TEORÍA DE CÓDIGOS Y CRIPTOGRAFÍA (Programa) • **Grado Matemáticas** • **Curso 2024–2025**

PROGRAMA

INTRODUCCIÓN:

Ideas generales. Códigos criptográficos y códigos detectores y correctores de errores.

BLOQUE A: CRIPTOGRAFÍA.

A1: Criptosistemas clásicos. Cesar, Vigenère, matrices de cifra. Análisis de frecuencias e índice de coincidencia.

A2: Criptografía de clave pública. Una aplicación: las firmas digitales.

A3: Algoritmos de factorización y tests de primalidad. Introducción a la idea de complejidad.

A4: El criptosistema RSA.

A5: Otros criptosistemas de clave pública. Más aplicaciones.

BLOQUE B: TEORÍA DE CÓDIGOS.

B1: Códigos detectores y correctores de errores. Propiedades generales y estudio de tres ejemplos prácticos: El código de barras, el ISBN y el NIF.

B2: Códigos lineales.

B3: Algoritmos de codificación y decodificación para códigos lineales. Decodificación incompleta.

B4: Códigos de Hamming. Relación con la geometría proyectiva.

B5: Códigos perfectos.

OBJETIVOS DEL CURSO

- Comprender el papel de las matemáticas en la transmisión segura y fiable de la información.
- Familiarizarse con algunos ejemplos notables de criptosistemas de clave simétrica. Saber cómo se usan, sus fortalezas y sus debilidades.
- Entender la diferencia entre criptografía de clave simétrica y criptografía de clave pública.
- Conocer algunas aplicaciones de la criptografía de clave pública, en particular las firmas digitales.
- Conocer el funcionamiento de RSA y de los criptosistemas basados en logaritmos discretos.
- Familiarizarse con los principales tests de primalidad y algoritmos de factorización.
- Conocer los fundamentos teóricos de los códigos detectores y correctores de errores.
- Trabajar con ejemplos usuales de códigos detectores (NIF, código de barras, ISBN, CCC, etc.).
- Familiarizarse con algunas familias de códigos correctores (Hamming, BCH).
- Saber utilizar los algoritmos de codificación/decodificación para detectar/corregir errores.

PRERREQUSITOS

- El curso pretende ser elemental. El requisito básico es tener confianza con las congruencias.
- Conjuntos y Números: divisibilidad y factorización; Algoritmo de Euclides; operaciones y polinomios con congruencias: el Pequeño Teorema de Fermat.
- Álgebra Lineal: sobre $\mathbb{F}_p$, p primo.
- Estructuras Algebraicas. Nociones básicas de grupos.

BIBLIOGRAFÍA

Referencias Básicas:

- R. Hill. A first course in coding theory. Oxford University Press 1986).
- N. Koblitz. *A course in Number Theory and Criptography*, 2nd ed.. Springer-Verlag (1994).

Otras referencias sobre Criptografía:

- J. Hoffstein, J. Pipher, J.H. Silverman. *An introduction to mathematical cryptography.* Springer (2008).
- D. R. Kohel. *Cryptography.*
- M. J. Lucena López, *Criptografía y seguridad en computadores.* (2022).
- J. Menezes, P. C. van Oorschot, S. A. Vanstone. *Handbook of applied cryptography.* CRC Press (1997).
- S. Singh. *Los códigos secretos*, Debate (2000).
- N. Smart, *Cryprography, an introduction.*
- D. R. Stinson. *Cryptography theory and practice.* Chapman & Hall/CRC (2006).

Otras referencias sobre Teoría de Códigos:

- J. I. Hall. *Notes on Coding Theory.*
- R. A. Podestá. *Introducción a la teoría de códigos autocorrectores.*

PROFESOR, HORARIO , AULA, TUTORÍAS

Aula: 01.17.AU.102 Tutorías: Solicitar cita.

Profesor	Despacho	email	Horario de clase
Enrique González Jiménez	01.17.509	`enrique.gonzalez.jimenez@uam.es`	12:30–13:30 LMJ

EXÁMENES

Parcial **A**	Parcial **B**	Ordinario	Extraordinario
J14 noviembre	X 18 diciembre	15 de enero	11 de junio

EVALUACIÓN

Para aprobar la asignatura se necesita aprobar cada una de las partes de la asignatura:

$$\mathbf{A} = \text{Criptografía} \qquad \text{y} \qquad \mathbf{B} = \text{Teoría de Códigos.}$$

En lo que sigue denotamos por:

$\mathbf{n_A}$=número de horas dedicadas a Criptografía,
$\mathbf{n_B}$=número de horas dedicadas a Teoría de Códigos.

Hay dos formas de aprobar la asignatura:

- **Opción 1**: A lo largo del curso se realizarán 2 parciales. Un parcial dedicado a cada una de las partes de la asignatura. Sea $\mathbf{C_A}$ (resp. $\mathbf{C_B}$) la calificación obtenida en el parcial dedicado a $\mathbf{A}$ (resp. a $\mathbf{B}$). Aquellos alumnos que hayan obtenido $\mathbf{C_A}, \mathbf{C_B} \geq 5$. Entonces la calificación final será:

$$\boxed{\mathbf{F} = \frac{\mathbf{n_A}}{\mathbf{n_A}+\mathbf{n_B}}\mathbf{C_A} + \frac{\mathbf{n_B}}{\mathbf{n_A}+\mathbf{n_B}}\mathbf{C_B}}$$

- **Opción 2**: El examen final (Ordinario o Extraordinario) constará de 2 partes, Cada una dedicado a una de las partes de la asignatura. Sea $\mathbf{F_A}$ (resp. $\mathbf{F_B}$) la calificación obtenida en la parte dedicada a $\mathbf{A}$ (resp. a $\mathbf{B}$). Aquellos alumnos que hayan obtenido $\mathbf{C_A} \geq 5$ (resp. $\mathbf{C_B} \geq 5$) podrán presentarse, si así lo desean, solo a la parte $\mathbf{B}$ (resp. $\mathbf{A}$). Entonces la calificación $\mathbf{F_A} = \mathbf{C_A}$ (resp. $\mathbf{F_B} = \mathbf{C_B}$). Para aprobar la asignatura será necesario obtener $\mathbf{F_A}, \mathbf{F_B} \geq 5$. La calificación final será

$$\boxed{\mathbf{F} = \frac{\mathbf{n_A}}{\mathbf{n_A}+\mathbf{n_B}}\mathbf{F_A} + \frac{\mathbf{n_B}}{\mathbf{n_A}+\mathbf{n_B}}\mathbf{F_B}}$$

  Observación: Aquellos alumnos que se presenten al examen final habiendo obtenido $\mathbf{C_A} \geq 5$ (resp. $\mathbf{C_B} \geq 5$) y obtengan $\mathbf{F_A} < 5$ (resp. $\mathbf{F_B} < 5$) suspenderán la asignatura..

Para aprobar la asignatura se ha de obtener $\mathbf{F} \geq 5$. Todas las calificaciones van de 0 a 10.