Seguretat Computacional (6 Crèdits)

Programa:

Tema I. Introducció a la seguretat computacional

- Definicions i terminologia bàsica.
- Anàlisi de riscos.
- Entorns on considerar la seguretat computacional.

Temps: 3 hores

Tema II. Secret i Autenticitat

- Sistema criptogràfic.
- Teoria del secret perfecte de Shannon.
- Teoria de l'autenticitat perfecta de Simmons.
- Disseny de criptosistemes.

Temps: 9 hores

Tema III. Criptosistemes de clau secreta

- Criptosistemes basats en transposicions.
- Criptosistemes basats en substitucions.
- El criptosistema DES.
- El criptosistema PES.

Temps: 9 hores

Tema IV. Criptosistemes de clau pública

- Complexitat computacional.
- Funcions unidireccionals. Funcions unidireccionals amb trampa.
- Criptosistemes RSA i ElGamal.
- Criptosistema Knapsack.
- Altres criptosistemes.

Temps: 9 hores

Tema V. Protocols criptogràfics.

- Definicions i exemples.
- Protocol de tres passos de Shamir.
- Protocols d'intercanvi de claus.
- Signatures digitals.
- Protocols d'autentificació.
- Proves sense transferència de coneixement.
- Dispositius criptogràfics. Smart Cards.

Temps: 9 hores

Bibliografia bàsica:

J. Rifà i LL. Huguet, *Comunicación Digital*, Ed. Masson, 1991.

G.S. Simmons, *Contemporary Cryptology*, IEEE Press, 1991.

J.A. Cooper, *Computer & Communications Security*, McGrawHill, 1989.

T.W. Madron, *Redes de Area Local. La siguiente generación*, Noriega, 1992.

D.E. Comer, *Internetworking with TCP/IP Vol. I, 2. Ed.*, Prentice Hall, 1991.