departamento de matemática aplicada I

Criptografía

Optativa de 5º curso de Ingeniería Informática

Segundo cuatrimestre

Curso 2008/2009

SITIO ACREDITADO CURSO 2007/08 UNIVERSIDAD D SEVILLA

Programa

Introducción

Necesidad de la seguridad. No sólo secreto. Ataques y defensas. Ataques pasivos. Ataques activos. Servicios de seguridad. ¿Qué es la Criptografía?. Cifrar y descifrar. Criptoanálisis. Seguridad computacional. Atacantes y sus recursos.

Fundamentos

Un poco de historia. Desplazamiento. Cifrado afín. Cifrado por sustitución. Cifrado por transposición. Cifrado de Vigenère. Cifrado XOR. Máquinas de rotores. Teoría de la información. Cifrado de Vernam. Cifrados en flujo.

Criptografía simétrica

Criptosistemas simétricos. Ventajas e inconvenientes. Cifrado por bloques. Cifrado producto. Cifrados por bloques. DES. AES. IDEA. Otros cifrados simétricos.

Criptografía de clave pública

Criptografía de clave pública. El criptosistema de mochila de Merkle-Hellman. El criptosistema RSA. El criptosistema Elgamal. Criptografía de curvas elípticas.

Aplicaciones

Sobre digital. Intercambio de claves de Diffie y Hellman. Autenticación e integridad. Funciones resumen. Firmas digitales. Firma digital RSA. Firma digital Elgamal. Certificados digitales. Algunos problemas resueltos.

Bibliografía

- **William Stallings**: ***Criptography and network security. Principles and Practice.*** Prentice hall, 1999.
- **Stinson, Douglas R**: ***Criptography. Theory and Practice.*** CRC Press. 1995.
- **Schneier, Bruce**: ***Applied criptography.*** John Wiley & Sons 1996.

- **Alfred J. Menezes, Paul C. van Oorschot y Scott A. Vanstone** : ***Handbook of Applied Cryptography.*** CRC Press (se puede descargar en PDF en http://www.cacr.math.uwaterloo.ca/hac/) .
- **Manuel José Lucena López**: ***Criptografía y Seguridad en Computadores.*** http://wwwdi.ujaen.es/~mlucena/wiki/pmwiki.php?n=Main.LCripto.
- **Konheim, Alan**: ***Criptography: A primer.*** John Wiley & Sons 1981.
- **Joseph Silverman**: ***A Friendly Introduction to Number Theory.*** Prentice Hall 1996.
- **Charles Kaufman, Radia Perlman, Michael Speciner**: ***Network Security: Private Communication in a Public World.*** Prentice Hall 1995.
- **Ramanujachary Kumanduri, Cristina Romero**: ***Number Theory with Computer Applications.*** Prentice Hall 1998.

Metodología

Consulte la Página de material para el curso actual.

NEW Puede acceder al portal de la asignatura mediante el enlace http://ma1.eii.us.es/cdoc

Evaluación

Todas las pruebas tendrán carácter teórico-práctico y se permitirá en ellas el uso de las transprencias de clase.

Prácticas

Dado el carácter eminentemente aplicado de esta asignatura todas las clases tendrán una orientación práctica.

Profesores

- **Armario Sampalo, José Andrés**
  Grupo 1.
- **Gudiel Rodríguez, Félix**
  Grupo 1 y 2.
- **Valeiras Reina, Gerardo (coordinador)**
  Grupo 2.

Tutorías

Los horarios de tutoria y asistencia al alumnado se publicarán en el Departamento.