San Pablo Catholic University (UCSP)
Undergraduate Program in
Computer Science
SILABO

Universidad Católica San Pablo
2023-I

CS1D3. Abstract Algebra (Mandatory)

1. General information

1.1 School	:	Ciencia de la Computación
1.2 Course	:	CS1D3. Abstract Algebra
1.3 Semester	:	3^{er} Semestre.
1.4 Prerrequisites	:	• CS1D1. Discrete Structures I. (1^{st} Sem) • CS112. Computer Science I. (2^{nd} Sem)
1.5 Type of course	:	Mandatory
1.6 Learning modality	:	Face to face
1.7 Horas	:	2 HT; 2 HP;
1.8 Credits	:	3
1.9 Plan	:	Plan Curricular 2016

2. Professors

Lecturer

- Sergio Moisés Aquise Escobedo <saquise@ucsp.edu.pe>
  - PhD in Ciencias de la Educación, Universidad Nacional de San Agustin - UNSA, Perú, 2019.
  - MSc in Ciencias de la Computación y Matemática Computacional, ICMC-USP, Brasil, 2014.

3. Course foundation

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. Summary

1. 2. 3. Cryptography 4.

5. Generales Goals

- 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. Contribution to Outcomes

This discipline contributes to the achievement of the following outcomes:

1) Analyze a complex computing problem and to apply principles of computing and other relevant disciplines to identify solutions. (**Assessment**)

6) Apply computer science theory and software development fundamentals to produce computing-based solutions. (**Assessment**)

7. Content

UNIT 1: (16)

Competences:

Content	**Generales Goals**
• 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 [Usage] • Describir algoritmos numérico teóricos básicos eficientes, incluyendo el algoritmo de Euclides y el algoritmo extendido de Euclides. [Assessment] • Establecer la importancia del estudio de la teoría de números. [Familiarity] • Discuss the importance of prime numbers in cryptography and explain their use in cryptographic algorithms [Familiarity]

Readings: Rosen (2011), Grimaldi (2003), Koshy (2007)

UNIT 2: (14)

Competences:

Content	**Generales Goals**
• 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 . [Familiarity] • Argumentar como los principales teoremas y algoritmos permiten resolver problemas criptográficos. [Assessment]

Readings: Grimaldi (2003), Gallian (2012), Koshy (2007)

UNIT 3: Cryptography (20)

Competences:

Content	Generales Goals
• Basic Cryptography Terminology covering notions pertaining to the different (communication) partners, secure/unsecure channel, attackers and their capabilities, encryption, decryption, keys and their characteristics, signatures • Cipher types (e.g., Caesar cipher, affine cipher) together with typical attack methods such as frequency analysis • Public Key Infrastructure support for digital signature and encryption and its challenges • Mathematical Preliminaries essential for cryptography, including topics in linear algebra, number theory, probability theory, and statistics • Cryptographic primitives: – pseudo-random generators and stream ciphers – block ciphers (pseudo-random permutations), e.g., AES – pseudo-random functions – hash functions, e.g., SHA2, collision resistance – message authentication codes – key derivations functions • Symmetric key cryptography – Perfect secrecy and the one time pad – Modes of operation for semantic security and authenticated encryption (e.g., encrypt-then-MAC, OCB, GCM) – Message integrity (e.g., CMAC, HMAC) • Public key cryptography: – Trapdoor permutation, e.g., RSA – Public key encryption, e.g., RSA encryption, EI Gamal encryption – Digital signatures – Public-key infrastructure (PKI) and certificates – Hardness assumptions, e.g., Diffie-Hellman, integer factoring • Authenticated key exchange protocols, e.g., TLS • Cryptographic protocols: challenge-response authentication, zero-knowledge protocols, commitment, oblivious transfer, secure 2-party or multi-party computation, secret sharing, and applications • Motivate concepts using real-world applications, e.g., electronic cash, secure channels between clients and servers, secure electronic mail, entity authentication, device pairing, voting systems. • Security definitions and attacks on cryptographic primitives:	• Describe the purpose of Cryptography and list ways it is used in data communications [Familiarity] • Define the following terms: Cipher, Cryptanalysis, Cryptographic Algorithm, and Cryptology and describe the two basic methods (ciphers) for transforming plain text in cipher text [Familiarity] • Discuss the importance of prime numbers in cryptography and explain their use in cryptographic algorithms [Familiarity] • Explain how Public Key Infrastructure supports digital signing and encryption and discuss the limitations/vulnerabilities [Familiarity] • Use cryptographic primitives and their basic properties [Familiarity] • Illustrate how to measure entropy and how to generate cryptographic randomness [Familiarity] • Use public-key primitives and their applications [Familiarity] • Explain how key exchange protocols work and how they fail [Familiarity] • Discuss cryptographic protocols and their properties [Familiarity] • Describe real-world applications of cryptographic primitives and protocols [Familiarity] • Summarize precise security definitions, attacker capabilities and goals [Familiarity] • Apply appropriate known cryptographic techniques for a given scenario [Familiarity] • Appreciate the dangers of inventing one's own cryptographic methods [Familiarity] • Describe quantum cryptography and the impact of quantum computing on cryptographic algorithms [Familiarity]

UNIT 4: (10)	
Competences:	
Content	**Generales Goals**
• 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. [Familiarity] • Aplicar técnicas que permitan la detección de errores, y si es necesario, proveer de métodos para reconstruir palabras originales. [Usage]
Readings: Grimaldi (2003), W.Trappe and Washington (2005)	

8. Methodology

1. El profesor del curso presentará clases teóricas de los temas señalados en el programa propiciando la intervención de los alumnos.
2. El profesor del curso presentará demostraciones para fundamentar clases teóricas.
3. El profesor y los alumnos realizarán prácticas
4. 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. Assessment

Continuous Assessment 1 : 20 %

Partial Exam : 30 %

Continuous Assessment 2 : 20 %

Final exam : 30 %

References

A.Menezes (1996). *Handbook of Applied Cryptography (Discrete Mathematics and Its Applications*. CRC Press.
Forouzan, B. (2008). *Introduction to Cryptography and Network Security*. McGraw-Hill.
Gallian, J. (2012). *Contemporary Abstract Algebra*. 8 ed. Brooks/Cole.
Grimaldi, R. (2003). *Discrete and Combinatorial Mathematics: An Applied Introduction*. 5 ed. Pearson.
Koshy, T. (2007). *Elementary Number Theory with Applications*. 2 ed. Academic Press.
Paar, C. and J. Pelzl (2011). *Understanding Cryptography: A Textbook for Students and Practitioners*. Springer.
Rosen, Kenneth H. (2011). *Matemática Discreta y sus Aplicaciones*. 7 ed. McGraw Hill.
W.Trappe and C. Washington (2005). *Introduction to Cryptography with Coding Theory*. Pearson Prentice Hall.