1. Datos Generales de la asignatura

Nombre de la asignatura:	Fundamentos de estructuras discretas para la ciberseguridad
Clave de la asignatura:	CBC-2418
SATCA[1]:	2-2-4
Carrera:	Ingeniería en Ciberseguridad.

2. Presentación

Caracterización de la asignatura

Aporta el perfil del Ingeniero en Ciberseguridad las siguientes habilidades:

- Utiliza sistemas operativos, lenguajes de programación, redes y entornos tecnológicos para integrar soluciones de seguridad con responsabilidad e inclusión social en las organizaciones.
- Emplea métodos criptográficos para establecer protocolos de seguridad en el transporte de datos seguros a nivel de aplicación, usando herramientas de seguridad basadas en dichos protocolos integrando excelencia, vanguardia e innovación social que fortalezcan el desarrollo humano.

A su vez proporciona una sólida base en conceptos y técnicas matemáticas fundamentales para el estudio de la criptografía y la seguridad de la información. Se abordan temas esenciales como bases aritméticas, lógica proposicional y de predicados, teoría de conjuntos, grafos y árboles, teoría de números, congruencias y aritmética modular. Estos conocimientos sientan las bases para comprender y aplicar algoritmos criptográficos modernos, protocolos de seguridad y técnicas de cifrado.

Aporta conocimientos a las asignaturas de introducción a la programación, redes de datos, criptografía, estructuras de datos y fundamentos de bases de datos.

Intención didáctica

La asignatura se organiza en cinco temas, los cuales incluyen contenidos conceptuales y la aplicación de estos a través de resolución de problemas y ejercicios prácticos.
En el tema de los sistemas numéricos el estudiante aprenderá el uso de los diferentes sistemas numéricos, como el binario, el octal y el hexadecimal.
En el segundo tema conocerá los conceptos básicos de la lógica proposicional y su aplicación en computación, igualmente se examinan los conceptos de lógica de predicados y algebra declarativa.
En el tema de relaciones y funciones identifica las propiedades que posee una relación expresada como conjunto de pares ordenados, como una expresión algebraica, de una forma verbal o

[1] Sistema de Asignación y Transferencia de Créditos Académicos

simbólica. De igual forma se realiza una identificación de funciones y se da solución a ejercicios prácticos.
En el tercer tema, teoría de grafos, el estudiante aplica los conceptos básicos de grafos para resolver problemas afines al área computacional, relacionados con el recorrido y búsqueda en grafos. El estudiante representa estructuras de información mediante grafos y árboles.

En el cuarto tema el estudiante conocerá los conceptos básicos de la teoría de números necesarios para comprender los algoritmos modernos de criptografía de clave pública y su seguridad.
En el quinto tema, el estudiante conocerá conceptos de álgebra modular esenciales para la comprensión de la criptografía, así como de la codificación de la información.

3. Participantes en el diseño y seguimiento curricular del programa

Lugar y fecha de elaboración o revisión	Participantes	Observaciones
Tecnológico Nacional de México del 4 al 6 de marzo del 2024.	Representantes de los Institutos Tecnológicos de: Aguascalientes, Cerro Azul, Ciudad Juárez, La Paz, Jiquilpan, Mérida, Morelia, Tuxtla Gutiérrez, Villahermosa. Institutos Tecnológicos Superiores de La Región Carbonífera, Las Choapas	Propuesta sintética de la carrera de Ingeniería en Ciberseguridad.
Tecnológico Nacional de México del 22 al 26 de abril del 2024.	Representantes de los Institutos Tecnológicos de: Aguascalientes, Cerro Azul, Ciudad Juárez, La Paz, Jiquilpan, Mérida, Morelia, Tuxtla Gutiérrez, Villahermosa. Institutos Tecnológicos Superiores de La Región Carbonífera, Las Choapas. Representante de Ciencias Básica de los Institutos de: Celaya, Morelia CENIDET y CIIDET.	Diseño y/o desarrollo curricular de la carrera de Ingeniería en Ciberseguridad
Tecnológico Nacional de México del 27 al 31 de mayo del 2024.	Representantes de los Institutos Tecnológicos de: Aguascalientes, Cerro Azul, Jiquilpan, Mérida, Villahermosa. Institutos Tecnológicos Superiores de La Región Carbonífera, Las Choapas	Consolidación curricular de la carrera de Ingeniería en Ciberseguridad.

