



UNIVERSIDAD DE GUADALAJARA

Centro Universitario de Ciencias Exactas e Ingenierías
División de Electrónica y Computación
INGENIERÍA FOTÓNICA

1. INFORMACIÓN DEL CURSO

Nombre: Seminario de problemas de métodos matemáticos I	Número de créditos: 5	Prerrequisitos: Ninguno
Departamento: Ciencias Computacionales	Tipo: Seminario	Nivel: Básica común
Horas teoría: 0	Horas práctica: 80	Total de horas por cada semestre: 80

2. DESCRIPCIÓN

2. DESCRIPCIÓN

Objetivo general

El seminario tiene la finalidad de que el alumno aprecie el valor y la belleza del álgebra lineal y la teoría de números, para codificar, encriptar y decodificar mensajes.

Contenido Temático

Parte I: Conceptos Preliminares de Álgebra Lineal y Teoría de Números

- 1) Divisibilidad de enteros, números primos, algoritmo de Euclides.
- 2) Congruencias módulo m .
- 3) Campos finitos.
- 4) Espacios y subespacios vectoriales sobre campos finitos. Bases y dimensión.
- 5) Transformaciones lineales (representación matricial, imagen y núcleo).

Parte II: Corrección de Errores

- 1) Conceptos básicos (emisor, receptor, canal, ruido, código). Códigos lineales y ejemplos (bit de paridad, triple repetición).
- 2) Distancia de Hamming y distancia mínima de un código. Teoremas de detección y corrección de errores.
- 3) Matrices generadora y verificadora. Teorema de Codificación de Canales con Ruido (o Teorema de Shannon).
- 4) Códigos de Hamming.
- 5) Códigos perfectos. Otros ejemplos de códigos: Golay, Reed-Solomon y Hadamard.

Parte III: Criptografía

- 1) Conceptos básicos (mensajes cifrados y llaves).
- 2) Cifrado de sustitución, sistema Vigenere y Playfair.
- 3) Cifrado de Hill y métodos de ataque.
- 4) Criptografía de llave pública. Sistema RSA.
- 5) Exactitud y confidencialidad del sistema RSA.