Universidad Católica San Pablo
Facultad de Ingeniería y Computación
Escuela Profesional de
Ciencia de la Computación
SILABO

CS107. Álgebra Abstracta (Obligatorio)

2010-1

1. DATOS GENERALES		
1.1 CARRERA PROFESIONAL	:	Ciencia de la Computación
1.2 ASIGNATURA	:	CS107. Álgebra Abstracta
1.3 SEMESTRE ACADÉMICO	:	3^{er} Semestre.
1.4 PREREQUISITO(S)	:	CS105. Estructuras Discretas I. (1^{er} Sem) , CS101O. Introducción a la Programación Orientada a Objetos. (2^{do} Sem)
1.5 CARÁCTER	:	Obligatorio
1.6 HORAS	:	2 HT; 2 HL;
1.7 CRÉDITOS	:	3

2. DOCENTE

3. FUNDAMENTACIÓN DEL CURSO

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

4. SUMILLA

1. AL/Algoritmos Criptográficos.2. Teoría de Números

5. OBJETIVO GENERAL

- Conocer las técnicas y métodos de encriptación de datos.

6. CONTRIBUCIÓN A LA FORMACIÓN PROFESIONAL Y FORMACIÓN GENERAL

Esta disciplina contribuye al logro de los siguientes resultados de la carrera:

a) Aplicar conocimientos de computación y de matemáticas apropiadas para la disciplina. [**Nivel Bloom: 4**]

b) Analizar problemas e identificar y definir los requerimientos computacionales apropiados para su solución. [**Nivel Bloom: 3**]

j) Aplicar la base matemática, principios de algoritmos y la teoría de la Ciencia de la Computación en el modelamiento y diseño de sistemas computacionales de tal manera que demuestre comprensión de los puntos de equilibrio involucrados en la opción escogida. [**Nivel Bloom: 3**]

7. CONTENIDOS

UNIDAD 1: AL/Algoritmos Criptográficos.(20 horas)	
Nivel Bloom: 3	
OBJETIVO GENERAL	**CONTENIDO**
▪ 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 cripto-sistema 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.	▪ Revisión histórica de la criptografía. ▪ Criptografía de llaves privadas y el problema del intercambio de llaves. ▪ Criptografía de llaves públicas. ▪ Firmas digitales. ▪ Protocolos de seguridad. ▪ Aplicaciones (pruebas de cero-conocimiento, autenticación y otros).
Lecturas: [Grimaldi, 1997], [Scheinerman, 2001]	

UNIDAD 2: Teoría de Números (20 horas)	
Nivel Bloom: 3	
OBJETIVO GENERAL	**CONTENIDO**
▪ 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
Lecturas: [Grimaldi, 1997], [Scheinerman, 2001]	

8. METODOLOGÍA

El profesor del curso presentará clases teóricas de los temas señalados en el programa propiciando la intervención de los alumnos.

El profesor del curso presentará demostraciones para fundamentar clases teóricas.

El profesor y los alumnos realizarán prácticas

Los alumnos deberán asistir a clase habiendo leído lo que el profesor va a presentar. De esta manera se facilitará la comprensión y los estudiantes estarán en mejores condiciones de hacer consultas en clase.

9. EVALUACIONES

Evaluación Permanente 1 : 20 %

Examen Parcial : 30 %

Evaluación Permanente 2 : 20 %

Examen Final : 30 %

Referencias

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

[Scheinerman, 2001] Scheinerman, E. R. (2001). *Introducción a la Teoría de Autómatas, Lenguajes y Computación.* Thomson Learning.