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

1. OBJECTIUS

En l'assignatura de *Seguretat Computacional* ja s'han introduit els conceptes bàsics de criptografia, necessaris per garantir la seguretat de les aplicacions de comerç electrònic. Aquesta assignatura, pensada com una continuació de l'anterior, pretèn aprofundir en aquelles tècniques, tot presentat protocols criptogràfics més complexos.

Els objectius concrets de l'assignatura són:

- Presentar a l'estudiants protocols criptogràfics avançats, que són emprats com a subprotocols d'eines segures més complexes.
- Mostrar a l'estudiant sistemes criptogràfics que permetin oferir una versió virtual segura d'algunes activitats desenvolupades en la vida real.
- Que l'estudiant sigui capaç d'analitzar quins subprotocols criptogràfics esdevenen imprescindibles per assolir cadascun dels nivells de seguretat desitjables en diferents aplicacions telemàtiques.

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

1. *Proves de coneixement zero i sistemes d'identificació*
    - Sistemes de prova interactius
    - Proves de coneixement zero perfectes i computacionalment segures
    - Proves de coneixement zero no interactives
    - Sistemes d'identificació feble
    - Sistemes d'identifiació repte-resposta mitjançant criptografia simètrica o asimètrica
    - Sistemes d'identifiació repte-resposta mitjançant proves de coneixement zero
2. *Seguretat en situacions de desconfiança mútua*
    - Compromís d'un bit (*Bit commitment*)
    - Intercanvi simultani de secrets
    - Transferència inconscient (*Oblivious transfer*).
    - Diner electrònic
    - Signatura simultània de contractes
    - Correu electrònic amb justificant de recepció
    - Datació electrònica (*Time-stamping*).
    - Notarització electrònica

- Protecció del copyright: *watermarking* i *fingerprinting.*
- Caixes de seguretat virtuals

3. *Criptografía distribuida o de grup.*
    - Esquemes per a compartir secrets: seguretat incondicional i computacional.
    - Criptosistemes de desxifrat compartit.
    - Computació multipart segura.
    - Esquemes de predistribució de claus i emissions xifrades.
    - Signatura digital de grup.
    - Custòdia de claus (*Key-escrow*).
    - Votació electrònica.

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

- Desmedt, Y.
  Some recent research aspects of threshold cryptography.
  Lecture Notes in Computer Science. Proc. Information Security, 1396:158-173.(1999).
- Domingo, J. and Herrera, J. .
  Criptografia: per als serveis telemàtics i el comerç electrònic.
  Universitat Oberta de Catalunya.(1999)
- Menezes, A., van Oorschot, P., and Vanstone, S.
  Handbook of Applied Cryptography.
  CRC Press.(1997).
- Schneier, B.
  Applied cryptography.
  Wiley, 2 edition. (1996).
- Stallings, W.
  Criptography and Network Security.
  Prentice-Hall, 2 edition. (1999).
- Stinson, D. .
  Cryptography. Theory and practice.
  CRC Press (1995).

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,...)