# Enginyeria Informàtica

# *Seguretat computacional*(20375)



---

## Objectiu

- Introduir el tema de la seguretat en sistemes informàtics i les seves components legals, polìtiques, administratives, físiques i, també, lògiques.
- Introduir a l'alumne al concepte de la seguretat en sistemes operatius, concretament a través del UNIX.
- Introduir a l'alumne en els fonaments matemàtics i tècniques utilitzades per a la protecció de la informació en sistemes informàtics.
- Donar a l'alumne els coneixaments necessaris per a l'aplicació de mètodes i algoritmes de protecció de la informació, tant des de la seva vesant clàsica com moderna.
- Donar a l'alumne els coneixaments necessaris per a l'aplicació dels mètodes i tècniques criptogràfiques adients, tant en criptosistemes de clau pública com privada.
- Introduir el concepte de protocol i, en general, esquemes de seguretat per a resoldre problemes d'autenticació, accés compartit, criptografia *scrow*, distribució i gestió de claus, proves d'identificació, proves de coneixament nul, etc.
- Apendre a utilitzar *software* apropiat per el maneig de grans

nombres primers de cara a implementar algun sistema criptogràfic amb utilitat pràctica.

▲ Index ▲

# Temari

1. Introducció
   - Seguretat en el tractament de la informació
   - Seguretat en sistemes operatius
   - Seguretat en bases de dades
   - Seguretat en xarxes de comunicacions
   - Polítiques i models de seguretat
   - Avaluació de sistemes segurs
   - La seguretat en el sistema *Unix*
2. Sistemes criptogràfics
   - Sistemes criptogràfics (Shannon 1949)
   - Criptosistemes de clau privada
   - Teoria del secret perfecte de Shannon (1949)
   - Teoria de l'autenticitat perfecta
   - Exemples d'autenticitat i secret perfecte
   - Principis de criptografia computacional
3. Criptografia de clau privada
   - Mètodes criptogràfics elementals
   - Criptografia clàssica
   - Criptografia de clau privada. El DES
   - Criptoanàlisi del DES
   - Modes d'operació del DES
   - Aplicacions DES
   - Criptografia de clau privada. L'IDEA
4. Previs aritmètics
   - L'algorisme de les divisions successives
   - MCD
   - Càlcul d'inversos
   - Fraccions contínues

- Algorisme estès d'Euclides
- Teorema de Dirichlet
- Síntesi d'un LFSR
- Aritmètica i nombres primers
- Quadrats i arrels quadrades a Z/p
- Quadrats i arrels quadrades a Z/q, on $q=p_1\ p_2$

5. Criptografia de clau pública
   - Criptografia de clau pública
   - Funcions unidireccionals
   - La funció exponencial
   - Problemes NP. El Knapsak
   - Utilització de les funcions unidireccionals
   - Criptosistema RSA
   - Perills en l'ús del RSA
   - La seguretat en l'RSA
   - Criptosistema ElGamal
   - Signatura digital DSS
   - Criptosistema Knapsak
   - Criptosistema de McEliece
   - Criptosistemes probabilístics
6. Protocols criptogràfics
   - Protocols criptogràfics
   - Protocol de tres-passes de Shamir
   - Protocols de gestió de claus
   - Protocols quàntics d'intercanvi de claus
   - Protocols d'autentificació. Signatures digitals
   - Signatures implícites
   - Signatures explícites
   - Funcions *hash* criptogràfiques
   - SHS (Secure Hash Standard)
   - Signatures digitals. Històries d'un estàndard
   - Problemes dels esquemes de signatura digital
   - Protocols d'autentificació. STS.
   - Transaccions amb rastre
   - Transaccions sense rastre. Firmes digitals cegues
   - Esquemes llindar

- Esquema de Shamir 1979
- Esquema de Rifà. 1993.
- Proves d'identitat
- Proves de coneixement nul
- Prova d'identitat d'Omura
- Tirar una moneda per telèfon
- Protocol de Fiat-Shamir

▲ Index ▲

# Bibliografia


- Brassard G.: *Modern Criptology*, LNCS, n.325, Springer-Verlag (1988).
- Hardy, G.H. and Wright, E.M.: *An Introduction to the Theory of Numbers*, Oxford Science Publications, Clarendon Press, Oxford (1989).
- Rifà, J.: *Seguretat Computacional*. Materials, 21. Servei de Publicacions de la UAB. 1998.
- Rifà, J. i Huguet, L.: *Comunicación Digital*. Masson Ed. (1991).
- Robling Denning D.E.: *Cryptography and Data Security*. Addison-Wesley Publishing Company (1988).
- Schneier, B.: *Applied Criptography*, John Wiley and Sons, Inc. 1996.
- Simmons, G.S.: *Contemporary Criptology. The Science of Information Integrity*, IEEE Press (1991).
- Pfleeger, C.P.: *Security in Computing.* , Prentice Hall (1997).


▲ Index ▲

# Pràctiques

- Utilització de les eines de seguretat del sistema operatiu UNIX i d'alguns paquets de seguretat de domini públic relacionats.
- Programació del criptosistema RSA utilitzant el paquet de càlcul PARI-GP.

▲ Index ▲

---

# Sistema d'Avaluació

La nota conjunta màxima de 2 punts, obtinguda en l'avaluació de les pràctiques, passarà a sumar-se directament a la nota de l'exàmen final (màxim de 8 punts) per obtenir la nota global de l'assignatura.

Per poder aprovar l'assignatura cal haver aprovat les dues parts per separat (exàmen, pràctiques).

**Nota:** Si una de les dues parts està suspesa, l'assignatura quedarà suspesa.

▲ Index ▲

---

# Recomanacions

▲ Index ▲

---

*Final de pàgina*