ALGORITMOS MATEMÁTICOS-CRIPTOGRÁFICOS

1. IDENTIFICACIÓN

Ubicación: Variable según mención

Prelación: Calculo 3, Algoritmos y Complejidad 3

T P L C: 3 1 0 1

Condición: Obligatoria

Departamento: Computación

Área Curricular de Formación: CC, IS

Nivel de Formación: Formativo.

2. JUSTIFICACIÓN

Esta asignatura introduce las herramientas matemáticas y algoritmos necesarios para la protección de la información

3. OBJETIVOS

- Capacidad para tener un conocimiento profundo de los principios fundamentales y modelos de la computación y saberlos aplicar para interpretar, seleccionar, valorar, modelar, y crear nuevos conceptos, teorías, usos y desarrollos tecnológicos relacionados con la informática.
- Capacidad para evaluar la complejidad computacional de un problema, conocer estrategias algorítmicas que puedan conducir a su resolución y recomendar, desarrollar e implementar aquella que garantice el mejor rendimiento de acuerdo con los requisitos establecidos.
- Capacidad para comprender, aplicar y gestionar la garantía y seguridad de los sistemas informáticos.

4. CONTENIDO PROGRAMÁTICO

UNIDAD 1. OPERACIONES CON MATRICES

UNIDAD 2. SERIES DE FOURIER

UNIDAD 3. RESOLUCIÓN SISTEMAS ECUACIONES

UNIDAD 4. INTRODUCCIÓN A LA CRIPTOGRAFÍA

UNIDAD 5. ALGORITMOS CRIPTOGRÁFICOS.

5. METODOLOGÍA DE ENSEÑANZA:

La enseñanza de este curso se realizará a través clases teórico-prácticas y clases guiadas en el laboratorio

6. RECURSOS

Recursos multimedia: proyector multimedia, proyector de transparencias.

Computadora portátil

Guías y problemario de estudio elaborado por el profesor.

Bibliotecas programadas de algoritmos y estructuras de datos.

Animaciones.

Laboratorio para la parte práctica dotado con un computador por estudiante con el lenguaje de programación de alto nivel disponible y planificado por la cátedra.

Acceso a Internet

7. EVALUACIÓN

Serán evaluados los siguientes aspectos:

- Asistencia
- Participación en clase
- Evaluación del conocimiento teórico a través de pruebas parciales escritas
- Evaluación del conocimiento práctico a través de ejercicios prácticos al finalizar cada tema de la unidad respectiva

8. BIBLIOGRAFÍA

O. Geddes, S. R. Czapor, G. Labahn, Algorithms for Computer Algebra, Springer, 1992.

P. Caballero, Introducción a la criptografía. 2ª edición, RA-MA 2002.

G. Brassard, Moderm Cryptography, a tutorial, Springer-Verlag, 1988.

G. Dawson, Cryptography: policy and algorithms, 1996.

N. Koblitz, A course in number theory and cryptography, Springer-Verlag, 1979.

A. Fúster ,Técnicas cirptográficas de protección de datos. 3ª ed. Actualizada, Ed. RA-MA 2004.

D.R. Stinson , Cryptography: Theory & Practice, CRC 1995.

William Stallings “Cryptography and Network Security: Principles and Practice", 3rd ed.. Prentice Hall, Inc; 2002.

Dark Stamp, Richard M. Low. “Applied Cryptanalysis: Breaking Ciphers in the Real World”, Wiley-IEEE Press 2007.

Reinhard Wobst. “Cryptology Unlocked”, John Wiley & Sons 2007.

Pino Caballero Gil “Introducción a la criptografía”, 2ª Edición,. Editorial Ra-Ma 2002.

Raúl Durán Díaz, Luis Hernández Encinas, Jaime Muñoz Masque, “El criptosistema RSA”. Editorial Ra-Ma 2005.