Plan 276 Lic. en Matemáticas

Asignatura 43988 MODELOS DISCRETOS EN TEORIA DE LA INFORMACION

Grupo 1

Presentación

Modelos Discretos. Aritmética. Introducción a la Teoría de la Información.

Programa Básico

1.- Teoría de la Información.
Concepto matemático de la información. Transmisión de la información. Tipos de canales. Codificación de la información. Códigos de longitud fija y de longitud variable. Canales sin ruido; Algoritmo de Huffman. Canales con ruido.

2.- Códigos correctores.
Conceptos básicos. Distancia de Hamming. Capacidad correctora de un código. Decodificación por mínima distancia. Teoremas de Shannon y consecuencias. Códigos lineales sobre cuerpos finitos. Decodificación por síndrome. Tableros completos e incompletos. Ejemplos de códigos lineales: Hamming, Golay, Reed-Muller.

3.- Criptografía.
Definiciones básicas. Criptografía y criptoanálisis. Criptosistemas de clave privada; sustitución, transposición, matriciales. Métodos de cifrado en bloque; DES. Métodos de cifrado en flujo. Criptosistemas de clave pública. Complejidad computacional. RSA y logaritmo discreto.

Objetivos

Proporcionar al alumno una introducción a los problemas de la teoría matemática de la información con especial énfasis en los métodos discretos y centrada en la protección de la información frente a errores (códigos correctores) y ataques a la privacidad (criptología).

Programa de Teoría

1. Teoría de la Información.
Concepto matemático de la información. Transmisión de la información. Tipos de canales. Codificación de la información. Códigos de longitud fija y de longitud variable. Canales sin ruido; Algoritmo de Huffman. Canales con ruido.

2. Códigos correctores.
Conceptos básicos. Distancia de Hamming. Capacidad correctora de un código. Decodificación por mínima distancia. Teoremas de Shannon y consecuencias. Códigos lineales sobre cuerpos finitos. Decodificación por síndrome. Tableros completos e incompletos. Ejemplos de códigos lineales: Hamming, Golay, Reed-Muller.

3. Criptografía.
Definiciones básicas. Criptografía y criptoanálisis. Criptosistemas de clave privada; sustitución, transposición, matriciales. Métodos de cifrado en bloque; DES, AES. Métodos de cifrado en flujo. Criptosistemas de clave pública. Complejidad computacional. RSA y logaritmo discreto.

Programa Práctico

Quince de las horas correspondientes a las clases prácticas se desarrollarán en el aula de informática. El alumno dispondrá de horas adicionales de libre disposición para finalizar la realización de las prácticas.

Evaluación

Es obligatoria la entrega y defensa de dos prácticas realizadas en el aula informática que aportará el 30% de la calificación final. El 70% restante se obtendrá de un examen teórico-práctico.

Bibliografía

* Hoffman, D.G., Leonard, D.A. y otros, Coding Theory. The essentials, Marcel Dekker, 1992.

* Hill R., A first course in coding theory, Oxford Univ. Press, 1986.

* Munuera, C y Tena, J, Codificación de la Información, Pub. UVA, Valladolid, 1997.

* Welsh D., Codes and Cryptography, Oxford Univ. Press, Oxford, 1988.

* Caballero, P., Introducción a la Criptografía, RAMA.

* Fuster, A., de la Guía, D., Hernandez, L., Montoya, F. y Muñoz, J., Técnicas criptografícas de protección de datos. 2ª ed., RAMA. Textos Universitarios, 2000.

* Koblitz, N., A course in number theory and cryptography. Graduate Texts in Mathematics, 114, Springer, 1994.

* Rincón, F., García y Martínez, Cálculo científico con Maple, RAMA, 1995.