	ENSENYAMENT D'ENGINYERIA INFORMÀTICA (2n cicle)		
	ASSIGNATURA: Seguretat Computacional (Bloc de Comerç Electrònic i Telemàtica)		
	PROFESSOR/A RESPONSABLE: Magda Valls		
	CURS: 2n	**CRÈDITS: 6**	**TIPUS: Optatiu**

1. OBJECTIUS

L'assignatura de *Seguretat Computacional* forma part del bloc de *Comerç Electrònic i Telemàtica*. Els mecanismes de seguretat esdevenen imprescindibles per al disseny d'aplicacions de comerç electrònic. En aquest sentit, en aquesta assignatura es pretén iniciar a l'estudiant en les tècniques criptogràfiques bàsiques necessàries per a la implementació d'aplicacions segures. Els objectius concrets de l'assignatura són:

- Aportar a l'estudiant coneixements bàsics sobre els fonaments matemàtics en els que es sustenta la seguretat dels criptosistemes actuals
- Oferir una visió general de les tècniques i algorismes criptogràfics emprats en l'actualitat
- Mostrar com es poden combinar els diferents procediments criptogràfics per tal de garantir diferents nivells de seguretat: confidencialitat, autenticitat, integritat i no repudi

2. ESTRUCTURA

Aquesta assignatura consta de 6 crèdits. D'aquests, 4.5 s'imparteixen de forma presencial i 1.5 estan dedicats al seguiment virtual de l'assignatura. Pel que fa als crèdits presencials, 3 estaran adreçats a classes teòriques i 1.5 a problemes.

3. PROGRAMA

- *Introducció.*
- *Fonaments matemàtics de la criptografia. (Introducció a la teoria de nombres. Introducció a la complexitat computacional. Problemes difícils. Generació de seqüències aleatòries).*
- *Criptografia simètrica clàssica. (Criptosistemes simètrics, esquemes de xifrat mono-alfabètics, esquemes clàssics de xifrat en bloc, criptoanàlisi).*
- *Criptografia simètrica moderna. (Esquemes moderns de xifrat en bloc: DES - Data Encription Standard, IDEA - International Data Encryption Algorithm,Rijndael).*
- *Criptografia de clau pública. (Protocol d'intercanvi de claus de Diffie-Hellman. Criptosistemes de clau pública: RSA i ElGamal).*
- *Autenticació, integritat i no repudi. (Codis d'autenticació. Funcions hash. Signatura digital)*
- *Signatura i certificació digital. (Infrastructura de clau pública (PKI). Normativa X.509).*
- *Criptografia amb corbes elíptiques (Introducció a les corbes elíptiques. Problema del Logaritme Discret Elíptic. Criptosistemes elíptics. Nivells de seguretat)*

4. MATERIALS DE L'ASSIGNATURA I PROGRAMARI

L'assignatura es gestiona mitjançant l'eina de campus virtual SAKAI (http://sakai.udl.es)
Les classes presencials es desenvoluparan amb el suport de pissarra i/o transparències. Els materials de l'assignatura estaran accessibles en el campus virtual.

5. BIBLIOGRAFIA

Bibliografia bàsica

- Domingo, J. and Herrera, J.
  Criptografia: per als serveis telemàtics i el comerç electrònic.
  Universitat Oberta de Catalunya (1999).
- Fernández, C., Gimbert, J., Mateu, C., and Valls, M.
  Notes sobre criptografia de clau compartida, volum 39.
  Quaderns EUP (2002).
- Koblitz, N.
  A course in number theroy and cryptography
  Springer-Verlag (1994)
- Lucena, M.
  Criptografía y seguridad en computadores. (2003).
  Es pot descarregar un versió digital a: http://wwwdi.ujaen.es/~mlucena/lcripto.html
- Menezes, A., Oorschot, P., and Vanstone, S. .
  Handbook of applied cryptography.
  CRC Press.(1997).
  Es pot descarregar una versió digital a: http://www.cacr.math.uwaterloo.ca/hac/
- Stallings, W.
  Criptography and Network Security.
  Prentice-Hall, 2 edition. (1999).

Bibliografia complementària

- Koblitz, N.
  Algebraic Aspects of Criptography.
  Springer.(1997).
- Schneier, B.
  Applied cryptography.
  Wiley, 2 edition. (1996).
- Singh, S.
  Los códigos secretos.
  Debate.(2000).
- Stinson, D.
  Cryptography. Theory and practice.
  CRC Press.(1995).
- van Tilborg, H.
  Fundamentals of Cryptology.
  Kluwer Academic Publishers. (2000).
- Welsh, D.
  Codes and Criptography.
  Oxford University Press. (1988).

6. AVALUACIÓ

L'avaluació de l'assignatura es pot realitzar amb dues modalitats:

- *Avaluació continuada*

  Consisteix en l'entrega de problemes i pràctiques al llarg del quadrimestre en que es desenvolupa l'assignatura, juntament amb una prova presencial de validació, que permetrà valorar si l'estudiant ha seguit correctament l'assignatura i ha realitzat els problemes i les pràctiques encomanades.

- *Avaluació no continuada*

  Es realitza un examen presencial sobre els continguts de l'assignatura.

En la convocatòria de setembre, l'únic model possible és el de l'avaluació no continuada.

En el model d'avaluació continuada es tindrà en compte, per matitzar la nota final, la participació de l'estudiant en el desenvolupament de l'assignatura (plantejament de qüestions i dubtes, lectures complementàries, participació en forums de discussió,...)