Universidad Nacional de San Agustín
VICE RECTORADO ACADÉMICO
SILABO

CODIGO DEL CURSO: CS107

1 Datos Generales

FACULTAD : Ingeniería de Producción y Servicios						
DEPARTAMENTO : Ingeniería de Sistemas e Informática			**ESCUELA :** Ciencia de la Computación			
PROFESOR : **TÍTULO :**						
ASIGNATURA : Estructuras Discretas III						
PREREQUISITO: CS105,CS101O	**CREDITOS:** 4		**Año**: 2010-1 **Sem:** 3^{er} Semestre.		**Total Horas:** 2 HT; 2 HT	2 HP 2 HL
Horario	Lun	Mar	Mie	Jue	Vie	Sáb
Total Semanal						
Aula						

2 Exposición de Motivos

El álgebra abstracta tiene un lado práctico que explotaremos para comprender en profundidad ter
como criptografía y álgebra relacional.

2 Objetivo

- Conocer las técnicas y métodos de encriptación de datos.

3 Contenido Temático

3 AL/Algoritmos Criptográficos.(20 horas)

Objetivos Específicos	Conte
▪ Describir algoritmos numérico-teóricos básicos eficientes, incluyendo el máximo común divisor, inversa multiplicativa mod n y elevar a potencias mod n. ▪ Describir al menos un criptosistema de llave pública, incluyendo una suposición necesaria de complejidad teórica sobre su seguridad. ▪ Crear extensiones simples de protocolos criptográficos, usando protocolos conocidos y primitivas criptográficas.	▪ E ▪ C p ▪ C ▪ E ▪ E ▪ A c c [1], [2]

	Objetivos Específicos	Contenidos	H
3 Teoría de Números (20 horas)	▪ Establecer la importancia de la teoría de números en la criptografía ▪ Utilizar las propiedades de las estructuras algebraicas en el estudio de la teoría algebraica de códigos	▪ Teoría de los números ▪ Aritmética Modular ▪ Teorema del Residuo Chino ▪ Factorización ▪ Grupos, teoría de la codificación y método de enumeración de Polya ▪ Cuerpos finitos y diseños combinatorios [1], [2]	

4 Actividades

- Asignaciones
- Controles de Lectura
- Exposiciones

5 Recursos Materiales

- Apuntes del curso
- Libro(s) de la bibliografía

6 Metodología

- Clase Magistral.
- Taller didáctico.
- Social Constructivismo.
- Prácticas personales y en grupo.

7 Evaluación

La nota final (NF) se obtiene de la siguiente manera:

NE Nota de Exámenes 60 %, esta nota se divide en
- Exámen Parcial 40 %
- Examen Final 60 %

NT Nota de Trabajos e Intervención en clase 40 %

$$NF = 0{,}6 * NE + 0{,}4 * NT$$

Referencias

[1] R. Grimaldi. *Matemáticas Discretas y Combinatoria.* Addison Wesley Iberoamericana, 1997.

[2] Edward R. Scheinerman. *Introducción a la Teoría de Autómatas, Lenguajes y Computación.* Thomson Learning, 2001.

Docente del curso