

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



**CS107. Álgebra Abstracta (Obligatorio)**

2016-2

**1. DATOS GENERALES**

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

**2. DOCENTE**

Dr. Ana María Cuadros Valdivia

- Dr. Ciencia de la Computación, Universidad Nacional San Agustín, Perú, 2013.
- Mag. Ciencia de la Computación, ICMC-USP, Brasil, 2007.
- Prof. Ingeniería Informática, Universidad Católica San Pablo, Perú, 2008.

**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:

- ) Aplicar conocimientos de computación y de matemáticas apropiadas para la disciplina. [**Nivel Bloom: 4**]
- ) Analizar problemas e identificar y definir los requerimientos computacionales apropiados para su solución. [**Nivel Bloom: 3**]
- ) 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**

<b>UNIDAD 1: AL/Algoritmos Criptográficos.(20 horas)</b>	
<b>Nivel Bloom: 3</b>	
<b>OBJETIVO GENERAL</b>	<b>CONTENIDO</b>
<ul style="list-style-type: none"> <li>▪ Describir algoritmos numérico-teóricos básicos eficientes, incluyendo el máximo común divisor, inversa multiplicativa mod n y elevar a potencias mod n.</li> <li>▪ Describir al menos un cripto-sistema de llave pública, incluyendo una suposición necesaria de complejidad teórica sobre su seguridad.</li> <li>▪ Crear extensiones simples de protocolos criptográficos, usando protocolos conocidos y primitivas criptográficas.</li> </ul>	<ul style="list-style-type: none"> <li>▪ Revisión histórica de la criptografía.</li> <li>▪ Criptografía de llaves privadas y el problema del intercambio de llaves.</li> <li>▪ Criptografía de llaves públicas.</li> <li>▪ Firmas digitales.</li> <li>▪ Protocolos de seguridad.</li> <li>▪ Aplicaciones (pruebas de cero-conocimiento, autenticación y otros).</li> </ul>
<b>Lecturas:</b> [Grimaldi, 1997], [Scheinerman, 2001]	

<b>UNIDAD 2: Teoría de Números (20 horas)</b>	
<b>Nivel Bloom: 3</b>	
<b>OBJETIVO GENERAL</b>	<b>CONTENIDO</b>
<ul style="list-style-type: none"> <li>▪ Establecer la importancia de la teoría de números en la criptografía</li> <li>▪ Utilizar las propiedades de las estructuras algebraicas en el estudio de la teoría algebraica de códigos</li> </ul>	<ul style="list-style-type: none"> <li>▪ Teoría de los números</li> <li>▪ Aritmética Modular</li> <li>▪ Teorema del Residuo Chino</li> <li>▪ Factorización</li> <li>▪ Grupos, teoría de la codificación y método de enumeración de Polya</li> <li>▪ Cuerpos finitos y diseños combinatorios</li> </ul>
<b>Lecturas:</b> [Grimaldi, 1997], [Scheinerman, 2001]	

<b>8. METODOLOGÍA</b>
<p>El profesor del curso presentará clases teóricas de los temas señalados en el programa propiciando la intervención de los alumnos.</p> <p>El profesor del curso presentará demostraciones para fundamentar clases teóricas.</p> <p>El profesor y los alumnos realizarán prácticas</p> <p>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.</p>

<b>9. EVALUACIONES</b>
<p><b>Evaluación Permanente 1 : 20 %</b></p> <p><b>Examen Parcial : 30 %</b></p> <p><b>Evaluación Permanente 2 : 20 %</b></p> <p><b>Examen Final : 30 %</b></p>

## 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.