4. Competencia(s) a desarrollar

Competencia(s) específica(s) de la asignatura
• Identifica las estructuras básicas de las matemáticas discretas para aplicarlas en el manejo, tratamiento y seguridad de la información.

5. Competencias previas

- Identifica aspectos elementales de los números naturales, reales, enteros.
- Aplica álgebra elemental.

6. Temario

No.	Temas	Subtemas
1	Bases aritméticas.	1.1. Bases aritméticas. 1.2. Representación de enteros en diferentes bases. 1.3. Conversión a diferentes bases. 1.4. Aritmética de enteros en diferentes bases.
2	Lógica y conjuntos.	2.1. Expresiones lógicas. 2.2. Tablas de verdad. 2.3. Equivalencias proposicionales. 2.4. Predicados y cuantificadores. 2.5. Cuantificadores anidados. 2.6. Métodos de demostración. 2.7. Conjuntos. 2.8. Operaciones con Conjuntos. 2.9. Funciones
3	Grafos y árboles.	3.1. Familias de grafos. 3.2. Representación de grafos. 3.3. Conexión. 3.4. Caminos de longitud mínima. Algoritmo de Dijkstra. 3.5. Definición de árboles. 3.6. Árboles generadores. 3.7. Recorrido de árboles
4	Introducción a la teoría de números.	4.1. Divisibilidad. 4.2. Máximo común divisor. 4.3. Números primos. 4.4. Teorema fundamental de la aritmética. 4.5. Algoritmo de Euclides. 4.6. Problema de la factorización en primos

5	Congruencias y aritmética modular.	5.1. Definición de congruencias. 5.2. Propiedades básicas de congruencias. 5.3. Teorema chino del residuo. 5.4. Campos finitos GF(p^n), GF(2^n). 5.5. Inversos y MCD. 5.6. Problema del logaritmo discreto. 5.7. Aritmética de puntos sobre una curva elíptica

7. Actividades de aprendizaje de los temas

1. Bases aritméticas.	
Competencias	Actividades de aprendizaje
Específica(s): Aplicar los diferentes sistemas numéricos, como el binario, octal y hexadecimal. *Genérica(s):* ● Habilidad de aplicar los conocimientos en la práctica. ● Habilidades en el uso de las tecnologías de la información y comunicaciones. ● Habilidad de investigación. ● Habilidad de aprender y actualizarse permanentemente. Transversal(es): ● Aplica los conocimientos en la práctica, identificando aquellos que incorporen el compromiso con la responsabilidad social. ● Usa comunicación oral y escrita atendiendo los principios de no discriminación, Inclusión y equidad social. ● Diseña e implementa soluciones a problemas propios de ámbito de su área de aplicación integrando aprendizajes, rasgos y capacidades de excelencia, vanguardia e innovación social que fortalezcan el desarrollo humano.	● Diferenciar los tipos de sistemas numéricos para identificar el uso de los sistemas numéricos posicionales. ● Investigar los tipos de sistemas numéricos. ● Realizar ejercicios de conversiones entre los diferentes sistemas de numeración. ● Resolver operaciones binarias en complemento a dos. ● Investigar la importancia de los sistemas numéricos y su aplicación en el hardware y software.

