	MÀSTER EN ENGINYERIA DE PROGRAMARI LLIURE		
	ASSIGNATURA: Seguretat		
	PROFESSORSRESPONSABLES: Francesc Solsona, Magda Valls		
	CURS: 2n	**CRÈDITS: 6**	**TIPUS: Obligatori**

1. OBJECTIUS

En general, podríem dir que la *seguretat informàtica* abarca tot un seguit de tècniques que permeten garantir que els recursos d'un sistema d'informació siguin emprats de forma correcta per aquelles entitats autoritzades a fer-ho. Més concretament, es considera que un sistema és segur si està dotat de mecanismes que en garanteixen la confidencialitat, integritat, disponibilitat i no-repudi.

En aquesta assignatura veurem una introducció a les tècniques criptogràfiques bàsiques que permeten implementar comunicacions segures.
D'altra banda, en la segona part de l'assignatura ens centrarem en estudiar solucions segures en un entorn particular: el de les xarxes GRID i Peer-to-Peer (P2P).

Els objectius concrets de l'assignatura són:

- 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.
La primera part de l'assignatura es desenvolparà a l'aula, on es presentaran els conceptes teòrics i resolució de problemes. La segona part de l'assingnatura constarà d'unes sessions teòriques introductòries, després de les quals cada estudiant escollirà un treball a realitzar, del que es farà un seguiment. Finalment, l'estudiant haurà de presentar als seus companys el treball desenvolupat.

3. PROGRAMA

La primera part de Criptografia, cobreix els següents continguts:

- *Fonaments matemàtics de la criptografia.*
- *Criptografia simètrica clàssica i moderna.*
- *Criptografia de clau pública: Diffie-Hellman. RSA i ElGamal.*
- *Autenticació, integritat i no repudi.*
- *Seguretat aplicada a entorns GRID i Peer-to-Peer (P2P).*

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 de criptografia

- 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 bàsica de GRID i P2P

- http://www-unix.globus.orgtoolkit/
- Chord. http://pdos.csail.mit.edu/chord/
- Pastry. http://research.microsoft.com/~antr/Pastry/
- http://sconce.ics.uci.edu/gac/. http://sconce.ics.uci.edu/gac/publication.html
- http://gridsec.usc.edu/files/TR/IPDPS-PowerTrust.pdf
- http://www.cag.lcs.mit.edu/bayanihan/papers/ccgrid01/

6. AVALUACIÓ

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

- *Avaluació continuada*
  Es realitzarà una prova corresponent a la part de criptografia, i es realitzarà un treball sobre algun tema de seguretat en sistemes P2P, que s'haurà de presentar a l'aula.
- *Avaluació no continuada*
  Es realitza un examen presencial sobre els continguts de l'assignatura.

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,...).