

	ENSENYAMENTS D'E.T. INFORMÀTICA DE SISTEMES I GESTIÓ		
	ASSIGNATURA: Bloc d'internet: administració, aplicacions i seguretat		
	PROFESSORAT: Ivan Canales, Magda Valls (Responsable)		
	CURS: 3r	CRÈDITS: 15	TIPUS: Optatiu

1. OBJECTIUS

L'objectiu d'aquest bloc és el d'introduir aspectes complementaris dins l'àrea de les comunicacions entre ordinadors, que puguin ser consolidats seguint una metodologia eminentment pràctica i que acostin a l'alumne a alguns dels aspectes que trobarà al món laboral.

Si tenim en compte que un dels possibles àmbits de treball dels futurs enginyers tècnics en informàtica de la UdL vindrà lligat a entitats o corporacions de petit o mitjà volum en procés de desenvolupar, consolidar i/o gestionar la seva connectivitat internat i externa, pensem que el caire adequat del bloc ha de tractar tres aspectes; instaurar, desenvolupar i protegir.

Aquests tres aspectes a tractar es reflexen en tres grups temàtics que li permetran:

- Abordar el disseny i manteniment de serveis de comunicacions internes que resultin útils a corporacions petites o mitjanes i que permeti la seva connexió d'una forma eficient a la resta d'internet.
- Tractar conceptes i eines de desenvolupament d'aplicacions, principalment dins l'àmbit del tractament i la representació de la informació.
- Dotar de seguretat tant a les entitats de comunicacions com a les aplicacions de que disposa.

2. ESTRUCTURA

El bloc s'estructura en tres mòduls:

- **Criptografia i seguretat a internet**
S'imparteix en el primer semestre i consta de 6 crèdits (3 teòrics, 2 de problemes i 1 de laboratori)
- **Construcció i administració de xarxes de comunicacions**
S'imparteix en el primer semestre i consta de 4 crèdits (2 teòrics i 2 de laboratori)
- **Desenvolupament d'aplicacions a internet**
S'imparteix en el segon semestre i consta de 5 crèdits (3 teòrics i 2 de laboratori)

3. PROGRAMA

1. Criptografia i seguretat a Internet

- Introducció.
- Fonaments matemàtics de la criptografia. (Introducció a la teoria de nombres: divisibilitat, aritmètica modular, teorema de Fermat, funció d'Euler, teorema d'Euler. Introducció a la complexitat computacional).

- 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 Encryption Standard, IDEA - International Data Encryption Algorithm, Rijndael).
- Criptografia de clau pública. (Protocol d'intercanvi de claus de Diffie-Hellman, esquemes de clau pública: RSA i ElGamal).
- Autenticació, integritat i no repudi. (Codis d'autenticació. Funcions hash. Signatura digital)
- Signatura i certificació digital. (Infraestructura de clau pública (PKI). Normativa X.509).
- Seguretat en el correu electrònic. (L'especificació S/MIME. Les eines PGP, Pretty Good Privacy).
- Comerç electrònic. (Protocol Secure Socket Layer (SSL), web sites segurs, Secure Electronic Transactions (SET)).

2. Construcció i Administració de Xarxes de Comunicacions

- Dispositius d'interconnexió i cablatge.
- Revisió del model OSI i el nivell d'enllaç de dades
- Arquitectura TCP/IP.
- Configuració bàsica del sistema (kernel, inetd i interfícies Ethernet i PPP).
- Configuració de l'encaminament (Estàtic, dinàmic interior, dinàmic exterior, masquerading).
- Eines de diagnosi (Ethereal, ping, route).
- Serveis de comunicacions (DNS, SMTP, POP, FTP, HTTP, DHCP).
- Configuració del DNS (resolver, named, nslookup)
- Configuració de serveis de xarxa (NFS, Samba, Web, DHCP, POP/SMTP (Sendmail)).

3. Desenvolupament d'aplicacions a Internet

- Arquitectura client/servidor.
- El llenguatge HTML i les fulles d'estil.
- Programació en el client, el llenguatge Javascript.
- Programació en el servidor, CGIs (Perl) i PHP.
- El llenguatge JAVA (llibries de seguretat i programació amb sockets).
- Accés a bases de dades (JDBC).
- El model d'n capes. (J2EE, JSP i JavaServlets, EJB).
- Introducció a l'XML.

4. MATERIALS DE L'ASSIGNATURA I PROGRAMARI

Les classes es desenvoluparan amb el suport de pissarra i/o transparències (aquestes seran accessibles per l'estudiantat)

5. BIBLIOGRAFIA

Criptografia i seguretat a Internet

- Domingo, J. and Herrera, J. (1999).
Criptografia: per als serveis telemàtics i el comerç electrònic
Universitat Oberta de Catalunya.
- Fernández, C., Gimbert, J., Mateu, C., and Valls, M. (2002b).
Notes sobre criptografia de clau compartida, volum 39.
Quaderns EUP.
- Menezes, A., Oorschot, P., and Vanstone, S. (1997a).
Handbook of applied cryptography.
CRC Press.
Es pot descarregar una versió digital a: <http://www.cacr.math.uwaterloo.ca/hac/>
- Stallings, W. (1999).
Cryptography and Network Security.
Prentice-Hall, 2 edition.

Construcció i Administració de Xarxes de Comunicacions

- Comer, D. (1991).
Internet networking with TCP/IP. Volume I: Principles, protocols and architecture
Prentice Hall.
- Costales, B. and Allman, E. (1997).
Sendmail.
O'Reilly, 2 edition.
- Hunt, C. (1998).
TCP/IP Network Administration.
O'Reilly.
- Stevens, W. (1990).
UNIX Network Programming.
Prentice Hall.

Desenvolupament d'aplicacions a Internet

- Chapman, B. and Zwicky, E. (1995).
Building Internet Firewalls.
O'Reilly.
- Flannagan, D. (1997).
JavaScript, the Definitive Guide.
O'Reilly, 2 edition.
- Gundavaram, S. (1996).
CGI Programming on the World Wide Web.
O'Reilly.
- Hunter, J. and Crawford, W. (2001).
Java Servlet Programming.
O'Reilly, 2 edition.

- Monson-Haefel, R. (2001).
Enterprise JavaBeans.
O'Reilly, 3 edition.
- Wall, L., Christiansen, T., and Orwant, J. (2000).
Programming Perl.
O'Reilly, 3 edition.

6. AVALUACIÓ

La nota final s'obindrà com a mitja de les notes obtingudes en els diferents mòduls, ponderada pel nombre de crèdits de cada mòdul.

En la nota corresponent a cada mòdul, es consideraran dos aspectes:

- Una prova final escrita
- Una avaluació continuada d'exercicis pràctics i pràctiques