

# Introducción a Códigos y Criptografía

(1er cuatrimestre de 2005)

Propuesta como materia Optativa (o Especialidad) para las Licenciaturas en Matemática y Computación.

Correlativas: Álgebra 1 (M. Discreta 1) y Álgebra 2. Horas: 90.

**Docente a cargo:** Roberto Miatello.

## **Bibliografía:**

1. D. Hoffman et al, Coding Theory. The Essentials, Marcel Dekker.
2. S. Roman, Information theory and Coding, Springer Verlag.
3. R. Mollin, An introduction to cryptography, Chapman-Hall Inc.
4. W. Ebeling, Lattices and codes, Vieweg Verlag.

## **Programa tentativo:**

- 1.1 Códigos autocorrectores, generalidades. Códigos lineales. Matriz de chequeo de paridad.
- 1.2 Códigos perfectos. Cotas. Código de Hamming, Golay, extendido, Reed-Müller. Decodificación rápida.
- 1.3. Cuerpos finitos, morfismos, polinomios minimales, polinomios irreducibles.
- 1.4. Códigos cíclicos, duales. Codificación y decodificación. Códigos BCH, de Reed-Solomon, decodificación. Algoritmo de Berlekamp-Massey. Decodificación de códigos de Reed-Müller y de códigos de convolución. Aplicación a "compact discs."
- 1.5 Criptografía. Orígenes históricos. Factorización. Primalidad.
- 1.6. Congruencias. Función phi de Euler. Logaritmos discretos.
- 1.7. Criptosistemas de clave pública. Autenticación.
- 1.8. Tests de primalidad.
- 1.9. Algoritmos de Factoreo. Cribas.
- 1.10. Residuos Cuadráticos. Reciprocidad. Aplicaciones a códigos y criptografía.

El programa se podrá adaptar a los conocimientos previos de los alumnos. Interesados comunicarse con

R. Miatello ([miatello@mate.uncor.edu](mailto:miatello@mate.uncor.edu))

O R. Podestá ([podesta@mate.uncor.edu](mailto:podesta@mate.uncor.edu)).