública
- Unitat 7: Seguretat i Privacitat en l'Aprenentatge Automàtic

## Activitats formatives i Metodologia

| Títol | Hores | ECTS | Resultats d'aprenentatge |
|---|---|---|---|
| Tipus: Dirigides | | | |
| Activitats pràctiques / laboratoris | 12 | 0,48 | 1, 2, 3, 4, 5 |
| Classes de problemes | 12 | 0,48 | 1, 2, 3, 4, 5 |
| Classes de teoria | 26 | 1,04 | 2, 3, 4 |
| Tipus: Supervisades | | | |
| Tutories i consultes | 14 | 0,56 | 1, 2, 3, 4, 5 |
| Tipus: Autònomes | | | |
| Preparació d'exàmens | 25 | 1 | 1, 2, 3, 4, 5 |
| Preparació de problemes i pràctiques | 25 | 1 | 1, 2, 3, 4, 5 |
| Treball personal | 25 | 1 | 1, 2, 3, 4, 5 |

El canal oficial de comunicació entre l'estudiantat i el professorat és el Campus Virtual de la UAB.

Les classes teòriques es basaran en lliçons magistrals, tot i que es fomentarà la participació de l'estudiantat en la resolució d'exemples, etc. A les classes de resolució de problemes, se seguirà una llista d'exercicis perquè l'estudiantat els intenti resoldre pel seu compte. Es fomentarà que l'estudiantat presenti els seus enfocaments de resolució de problemes. Les sessions pràctiques aprofundiran en temes relacionats: escenaris del món real, ampliació de temes específics amb tècniques i algoritmes alternatius als ja tractats.

Al llarg del curs, es realitzaran les següents activitats:

- Classes teòriques: Es presentarà la teoria amb diversos exemples d'exercicis, i es fomentarà la participació de l'estudiantat en la seva resolució.
- Classes de resolució de problemes: Aquestes són sessions amb tot el grup o grups petits orientades a aplicar la teoria a la resolució de problemes. L'estudiantat disposarà d'una llista de problemes a resoldre. En alguns casos, el professorat pot demanar solucions als exercicis abans del seminari i discutir-ne la resolució durant aquestes sessions. Aquestes sessions pretenen promoure habilitats analítiques i sintètiques, raonament crític, resolució de problemes i treball en equip.
- Sessions pràctiques: Aprofundiran en els temes relacionats amb els coberts a la teoria. Es farà èmfasi en els escenaris del món real, ampliant temes específics amb tècniques i algoritmes alternatius.
- Sessions de presentació de projectes: Durant el curs, l'estudiantat realitzarà un projecte engrup sobre el tema final de l'assignatura. En les sessions de presentació de projectes, una part de l'estudiantat presentarà el seu treball mentre altres escoltaran i faran preguntes. Els temes presentats durant les sessions de presentació de projectes també seran avaluats en els exàmens de l'assignatura.

Nota: es reservaran 15 minuts d'una classe, dins del calendari establert pel centre/titulació, per a la complementació per part de l'alumnat de les enquestes d'avaluació de l'actuació del professorat i d'avaluació de l'assignatura/mòdul.

## Avaluació

## Activitats d'avaluació continuada

| Títol | Pes | Hores | ECTS | Resultats d'aprenentatge |
|---|---|---|---|---|
| Activitats pràctiques / laboratoris | 3 | 2 | 0,08 | 1, 2, 3, 4, 5 |
| Exàmens | 5 | 3 | 0,12 | 1, 2, 3, 4, 5 |
| Resolució d'exercicis | 1 | 4 | 0,16 | 1, 2, 3, 4, 5 |
| Treball final | 1 | 2 | 0,08 | 1, 2, 3, 4, 5 |

Les dates per a les activitats d'avaluació continuada es publicaran al campus virtual i a les diapositives de presentació del curs. Aquestes dates poden estar subjectes a reprogramació a causa de possibles incidents. Qualsevol canvi es comunicarà sempre a través del campus virtual de la UAB, ja que es considera la plataforma habitual d'intercanvi d'informació entre professorat i estudiantat.

L'avaluació del curs, sobre 10 punts, es durà a terme de la següent manera:

- Exàmens (5 punts): Dos exàmens parcials individuals per a un total de 5 punts (2,5 punts cadascun). Com a part de l'avaluació continuada, aquestes proves es duran a terme durant les sessions de classe. Cada prova avaluarà una part del temari, i la nota final serà la mitjana aritmètica de les dues proves. Cada prova només farà mitjana si es qualifica amb més de 4 sobre 10. Si alguna de les proves no obté més de 4 punts, els exàmens parcials es consideraran suspesos.
- Exercicis (1 punt): Com a part de l'avaluació continuada, els estudiants hauran de lliurar les solucions a les activitats o exercicis proposats al llarg del curs.
- Activitats de laboratori (3 punts): Com a part de l'avaluació continuada, algunes activitats de laboratori s'hauran de completar al Laboratori Integrat. Cada activitat de laboratori només farà mitjana si es qualifica amb més de 4 sobre 10. Si alguna de les activitats de laboratori no obté més de 4 punts, les activitats de laboratori es consideraran suspeses. La mitjana de les qualificacions de les activitats de laboratori ha de ser superior a 5 sobre 10 per aprovar el curs.
- Projecte final (1 punt): S'haurà de fer un informe escrit i una presentació oral i defensa del projecte final.

