Plan 254 Ing. en Informática

Asignatura 14023 CRIPTOGRAFIA

Grupo 1

Presentación

Criptología. Sistemas criptográficos de clave pública y de clave privada. Protocolos criptográficos.

Programa Básico

1.- Introducción a los criptosistemas clásicos.

2.- Criptosistemas simétricos o de clave privada. Técnicas de cifrado en bloque. Técnicas de cifrado en flujo. Implementación.

3.- Complejidad computacional de algoritmos y problemas matemáticos.

4.- Criptosistemas asimétricos o de clave pública: condiciones de Diffie-Hellman, funciones de una vía y funciones trampa, factorización y RSA, logaritmo discreto. Implementación de alguno de los sistemas.

5.- Autentificación y firma digital.

6.- Protocolos criptográficos.

Objetivos

Proporcionar al alumno una visión general del estado actual de la Criptografía y temas relacionados: Autentificación de mensajes, Firma Digital, Seguridad en Redes de Computadores, Protocolos Criptógráficos, etc. Desarrollar las herramientas y algoritmos esenciales en Criptografía.

Programa de Teoría

1.- Introducción a los criptosistemas clásicos.

2.- Criptosistemas simétricos o de clave privada. Técnicas de cifrado en bloque. Técnicas de cifrado en flujo. Implementación.

3.- Complejidad computacional de algoritmos y problemas matemáticos.

4.- Criptosistemas asimétricos o de clave pública: condiciones de Diffie-Hellman, funciones de una vía y funciones trampa, factorización y RSA, logaritmo discreto. Implementación de alguno de los sistemas.

5.- Autentificación y firma digital.

6.- Protocolos criptográficos.

Programa Práctico

Criptografía y criptoanálisis de métodos clásicos.
Cifrado en flujo (Vernam).
Cifrado en bloques (Feistel o Rijndael).
Clave pública: RSA.
Algoritmos básicos del RSA.
Primalidad y factorización.
Otros métodos.
Protocolos criptográficos.

Evaluación

El 30% de la calificación se obtendrá mediante el desarrollo de una práctica implementando uno o varios sistemas criptográficos.
El 70% restante se obtendrá de un examen final teórico-práctico.

Ambos apartados son obligatorios, aunque no se establece nota mínima en ninguno de ellos.

El examen teórico-práctico incidirá en las partes esenciales de la asignatura y combinará temas, cuestiones teóricas y ejercicios.

Las prácticas se desarrollarán preferiblemente en el Laboratorio de la asignatura, dentro del horario reservado a la misma, en un lenguaje simbólico predeterminado (normalmente Maple), aunque no se exigen conocimientos previos del mismo. Si son convenientes conocimientos previos de programación.
De forma excepcional se pueden contemplar otras opciones para el desarrollo de la práctica. Éstas deben ser autorizadas por el profesor de manera individualizada.

Bibliografía

* J.A. Buchmann: "Introduction to cryptography". UTM. Springer-Verlag. 2001.

* Amparo Fuster & Dolores de la Guía & Edt., "Técnicas Criptográficos de Protección de Datos", Ra-Ma.

* Carlos Munuera & Juan Tena, "Codificación de la Información", Secretariado de Publicaciones de la Universidad de Valladolid.

* Jose Pastor & Miguel Ángel Sarasa, "Criptografia Digital", Prensas Universitarias de Zaragoza.

* William Stalling., "Cryptography and Network Security", Prentice Hall International.