Seguretat Computacional

Enginyeria en Informatica.

Programa

1. Seguretat computacional
    - Introducció
    - Seguretat en el tractament de la informació
    - Seguretat en sistemes operatius
    - La seguretat en el S.O. *Unix*
    - Seguretat en bases de dades
    - Seguretat en xarxes de comunicacions
    - Polítiques i models de seguretat
    - Avaluació de sistemes segurs
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'autenticitatat i secret
    - 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 $\mathcal{Z}/p$
   - Quadrats i arrels quadrades a $\mathcal{Z}/q$, on $q = p_1 \cdot p_2$

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-passos de Shamir
   - Protocols de gestió 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

Bibliografia

[1] Brassard G.: *Modern Criptology*, LNCS, n.325, Springer-Verlag (1988).

[2] Hardy, G.H. and Wright, E.M.: *An Introduction to the Theory of Numbers*, Oxford Science Publications, Clarendon Press, Oxford (1989).

[3] Rifà, J.: *Seguretat Computacional.* Materials, 21. Servei de Publicacions UAB. (1995).

[4] Rifà, J. i Huguet, L.: *Comunicación Digital.* Masson Ed. (1991).

[5] Robling Denning D.E.: *Cryptography and Data Security.* Addison-Wesley Publishing Company (1988).

[6] Schneier, B.: *Applied Criptography*, John Wiley & Sons, Inc. 1993.

[7] Simmons, G.S.: *Contemporary Criptology. The Science of Information Integrity*, IEEE Press (1991).

Pràctiques

L'assignatura comprèn la realització de dues pràctiques, en grups de 2 o 3 persones:

1. **Utilització de les mesures de seguretat que ofereix Unix**: Sessió pràctica, amb una durada prevista d'aproximadament tres hores, al laboratori C5-129, on cada estudiant seguirà un guió preestablert.

2. **Programació de criptosistemes de clau pública: RSA i ElGamal**: La pràctica consisteix en la programació en llenguatge C, sobre PC, dels criptosistemes RSA i ElGamal. L'horari és de laboratori obert al laboratori C5-129, amb una durada prevista de realització de la pràctica d'unes 12h. Tot i així, també hi haurà un horari tancat durant el qual es podran resoldre dubtes a la mateixa aula.

Avaluació

- Hi ha 4.5 crèdits entre teoria i problemes, i això dóna just per fer el temari previst en el programa que s'adjunta. També hi ha 1.5 crèdits de pràctiques.

- **Avaluació de les pràctiques:**

  Les sessions estan destinades a l'aclariment de consultes. Pel que fa a la pràctica 1, es portarà a terme un control d'assistència. L'assistència a la pràctica 2 és opcional. Tantmateix serà imprescindible entregar els criptosistemes de manera que s'ajustin perfectament al banc de proves que es donarà.

  Havent superat aquests requisits, l'alumne serà qualificat amb *Apte* o *Apte+* i podrà optar a aprovar l'assignatura.

- **Avaluació de l'assignatura:**

  El sistema d'avaluació global de tota l'assignatura consisteix en un examen al final del període lectiu en el que un 80% de la nota respon a les activitats dutes a terme en les classes de teoria i de problemes. El 20% restant consisteix en preguntes que fan referència a trets concrets que els alumnes s'han trobat en l'execució de les pràctiques de la assignatura.