

## Seguretat computacional

| Codi  | Tipus                 | Curs/Semestre | Crèdits |
|-------|-----------------------|---------------|---------|
| 20375 | Optativa<br>Semestral | 4rt / 1r      | 6       |

## Objectius

---

### Competències específiques

#### Coneixements

- Introduir el tema de la seguretat en sistemes informàtics i les seves components legals, polítiques, administratives, físiques i, també, lògiques.
- Introduir a l'alumne al concepte de la seguretat en sistemes operatius, concretament a través del UNIX i Windows NT.
- Introduir a l'alumne en els fonaments matemàtics i tècniques utilitzades per a la protecció de la informació en sistemes informàtics.
- Donar a l'alumne els coneixements necessaris per a l'aplicació de mètodes i algorismes de protecció de la informació, tant des de la seva vessant clàssica com moderna.
- Donar a l'alumne els coneixements necessaris per a l'aplicació dels mètodes i tècniques criptogràfiques adients, tant en criptosistemes de clau pública com privada.
- Introduir el concepte de protocol i, en general, esquemes de seguretat per a resoldre problemes d'autenticació, accés compartit, criptografia *scrow*, distribució i gestió de claus, proves d'identificació, proves de coneixement nul, etc.
- Aprendre a utilitzar *software* apropiat per la construcció i l'administració d'infraestructures de clau pública (PKI).

Pel que fa als aspectes específics de les pràctiques:

- Utilitzar d'eines per garantir la seguretat en màquines amb sistemes operatius Linux. Es veuran algunes de les solucions criptogràfiques adoptades per aquests sistemes per garantir la seguretat.
- Veure el funcionament de l'arquitectura de proveïdors criptogràfics de JAVA. Treballar amb eines per utilitzar criptografia de clau pública i certificats Digitals. Comunicacions segures amb SSL.

#### Habilitats

### Competències genèriques

## Capacitats prèvies

---

## Continguts

---

|              |  |
|--------------|--|
| Introducció. |  |
|--------------|--|

- Objectius, Vulnerabilitats i amenaces.
- Mesures de seguretat: legals, polítiques, administratives, físiques i lògiques.
- La seguretat en els sistemes d'informació.

**Fonaments teòrics de la criptografia.**

- Definicions generals.
- Teoria de la informació: entropia i informació mutua.
- Teoria del secret perfecte - Shannon (1949).
- Teoria de l'autenticitat perfecta - Simmons (1984).

**Previs d'aritmètica modular.**

- L'algorisme de les divisions successives: mcd, algoritme d'Euclides, teorema de Bezout, càlcul d'inversos.
- Teorema xinès dels residus.
- Teorema de Dirichlet.
- Aritmètica i nombres primers: Funció d'Euler, teorema d'Euler i Fermat, tests de primalitat (Fermat-Euler, Miller).

**Criptografia de clau privada: Criptosistemes històrics.**

- Mètodes criptogràfics elementals.
- Criptografia clàssica.

**Criptografia de clau privada: Criptosistemes en flux.**

- Seqüències pseudoaleatòries.
- Generadors lineals: LFSR (Linear Feedback Shift Register).
- Generadors no lineals.

**Criptografia de clau privada. Criptosistemes de bloc.**

- L'estàndard DES.
- L'estàndard AES (Rijndael).
- Modes d'operació dels xifratges en bloc.

**Criptografia de clau pública.**

- Definicions generals.
- Funcions unidireccionals.
- Criptosistema RSA

- Criptosistema ElGamal
- Problemes NP. Criptosistema Knapsak
- Criptosistema McEliece
- Criptosistemes probabilístics

#### Signatures digitals i PKI.

- Definicions i propietats.
- Signatura amb RSA.
- Signatura amb ElGamal.
- DSS-DSA.
- Funcions *Hash*.
- Standards de funcions *hash*.
- Infraestructures de clau pública (PKI).

#### Protocols criptogràfics.

- Intercanvi de claus de Diffie-Hellman.
- Protocol de tres-passes de Shamir.
- Protocols d'autenticació.
- Estratègies d'atacs i vulnerabilitats clàssiques dels protocols.
- Esquemes de compartició de secrets.
- Diners digitals utilitzant signatures digitals.

## Metodologia docent

---

L'assignatura consta de classes amb exposició oral on el professor explica el contingut de l'assignatura i sessions de problemes, amb grups més reduïts, que permeten exercitar els continguts pràctics que s'imparteixen en l'assignatura. Addicionalment, per aquella temàtica que requereix un nivell de treball pràctic més elevat es realitzen sessions en el laboratori exclusivament pràctiques. L'objectiu d'aquestes sessions de laboratori són que l'estudiant es familiaritzi amb el software criptogràfic i de seguretat que implementa els conceptes teòrics que s'han explicat en la teoria i s'han exemplificat amb els problemes.

