Universidad Católica San Pablo
Escuela Profesional de
Ciencia de la Computación
SILABO

CS1D3. Álgebra Abstracta (Obligatorio)

2018-I

1. DATOS GENERALES		
1.1 CARRERA PROFESIONAL	:	Ciencia de la Computación
1.2 ASIGNATURA	:	CS1D3. Álgebra Abstracta
1.3 SEMESTRE ACADÉMICO	:	3^{er} Semestre.
1.4 PREREQUISITO(S)	:	CS1D1. Estructuras Discretas I. (1^{er} Sem) , CS112. Ciencia de la Computación I. (2^{do} 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, 2015.
- Mag. Ciencia de la Computación, ICMC-USP, Brasil, 2007.
- Prof. Ingeniería Informática, Universidad Católica San Pablo, Perú, 2008.

3. FUNDAMENTACIÓN DEL CURSO

En algebra abstracta se explotará las nociones de teoria de números, grupos, anillos y campos para comprender en profundidad temas de computación como criptografía y teoría de la codificación.

4. SUMILLA

1. 2. 3. Criptografía4.

5. OBJETIVO GENERAL

- Entender los conceptos de estructuras algebraicas como anillos, dominios, cuerpos y grupos.
- Utilizar las propiedades de las estructuras algebraicas para resolver problemas
- Conocer las técnicas y métodos de sistemas criptográficos y como los teoremas permiten la realización de cálculos rápidos y eficientes.

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. (**Evaluar**)

i) Utilizar técnicas y herramientas actuales necesarias para la práctica de la computación. (**Usar**)

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. (**Evaluar**)

7. COMPETENCIAS ESPECÍFICAS DE COMPUTACIÓN

Esta disciplina contribuye a la formación de las siguientes competencias del área de computación (IEEE):

C1. La comprensión intelectual y la capacidad de aplicar las bases matemáticas y la teoría de la informática (computer science).⇒ **Outcome a**

C8. Entendimiento de lo que las tecnologías actuales pueden y no pueden lograr.⇒ **Outcome a**

C16. Capacidad para identificar temas avanzados de computación y de la comprensión de las fronteras de la disciplina.⇒ **Outcome j**

CS2. Identificar y analizar los criterios y especificaciones apropiadas a los problemas específicos, y planificar estrategias para su solución.⇒ **Outcome i**

8. CONTENIDOS

UNIDAD 1: (16)

Competencias: C1,CS2

CONTENIDO	OBJETIVO GENERAL
▪ Número enteros, algoritmos de la división, máximo común divisor, algoritmo de Euclides y algoritmo extendido de Euclides. Ecuaciones diofánticas ▪ Aritmética Modular y Operaciones en Zn: suma, resta, multiplicación, inversa y exponenciación. ▪ Congruencia, conjunto de residuos, congruencia lineal, teorema chino del resto. ▪ Generadores de números primos y pseudo-aleatorios, función phi de Euler, teorema pequeño de Fermat, teorema de Euler, teorema fundamental de la aritmética y factorización.	▪ Realizar cálculos que involucren aritmética modular [Usar] ▪ Describir algoritmos numérico teóricos bÃąsicos eficientes, incluyendo el algoritmo de Euclides y el algoritmo extendido de Euclides. [Evaluar] ▪ Establecer la importancia del estudio de la teoría de números. [Familiarizarse] ▪ Discutir la importancia de los números primos en criptografía y explicar su uso en algoritmos criptográficos[Familiarizarse]

Lecturas: [Rosen, 2011], [Grimaldi, 2003], [Koshy, 2007]

UNIDAD 2: (14)

Competencias: C1, C16

CONTENIDO	OBJETIVO GENERAL
▪ Grupos: propiedades, operaciones, homomorfismos e isomorfismo, orden de un grupo, grupos cíclicos, teorema de Lagrange y raíces primitivas. ▪ Anillos y cuerpos: propiedades, sub-anillos, dominios de integridad.	▪ Adquirir habilidad en la resolución de problemas abstractos y en la formulación de conjeturas . [Familiarizarse] ▪ Argumentar como los principales teoremas y algoritmos permiten resolver problemas criptográficos. [Evaluar]

Lecturas: [Grimaldi, 2003], [Gallian, 2012], [Koshy, 2007]

