	ENSENYAMENT D'ENGINYERIA INFORMÀTICA (2n cicle)		
	ASSIGNATURA: Seguretat Computacional (Bloc de Comerç Electrònic i Telemàtica)		
	PROFESSOR/A RESPONSABLE: Francesc Sebé		
	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 aquesta assignatura s'inicia l'estudiant en les tècniques criptogràfiques bàsiques necessàries per a la implementació d'aplicacions segures. Els objectius concrets de l'assignatura són:

•Conèixer els algorismes actuals de xifratge mitjançant criptografia de clau compartida.
•Conèixer els algorismes actuals de xifratge i signatura digital amb criptografia de clau pública.
•Saber utilitzar la criptografia com a eina per transmetre dades de forma confidencial, íntegra, autenticada i no repudiable.
•Conèixer els protocols utilitzats a Internet per la transmissió segura de dades.
•Saber utilitzar eines per l'enviament segur de correu electrònic.
•Saber configurar un servidor web segur i navegar per Internet de forma segura.

1. ESTRUCTURA

Aquesta assignatura consta de 6 crèdits, 4.5 dels quals s'imparteixen de forma presencial i 1.5 de forma no presencial. Les sessions presencials tenen una durada de dues hores. En la primera hora, el professor imparteix una classe magistral. A la segona hora, es planteja un o diversos exercicis que es resolen a classe.

Les sessions no presencials es dediquen a la realització d'exercicis pràctics davant de l'ordinador. Aquests exercicis consisteixen en la implementació de petits programes o en la utilització d'eines criptogràfiques de lliure distribució.

2. PROGRAMA

1.Introducció i conceptes bàsics (criptologia, criptografia, criptoanàlisi, confidencialitat, integritat, autenticació, no repudi, tipus d'atacant).

2.Criptografia de clau compartida clàssica (xifres de substitució i transposició).

3.Criptografia de clau compartida moderna (xifres de bloc, modes de xifratge, xifres de flux).
4.Criptografia de clau pública (les xifres RSA i ElGamal, signatura digital, certificats digitals, infraestructures de clau pública).

5.Protocols segurs de comunicació (seguretat en xarxes sense fils, els protocols IPsec, SSL/TLS, SSH, correu electrònic segur).

6.Criptografia sobre corbes el·líptiques (introducció a les corbes el·líptiques).

1. 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.

Els exercicis pràctics es faran utilitzant programari de lliure distribució: Java, OpenSSL, Apache.

2. BIBLIOGRAFIA

•J.Domingo, J.Herrera, Criptografia per als serveis telemàtics i el comerç electrònic. Universitat Oberta de Catalunya. 1999.

•E.Mainwald. Fundamentos de seguridad en redes. McGraw-Hill. 2004.

•The OpenSSL Project. http://www.openssl.org.

•Apache Web Server. http://www.apache.com

1. AVALUACIÓ

L'estudiant pot escollir entre seguir l'avaluació continuada (forma recomanada sobretot als estudiants que poden assistir a classe) o realitzar un examen final.

Per als qui segueixin l'avaluació continuada, la nota final de l'assignatura depèn de tres factors:

•Lliurament dels exercicis fets en hores de classe (20%)
•Realització dels exercicis fets en les sessions no presencials (20%)
•Prova escrita a final de curs (60%)

Els estudiants no interessats en seguir l'avaluació continuada podran avaluar-se mitjançant la realització d'un examen global a final de curs. En aquest cas, la nota final depèn de dos factors:

•Realització dels exercicis fets en les sessions no presencials (20%)
•Examen global a final de curs (80%)

La realització dels exercicis de les sessions no presencials és obligatòria en tots els casos.