



1. INFORMACIÓN DEL CURSO

Título: Seminario de solución de problemas de métodos matemáticos I	Número de créditos: 5	Prerrequisitos: Ninguno
Departamento: Ciencias Computacionales	Tipo: Curso	Nivel: Licenciatura
Horas por semana 4	Clave: I5894	Total de horas por semestre: 68

2. DESCRIPCIÓN

Objetivo general

El seminario tiene la finalidad de apoyar a los estudiantes en la solución de tareas que deben realizar fuera del aula.

Contenido

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

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

Parte III: Criptografía

- 10) Conceptos básicos (mensajes cifrados y llaves).
- 11) Cifrado de sustitución, sistema Vigenere y Playfair.
- 12) Cifrado de Hill y métodos de ataque.
- 13) Criptografía de llave pública. Sistema RSA.
- 14) Exactitud y confidencialidad del sistema RSA.

Modalidades de enseñanza aprendizaje

Resolución de problemas.

Modalidad de evaluación

Realización satisfactoria de las actividades del seminario y entrega oportuna de todas las tareas.

Competencia a desarrollar

Aprendizaje autogestivo y adquisición del hábito del trabajo permanente en la vida cotidiana.

Campo de aplicación profesional

Sistemas Inteligentes.

3. BIBLIOGRAFÍA

Título	Autor	Editorial	Año de la edición más reciente
<i>Codes: An Introduction to Information Communication and Cryptography</i>	Biggs, Norman L.	Springer Undergraduate Mathematics Series, Springer	2008
<i>Error-Correcting Codes and Finite Fields</i>	Pretzel, Oliver	Claredon Press	1992
<i>Linear Algebra: A Pure Mathematical Approach</i>	Rose, H. E.	Birkhäuser	2002
<i>Basic Linear Algebra</i> , Springer Undergraduate Mathematics Series	T. S. Blyth y E. F. Robertson	Springer-Verlag	1998
<i>Conjuntos y números</i>	Castillo Pérez, Castillo Ramírez, de la Cruz García y Hernández Magdaleno	Editorial Universitaria, Universidad de Guadalajara	2014

Elaboraron:	Mtro. Alonso Castillo Pérez / Dr. Rubén Sánchez Gómez
Fecha de creación:	Octubre 2011
Actualización:	Diciembre 2014
Participaron en la modificación:	Dr. Alonso Castillo Ramírez/Mtro. Alonso Castillo Pérez
Participantes de la evaluación:	Dr. Alonso Castillo Ramírez/Mtro. Alonso Castillo Pérez
Fecha de la Modificación:	Julio 2015
Participantes en la modificación:	

Formato con base en el Artículo 21 del Reglamento General de planes de estudios de la U.de G.