UNIDAD 3: Criptografía(20)	
Competencias: C8, C16	
CONTENIDO	**OBJETIVO GENERAL**
▪ Terminología básica de criptografía cubriendo las nociones relacionadas con los diferentes socios (comunicación), canal seguro / inseguro, los atacantes y sus capacidades, cifrado, descifrado, llaves y sus características, firmas. ▪ Tipos de cifrado (por ejemplo, cifrado César, cifrado affine), junto con los métodos de ataque típicas como el análisis de frecuencia. ▪ Apoyo a la infraestructura de clave pública para la firma digital y el cifrado y sus desafíos. ▪ Preliminares matemáticos esenciales para la criptografía, incluyendo temas de álgebra lineal, teoría de números, teoría de la probabilidad y la estadística. ▪ Primitivas criptográficas: • generadores pseudo-aleatorios y cifrados de flujo • cifrados de bloque (permutaciones pseudo-aleatorios), por ejemplo, AES • funciones de pseudo-aleatorios • funciones de hash, por ejemplo, SHA2, resistencia colisión • códigos de autenticación de mensaje • funciones derivaciones clave ▪ Criptografía de clave simétrica: • El secreto perfecto y el cojín de una sola vez • Modos de funcionamiento para la seguridad semántica y encriptación autenticada (por ejemplo, cifrar-entonces-MAC, OCB, GCM) • Integridad de los mensajes (por ejemplo, CMAC, HMAC) ▪ La criptografía de clave pública: • Permutación de trampilla, por ejemplo, RSA • Cifrado de clave pública, por ejemplo, el cifrado RSA, cifrado El Gamal • Las firmas digitales • Infraestructura de clave pública (PKI) y certificados • Supuestos de dureza, por ejemplo, Diffie-Hellman, factoring entero ▪ Protocolos de intercambio de claves autenticadas, por ejemplo, TLS . ▪ Los protocolos criptográficos: autenticación desafío-respuesta, protocolos de conocimiento cero, el compromiso, la transferencia inconsciente, seguro 2-partido o multipartidista computación, compartición de secretos y aplicaciones .	▪ Describir el propósito de la Criptografía y listar formas en las cuales es usada en comunicación de datos[Familiarizarse] ▪ Definir los siguientes términos: Cifrado, Criptoanálisis, Algorítmo Criptográfico, y Criptología y describe dos métodos básicos (cifrados) para transformar texto plano en un texto cifrado[Familiarizarse] ▪ Discutir la importancia de los números primos en criptografía y explicar su uso en algoritmos criptográficos[Familiarizarse] ▪ Explicar como una infraestructura de Clave Pública soporta firmas digitales y encriptación y discutir sus limitaciones/vulnerabilidades[Familiarizarse] ▪ Usar primitivas criptográficas y sus propiedades básicas[Familiarizarse] ▪ Ilustrar como medir la entropía y como generar aleatoriedad criptográfica[Familiarizarse] ▪ Usa primitivas de clave pública y sus aplicaciones[Familiarizarse] ▪ Explicar como los protocolos de intercambio de claves trabajan y como es que pueden fallar[Familiarizarse] ▪ Discutir protocolos criptográficos y sus propiedades[Familiarizarse] ▪ Describir aplicaciones del mundo real de primitivas criptográficas y sus protocolos[Familiarizarse] ▪ Resumir definiciones precisas de seguridad, capacidades de ataque y sus metas[Familiarizarse] ▪ Aplicar técnicas conocidas y apropiadas de criptografía para un escenario determinado[Familiarizarse] ▪ Apreciar los peligros de inventarse cada uno sus propios métodos criptográficos[Familiarizarse] ▪ Describir la criptografía cuántica y el impacto de la computación cuántica en algoritmos criptográficos[Familiarizarse]

UNIDAD 4: (10)	
Competencias: CS2	
CONTENIDO	**OBJETIVO GENERAL**
▪ Elementos, proceso de transmitir una palabra ▪ Esquemas de codificación: paridad, triple repetición, verificación de paridad y generación de códigos de grupo.	▪ Utilizar las propiedades de las estructuras algebraicas en el estudio de la teoria algebraica de los códigos. [Familiarizarse] ▪ Aplicar técnicas que permitan la detección de errores, y si es necesario, proveer de métodos para reconstruir palabras originales. [Usar]
Lecturas: [Grimaldi, 2003], [W.Trappe and Washington, 2005]	

9. 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.

10. EVALUACIONES

Evaluación Permanente 1 : 20 %

Examen Parcial : 30 %

Evaluación Permanente 2 : 20 %

Examen Final : 30 %

Referencias

[A.Menezes, 1996] A.Menezes (1996). *Handbook of Applied Cryptography (Discrete Mathematics and Its Applications.* CRC Press.

[Forouzan, 2008] Forouzan, B. (2008). *Introduction to Cryptography and Network Security.* McGraw-Hill.

[Gallian, 2012] Gallian, J. (2012). *Contemporary Abstract Algebra.* Brooks/Cole, 8 ed. edition.

[Grimaldi, 2003] Grimaldi, R. (2003). *Discrete and Combinatorial Mathematics: An Applied Introduction.* Pearson, 5 ed. edition.

[Koshy, 2007] Koshy, T. (2007). *Elementary Number Theory with Applications.* Academic Press, 2 ed. edition.

[Paar and Pelzl, 2011] Paar, C. and Pelzl, J. (2011). *Understanding Cryptography: A Textbook for Students and Practitioners.* Springer.

[Rosen, 2011] Rosen, K. H. (2011). *Matemática Discreta y sus Aplicaciones.* McGraw Hill, 7 ed. edition.

[W.Trappe and Washington, 2005] W.Trappe and Washington, C. (2005). *Introduction to Cryptography with Coding Theory.* Pearson Prentice Hall.