2. Lógica y conjuntos.	
Competencias	Actividades de aprendizaje
Específica(s): • Conoce los conceptos básicos de la lógica proposicional, lógica de predicados y álgebra declarativa. • Identifica las propiedades que posee una relación expresada como conjunto de pares ordenados, como una expresión algebraica, de una forma verbal o simbólica. *Genérica(s):* • Habilidad de aplicar los conocimientos en la práctica. • Habilidades en el uso de las tecnologías de la información y comunicaciones. • Habilidad de investigación. • Habilidad de aprender y actualizarse permanentemente. Transversal(es): • Aplica los conocimientos en la práctica, identificando aquellos que incorporen el compromiso con la responsabilidad social. • Usa comunicación oral y escrita atendiendo los principios de no discriminación, Inclusión y equidad social. • Diseña e implementa soluciones a problemas propios de ámbito de su área de aplicación integrando aprendizajes, rasgos y capacidades de excelencia, vanguardia e innovación social que fortalezcan el desarrollo humano.	• Investigar el concepto de argumento, proposición y proposición lógica. • Presentar ejemplos de proposiciones lógicas. • Elaborar un esquema con los tipos de conexiones lógicas, su representación y tabla de verdad. • Representar enunciados usando para ello notación lógica. • Analizar ejemplos de evaluación de proposiciones lógicas compuestas mediante tablas de verdad. • Investigar las reglas de inferencia. • Realizar ejercicios en donde se apliquen las reglas de inferencia. • Discutir las diferencias entre tautologías, • Contradicciones y contingencias. • Investigar la aplicación del álgebra declarativa y la inducción matemática. • Investigar qué es un conjunto, los tipos de conjuntos y sus elementos. • Investigar las operaciones básicas de los conjuntos. • Construir diagramas de Venn. • Analizar el álgebra de conjuntos y dar solución a problemas reales. • Investigar los conceptos de: producto cartesiano, relación y relación binaria, utilizando diferentes fuentes de información. • Utilizando conjuntos, matrices y diagramas de flechas presentar ejemplos de relaciones. • Investigar otros tipos de representación y discutirlas en grupos de trabajo. • Identificar las diferentes operaciones que pueden realizarse entre relaciones: unión, intersección, complemento, inversa y composición, resolver ejercicios en grupos de trabajo.

	• Hacer que una relación que no tenga la propiedad de equivalencia adquiera esta propiedad aplicando las cerraduras reflexiva, simétrica y transitiva.
3. Grafos y árboles.	
Competencias	Actividades de aprendizaje
Específica(s): • Aplica los conceptos básicos de grafos para resolver problemas afines al área computacional, relacionados con el recorrido y búsqueda en grafos. • Representa estructuras de información mediante grafos. • Reconoce las estructuras de datos jerárquicas (árboles). • Realiza ordenaciones y búsquedas utilizando árboles. *Genérica(s):* • Habilidad de aplicar los conocimientos en la práctica. • Habilidades en el uso de las tecnologías de la información y comunicaciones. • Habilidad de investigación. • Habilidad de aprender y actualizarse permanentemente. Transversal(es): • Aplica los conocimientos en la práctica, identificando aquellos que incorporen el compromiso con la responsabilidad social. • Usa comunicación oral y escrita atendiendo los principios de no discriminación, Inclusión y equidad social.	• Investigar en diferentes fuentes de información los elementos y características de los grafos (vértice, arista, lazos, valencias, caminos) • Formar mesas de discusión de los temas investigados con la finalidad de enriquecer el conocimiento. • Realizar un cuadro sinóptico de los diferentes tipos de grafos, sus características y ejemplos de cada uno de ellos. • Investigar cómo se representan los grafos utilizando matrices e identificar las razones por las cuales se utilizan cada una de las representaciones. • Representar grafos mediante matrices. • Investigar los diferentes algoritmos para el cálculo del número de caminos en un grafo, así como el camino más corto. • Resolver ejercicios utilizando los diferentes algoritmos para el cálculo de caminos en un grafo, así como para encontrar el camino más corto. • Investigar algoritmos de recorrido y búsqueda existentes. • Exponer en clase por equipos los algoritmos de recorrido y búsqueda investigados. • Realizar ejercicios de grafos en la que se aplique búsqueda de información a lo ancho y en profundidad. • Investigar los conceptos básicos de árboles y sus propiedades. • Discutir en el grupo sobre la estructura jerárquica de los árboles. • Realizar un reporte de las conclusiones obtenidas en la discusión grupal.