L'estudiantat que hagi suspès la part teòrica del curs tindran l'opció de fer l'examen final, que cobrirà tot el temari del curs, independentment de les puntuacions obtingudes als exàmens parcials. La nota d'aquest examen de recuperació es considerarà com la qualificació dels exàmens per al càlcul de la nota final del curs, representant el 50% de la nota final del curs. Per aprovar el curs, la qualificació de l'examen de recuperació ha de ser superior a 5 sobre 10. L'estudiantat que desitgi millorar les seves qualificacions dels exàmens parcials pot fer l'examen final per a la millora de la nota. En aquest cas, presentar l'examen i que aquest sigui qualificat pel professorat substituirà les qualificacions d'exàmens anteriors.

El lliurament d'exercicis, activitats de laboratori i el projecte final no es poden recuperar.

Per a cada activitat d'avaluació, s'indicarà un lloc, data i hora de revisió, durant la qual l'estudiantat podrà revisar l'activitat amb el professorat. En aquest context, es poden fer reclamacions sobre la qualificació de l'activitat, que seran avaluades pel professorat del curs. Si una persona no assisteix a aquesta revisió, l'activitat no es revisarà posteriorment.

Aquest curs no inclou un sistema d'avaluació única.

---

L'estudiantat que hagi cursat el curs anteriorment i hagi aprovat les activitats de laboratori podrà conservar les seves notes de laboratori. No obstant això, és important que contactin amb el professorat de laboratori a l'inici del curs (quan es formin els grups de pràctiques) per informar-los d'això. En cap cas es conservaran les notes dels exàmens teòrics, la presentació de problemes ni el projecte final de cursos anteriors.

Sense perjudici d'altres mesures disciplinàries que es considerin oportunes, i d'acordamb la normativa acadèmica vigent, les irregularitats comeses per un estudiant que puguin conduir a una variació de la nota es qualificaran amb un zero (0). Les activitats d'avaluació qualificades d'aquesta manera i per aquest procediment no seran recuperables. Si aprovar qualsevol d'aquestes activitats d'avaluació és necessari per aprovar el curs, el curs serà directament suspès, sense oportunitat de recuperar-lo en el mateix curs acadèmic. Aquestes irregularitats inclouen, entre altres:

- Còpia total o parcial d'una pràctica, informe o qualsevol altra activitat d'avaluació;
- Permetre que altres copiïn;
- Presentar un treball en grup no fet íntegrament pels membres del grup;
- Ús no autoritzat d'IA (per exemple, Copilot, ChatGPT o equivalents) per resoldre exercicis, pràctiques i/o qualsevol altra activitat avaluable;
- Presentar com a propis materials creats per un tercer, encara que siguin traduccions o adaptacions, i en general, treballs amb elements no originals i exclusius de l'estudiant;
- Tenir dispositius de comunicació (com telèfons mòbils, rellotges intel·ligents, etc.) accessibles durant les proves d'avaluació teòrico-pràctiques individuals (exàmens);
- Parlar amb companys durant les proves d'avaluació teòrico-pràctiques individuals (exàmens);
- Copiar o intentar copiar d'altres estudiants durant les proves d'avaluació teòrico-pràctiques (exàmens);
- Utilitzar o intentar utilitzar escrits relacionats amb la matèria durant les proves d'avaluació teòrico-pràctiques (exàmens), quan aquests no han estat explícitament permesos.

En futures edicions d'aquest curs, els estudiants que hagin comès irregularitats en un acte d'avaluació no tindran cap deles seves activitats d'avaluació convalidades. En resum: copiar, permetre copiar o plagi (o intentar qualsevol d'aquestes accions) en qualsevol de les activitats d'avaluació resulta en una suspensió immediata, no compensable, i sense convalidació de parts del curs en anys posteriors.

Els estudiants que aconsegueixin el nombre mínim de punts per aprovar el curs però no arribin a la nota mínima en alguna de les activitats d'avaluació seran qualificats amb una nota final de 4,5. Si el curs no s'aprova a causa d'una nota de zero en una activitat per còpia, la nota final del curs serà de 3, la qual cosa no permetrà compensar el curs.

Finalment, els estudiants que no assisteixin a cap prova individual (exàmens parcials i l'examen final) rebran una qualificació de "No Avaluable." La participació en qualsevol d'aquestes activitats d'avaluació resultarà en una qualificació diferent de "No Avaluable."

Cap activitat d'avaluació es realitzarà en un moment diferent de l'horari establert, tret que hi hagi una causa justificada, prèvia notificació abans de l'activitat, i consentiment del professor. En qualsevol altre cas, si un estudiant no assisteix a una activitat, aquesta no es podrà recuperar.

Pel que fa a les qualificacions d'honors, aquestes es poden atorgar als estudiants que hagin aprovat el curs amb una nota final de 9 o superior. Atès que el nombre de qualificacions d'honors no pot superar el 5% dels estudiants matriculats, s'atorgaran als que tinguin les notes més altes. En cas d'empat, es consideraran les solucions proposades en cadascuna de les activitats d'avaluació realitzades al llarg del curs.

## Bibliografia


- 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


## Programari

Les activitats de laboratori del curs es desenvoluparan utilitzant Python.

## Llista d'idiomes

| Nom | Grup | Idioma | Semestre | Torn |
|---|---|---|---|---|
| (PAUL) Pràctiques d'aula | 1 | Anglès | primer quadrimestre | tarda |
| (TE) Teoria | 1 | Anglès | primer quadrimestre | tarda |