Els aspectes metodològics i organitzatius més rellevants de les pràctiques es descriuen a continuació:

- Les pràctiques es fan en grups de 2 persones.
- Per apuntar-se a pràctiques cal fer servir l'aplicació de pràctiques de la Web del dEIC (Docència -> pràctiques). Cada alumne s'ha de registrar i després triar el grup on vol anar (A, B, C, D, E, o F).
- És **obligada** l'assistència a totes les sessions de pràctiques (laboratori tancat).
- A principi de curs caldrà lliurar al professor de pràctiques el **full de compromís ètic**.
- Per poder accedir al laboratori **cal lliurar l'informe previ** que acompanya l'enunciat. No presentar aquest informe impossibilitarà l'accés al laboratori, i quedarà la pràctica suspesa.
- Cada pràctica té destinada una sessió de laboratori. La correcció d'aquesta pràctica es farà al llarg de la següent sessió de laboratori. **Dues hores abans** de la sessió d'entrega es farà una còpia automàtica del vostre directori de la pràctica. Durant la segona hora de la sessió es farà la correcció ràpida de la pràctica, directament de la còpia que s'ha fet. **En cap cas s'admetran modificacions de la pràctica**

que s'està evaluant.

- Es farà una **prova de validació per cada una de les pràctiques** per evaluar si s'ha treballat en elles i si s'han assolit els coneixements i habilitats associades. Si se suspén la part de la prova associada a una pràctica, la pràctica queda suspesa. Aquesta prova de validació es farà juntament amb la prova de validació de teoria.
- La recuperació de pràctiques en segona convocatòria es farà el mes d' **abril**. La data exacta es farà pública al fòrum de l'assignatura en finalitzar el primer semestre.
- Per recuperar les pràctiques caldrà presentar-les de nou amb les parts opcionals obligatòriament i fer una nova prova de validació.

Les pràctiques es puntuaran sobre 10.

## Avaluació

| 1a convocatòria (febrer/juny)  |  | 2a convocatòria (juliol/setembre)   |
|--|--|---|
| Avaluació en grups   | Avaluació individual   |   |
| L'avaluació en grup d'aquesta assignatura fa referència a la part pràctica. Les pràctiques es realitzaran en grups de dues persones i la seva avaluació seguirà un model d'avaluació continuada. Els alumnes lliuraran cada una de les pràctiques al llarg del curs dins dels terminis establerts. Si no es lliuren totes i cada una de les pràctiques previstes, l'alumne té un no presentat. | La part teòrica i de problemes d'aquesta assignatura té una avaluació individual i no segueix un model d'avaluació continuada. L'avaluació es realitza per mitjà d'un examen final. Si l'alumne no es presenta a l'examen final obté un no presentat com a qualificació. | La segona convocatòria de pràctiques consisteix en el lliurament de totes les pràctiques complertes (incloent les parts opcionals). La segona convocatòria de teoria/problemes consisteix en un examen. En els dos casos, si s'ha aprovat una part, la nota es conserva per a la segona convocatòria. |

## Bibliografia bàsica

- Josep Domingo i Ferrer and Jordi Herrera i Joancomartí, Criptografia per als Serveis Telemàtics i el Comerç Electrònic, Col·lecció Manuals no. 31, Barcelona: Editorial UOC, 1999. ISBN 84-8429-007-7.
- A. Menezes, P. van Oorschot and S. Vanstone.: Handbook of Applied Cryptography, CRC Press. (1996). Available at <http://www.cacr.math.uwaterloo.ca/hac>.
- Rifà, J.: Seguretat Computacional. Materials, 21. Servei de Publicacions de la UAB. 1998.

## Bibliografia complementària

- An Introduction to Computer Security: The NIST Handbook. Special Publication 800-12. NIST(1995).

<http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf>

- Rifà, J. i Huguet, L.: Comunicació Digital. Masson Ed. (1991).
- Robling Denning D.E.: Cryptography and Data Security. Addison-Wesley Publishing Company (1988).
- Schneier, B.: Applied Cryptography, John Wiley and Sons, Inc. 1996.
- Simmons, G.S.: Contemporary Cryptology. The Science of Information Integrity, IEEE Press (1991).
- Anderson, R.: Security Engineering: A Guide to Building Dependable Distributed System, Wiley (2001).
- Pfleeger, C.P.: Security in Computing. , Prentice Hall (1997).
- V. Shoup. : A computational Introduction tonumber theory and Algebra. <http://shoup.net/ntb/>

## Enllaços

---

[Applet que simula un LFSR](#)

[RSA Security](#)

[RSA Laboratories' Frequently Asked](#)

[Questions About Today's Cryptography,](#)

[Version 4.1](#)

[CryptoBytes Technical Newsletter](#)

[Prime pages](#)

[Applet amb implementació de l?AES](#)

<http://www.eecircle.com/applets/009/LFSR.html>

<http://www.rsasecurity.com/>

<http://www.rsasecurity.com/rsalabs/faq/index.html>

<http://www.rsa.com/rsalabs/cryptobytes/index.html>

<http://primes.utm.edu/>

<http://www.lapo.it/AES.html>