ASIGNATURA: Métodos Criptográficos.

Curso: 2003/2004

Carácter: Optativa **Temporalidad:** 2º Cuatrimestre **Créditos:** 4,5 (3T+1,5P)

Profesor: Andrés Santiago Martín **Despacho:** Despacho 10

Web: http://cum.unex.es/profesores/asanmar/default.htm **E-mail:** asanmar@unex.es

NORMAS GENERALES:

- Las convocatorias de los exámenes serán fijadas por la Subdirección Académica del Centro.
- Todo alumno deberá entregar obligatoriamente una ficha al profesor de la asignatura.
- En los trabajos prácticos de la asignatura el profesor establecerá, en su momento, la fecha límite de entrega de cada uno de dichos trabajos.

CRITERIOS DE EVALUACIÓN:

- **Parte de Teoría:**
  - Habrá un examen de teoría, problemas y ejercicios prácticos sobre los contenidos de la asignatura: Supondrá el 75 % de la nota.
- **Parte Práctica:**
  - Ejercicios prácticos de laboratorio: Supondrán el 25 % de la nota y su realización será obligatoria.
  - Cualquier sospecha de copia sobre una práctica entregada o parte de la misma, implicará inexorablemente suspender la práctica completa.
- **Trabajos voluntarios presentados.**
  - Dichos trabajos versarán sobre temas relacionados directamente con la asignatura, y necesitarán de la aprobación previa del profesor.
  - Estos trabajos, tras su evaluación por el profesor, podrán subir de 0,5 a 1 puntos que se sumarán a la nota conseguida en los apartados anteriores, siempre que en los mismos se obtenga la calificación mínima exigida.
  - La entrega de trabajos sólo se aplicará a la convocatoria de Febrero.
- La nota final será igual a:
  - **Si** (teoría ≥ 4,5) y (práctica ≥ 4,5) y ([(teoría * 0,75) + (práctica * 0,25)] ≥ 4)
    - nota final = (teoría * 0,75) + (práctica * 0,25) + nota trabajos
  - **Si no**
    - nota final = Suspenso
  - **Fin** si
- En todo caso, sólo se aprobará si la nota final es igual o superior a 5.
- Si un alumno tiene una parte aprobada, nota mayor o igual a 5, y tiene la otra parte suspensa (no compensable), con nota menor que 4,5, la nota final obtenida será la de la parte suspensa.
- Tanto la nota del examen teórico como la nota de la práctica podrán ser guardadas hasta la convocatoria de septiembre del presente curso, siempre que sea superior a 5 puntos.
- Si un alumno presenta un trabajo voluntario en la convocatoria de Febrero, y en cambio no aprueba la asignatura, la nota de dicho trabajo se guarda hasta la convocatoria de septiembre del presente curso.

OBJETIVOS GENERALES:

- Introducir al alumno en los fundamentos matemáticos y técnicas utilizadas para la protección de la información, y en las políticas y planes de seguridad, técnicas criptográficas, su historia y desarrollo.
- Proporcionar los conocimientos necesarios para aplicar técnicas criptográficas adecuadas en criptosistemas de bloque, tanto de clave privada como pública, y criptosistemas de flujo.
- Introducir los conceptos de protocolos, esquemas de seguridad y, en particular, la gestión de claves, tanto con técnicas simétricas como con técnicas asimétricas.
- Introducir al alumno en la problemática de la protección de la información en medios electrónicos de intercambio de mensajes como el correo electrónico, páginas Web y demás sistemas de comunicación electrónica.

METODOLOGÍA:

- En las dos clases de teoría semanales se exponen los conceptos teóricos sobre protección de la información, técnicas criptográficas, protocolos, esquemas de seguridad, gestión de claves, etc.
- Así mismo, están las horas de tutorías en las que los alumnos pueden consultar con el profesor la resolución de cualquier duda planteada sobre cualquier aspecto de la asignatura.
- En las clases teóricas se utilizan medios audiovisuales de divulgación informática.
- Las clases prácticas se destinan a manejar de forma práctica los conceptos vistos en teoría.
- En la página Web del profesor y en la copistería del centro se encuentra a disposición de los alumnos, los horarios de tutorías, temario de la asignatura, criterios de evaluación así como todo el material didáctico usado en la misma.

PROGRAMA TEÓRICO:

TEMA 1 INTRODUCCIÓN.

Introducción.
Conceptos fundamentales.
Políticas de seguridad.
Análisis y gestión de riesgos.
Principios fundamentales de la Seguridad Informática.
El papel de la Criptografía en la seguridad de la información.

TEMA 2 FUNDAMENTOS TEÓRICOS DE LA CRIPTOGRAFÍA.

