SEGURETAT COMPUTACIONAL

Enginyeria Informàtica

Optativa: 6 crèdits (3+3)

Objectius:

? 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 i Windows NT.
? 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 coneixements 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 coneixements 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 coneixement nul, etc.
? Aprendre a utilitzar *software* apropiat per la construcció i l'administració d'infraestructures de clau pública (PKI).

Programa de l'assignatura:

1. Introducció
o Seguretat en el tractament de la informació
o Seguretat en sistemes operatius
o Seguretat en bases de dades
o Seguretat en xarxes de comunicacions
o Polítiques i models de seguretat
o Avaluació de sistemes segurs
o La seguretat en el sistema *Unix*

2. Sistemes criptogràfics
o Sistemes criptogràfics (Shannon 1949)
o Criptosistemes de clau privada
o Teoria del secret perfecte de Shannon (1949)
o Teoria de l'autenticitat perfecta
o Exemples d'autenticitat i secret perfecte
o Principis de criptografia computacional

3. Criptografia de clau privada
o Mètodes criptogràfics elementals
o Criptografia clàssica
o Criptografia de clau privada. El DES
o Criptoanàlisi del DES
o Modes d'operaciò del DES
o Aplicacions DES
o L'**AES** (Rijndael), el nou estàndard en criptografia de clau privada.

4. Previs aritmètics
o L'algorisme de les divisions successives
o MCD
o Càlcul d'inversos
o Algorisme estès d'Euclides
o Teorema de Dirichlet
o Síntesi d'un LFSR
o Aritmètica i nombres primers
o Quadrats i arrels quadrades a Z/p
o Quadrats i arrels quadrades a Z/q, on $q=p1 \cdot p2$

5. Criptografia de clau pública
o Criptografia de clau pública
o Funcions unidireccionals
o La funció exponencial
o Problemes NP. El Knapsak
o Utilització de les funcions unidireccionals
o Criptosistema RSA
o Perills en l'ús del RSA
o La seguretat en l'RSA
o Criptosistema ElGamal
o Signatura digital DSS
o Criptosistema Knapsak
o Criptosistemes probabilístics
o Infraestructures de clau pública (PKI). Certificats CCITT X.509

6. Protocols criptogràfics
o Protocols criptogràfics
o Protocol de tres-passes de Shamir
o Protocols de gestió de claus
o Protocols quàntics d'intercanvi de claus
o Protocols d'autentificació. Signatures digitals
o Signatures implícites
o Signatures explícites
o Funcions *hash* criptogràfiques
o SHS (Secure Hash Standard)
o Signatures digitals.
o Problemes dels esquemes de signatura digital

o Protocols d'autentificació. STS. SSL.
o Transaccions amb rastre
o Transaccions sense rastre. Firmes digitals cegues
o Esquemes llindar
o Esquema de Shamir 1979
o Proves d'identitat
o Proves de coneixement nul
o Prova d'identitat d'Omura
o Tirar una moneda per telèfon
o Protocol de Fiat-Shamir

Pràctiques:

? Utilització de les eines de seguretat del sistema operatiu UNIX, i d'alguns paquets de seguretat de domini públic relacionats.
? Utilització de la llibreria OpenSSL.

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).

Avaluació de l'assignatura:

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.