Introducción e historia.
Componentes de un criptosistema.
Requisitos de un criptosistema.
Métodos de ataque a un criptosistema.
Fuerza de un criptosistema.
Tipos de criptosistemas.
La Criptografía en la Seguridad Informática.

TEMA 3 MÉTODOS CRIPTOGRÁFICOS CLÁSICOS.

Introducción.
Cifrado por sustitución.
Cifrado por transposición.
Clasificación de los métodos clásicos.
Características de un buen cifrador.
Criptoanálisis básico.

TEMA 4 CRIPTOGRAFÍA MODERNA.

Introducción.
Introducción al cifrado de flujo.
Introducción al cifrado en bloque.

TEMA 5 CRIPTOSISTEMAS DE CLAVE SECRETA.

Cifrado de producto.
Algoritmos de clave privada.
Algoritmo DES.
Variantes del algoritmo DES.
Algoritmo IDEA.
Algoritmo Rijndael (AES).
Modos de cifrado para algoritmos de cifrado por bloques.
Criptoanálisis de algoritmos simétricos.

TEMA 6 CRIPTOSISTEMAS DE CLAVE PÚBLICA.

Introducción.
Cifrado exponencial.
Intercambio de clave de Diffie y Hellman.
Algoritmo de cifrado asimétrico RSA.
Algoritmo de cifrado asimétrico de Elgamal.
Consideraciones sobre el bloque.
Fortaleza del cifrado exponencial.

TEMA 7 CRIPTOSISTEMAS CON CIFRADO EN FLUJO.

Introducción.
Secuencias pseudoaleatorias.
Tipos de generadores de secuencia.
Registros de desplazamiento retroalimentados.
Otros generadores de secuencia.

TEMA 8 FUNCIONES HASH O FUNCIONES RESUMEN.

Introducción.
Longitud adecuada para una firma.
Estructura de una función resumen.
Funciones Hash. MD5 y SHA-1.

TEMA 9 AUTENTIFICACIÓN Y FIRMA DIGITAL.

Introducción.
Funciones y esquemas de autenticación.
Firma digital.
Algoritmos de firma digital. RSA, ElGamal y DSS.

TEMA 10 OTROS ASPECTOS DE LA SEGURIDAD INFORMÁTICA.

Aplicaciones de Correo Seguro.
Protocolos y Esquemas Criptográficos.
Esteganografía.
Introducción al Cifrado con Curvas Elípticas.
Certificados Digitales y Estándar PKCS.

PROGRAMA PRÁCTICO:

- Las prácticas consistirán en observar el funcionamiento de diversos algoritmos vistos en teoría, para evaluar su funcionamiento, y estudiar sus ventajas e inconvenientes.
- Para el desarrollo de las prácticas se utilizará software de libre distribución desarrollado en el **Departamento de Lenguajes, Proyectos y Sistemas Informáticos** de la **Escuela Universitaria de Informática** de la **Universidad Politécnica de Madrid**.

BIBLIOGRAFÍA:

- **Referencias principales.**
  1. *Fúster, A.; De la Guía, D.; Hernández, L.; Montoya, F.; Muñoz, J.* "**Técnicas Criptográficas de Protección de Datos**", 2ª edición, Ra-Ma, 2000.
  2. *Lucena López, Manuel José* "**Criptografía y Seguridad en Computadores"**, 4ª edición (Versión 0.6.2) Universidad de Jaén, 2005. Este documento está disponible en: http://www.telefonica.net/web2/lcripto/lcripto.html
  3. *Ramió Aguirre, Jorge* "**Libro Electrónico de Seguridad Informática y Criptografía"**, Versión v 4.0 Dpto. de Publicaciones E.U.I. Universidad Politécnica de Madrid. Marzo 2005. Este documento está disponible en: http://www.criptored.upm.es/guiateoria/gt_m001a.htm

- **Otras referencias.**
  1. *Denning, Dorothy Elizabeth,* **"Cryptography and Data Security"**, Addison-Wesley, 1983.
  2. *Morant J.L., Ribagorda A., Sancho J* **"Seguridad y protección de la información"**, Editorial Centro de Estudios Ramón Areces, Madrid, 1994.
  3. *Pastor, José; Sarasa, Miguel Ángel,* **"Criptografía Digital"**, Colección Textos Docentes; Prensas Universitarias de Zaragoza; 1998.
  4. *Pfleeger, Charles P.,* **"Security in Computing"**, Prentice-Hall, 1989.
  5. *Ramió Aguirre, Jorge* **"Aplicaciones Criptográficas"**, Segunda Edición Dpto. de Publicaciones E.U.I. Universidad Politécnica de Madrid. Junio 1999.
  6. *Schneier, Bruce,* **"Applied Cryptography. Protocols, Algorithms, and Source Code in C"**, 2ª edición, John Wiley & Sons, Inc.; 1996.