• Diseña e implementa soluciones a problemas propios de ámbito de su área de aplicación integrando aprendizajes, rasgos y capacidades de excelencia, vanguardia e innovación social que fortalezcan el desarrollo humano.	• Resolver ejercicios para encontrar los árboles generadores de un grafo, así como el generador mínimo. • Investigar el uso de los árboles para realizar ordenaciones y búsquedas de datos. • Investigar los diferentes algoritmos para realizar el recorrido de un árbol y la ordenación y búsqueda de los elementos. • Elaborar un cuadro sinóptico de los algoritmos de recorrido, ordenación y búsqueda. • Resolver ejercicios para el recorrido de árboles en preorden, inorden y postorden. • Investigar las aplicaciones de los recorridos de árboles en el área de las ciencias computacionales. • Estructurar la información en un árbol para llevar a cabo evaluación de ecuaciones matemáticas y ordenamiento de información por medio de sus diferentes recorridos.
4. Introducción a la teoría de números.	
Competencias	Actividades de aprendizaje
Específica(s): • Identifica los fundamentos matemáticos de la Criptografía. • Identifica algunos algoritmos de factorización y de números primos en Criptografía. *Genérica(s):* • Habilidad de aplicar los conocimientos en la práctica. • Habilidades en el uso de las tecnologías de la información y comunicaciones. • Habilidad de investigación. • Habilidad de aprender y actualizarse permanentemente.	• Aplicar el algoritmo de Euclides para obtener el máximo común denominador de pares de números enteros. • Utilizar la criba de Eratóstenes para generar números primos. • Investigar sobre los algoritmos existentes para factorización de enteros en números primos. • Investigar sobre el uso de los números primos para la generación de claves criptográficas. • Investigar sobre la factorización de los números primos y su relación con la seguridad de la criptografía de clave pública.

Transversal(es): • Aplica los conocimientos en la práctica, identificando aquellos que incorporen el compromiso con la responsabilidad social. • Usa comunicación oral y escrita atendiendo los principios de no discriminación, Inclusión y equidad social. • Diseña e implementa soluciones a problemas propios de ámbito de su área de aplicación integrando aprendizajes, rasgos y capacidades de excelencia, vanguardia e innovación social que fortalezcan el desarrollo humano.	
5. Congruencias y aritmética modular.	
Competencias	Actividades de aprendizaje
Específica(s): • Identifica los fundamentos matemáticos de la Criptografía. • Identifica la relevancia de la aritmética modular en la Criptografía y en la Teoría de Códigos. *Genérica(s):* • Habilidad de aplicar los conocimientos en la práctica. • Habilidades en el uso de las tecnologías de la información y comunicaciones. • Habilidad de investigación. • Habilidad de aprender y actualizarse permanentemente.	• Realizar cálculos aritméticos modulares para enteros modulo un primo grande. • Investigar y utilizar algoritmos para la obtención de logaritmos discretos. • Investigar sobre la aplicación de la aritmética modular en los protocolos de autenticación. • Investigar sobre la aplicación de la aritmética modular en la criptografía de clave pública. • Investigar sobre la relación entre el problema del logaritmo discreto y la seguridad de la criptografía de clave pública. • Investigar sobre la aplicación de la aritmética modular en los códigos para detección y corrección de errores.

Transversal(es): • Aplica los conocimientos en la práctica, identificando aquellos que incorporen el compromiso con la responsabilidad social. • Usa comunicación oral y escrita atendiendo los principios de no discriminación, Inclusión y equidad social. • Diseña e implementa soluciones a problemas propios de ámbito de su área de aplicación integrando aprendizajes, rasgos y capacidades de excelencia, vanguardia e innovación social que fortalezcan el desarrollo humano.	

8. Práctica(s)

- Utilizar la calculadora para comprobar las conversiones entre sistemas numéricos.
- Realizar investigación sobre la importancia de los sistemas numéricos y su aplicación en el hardware y software.
- Probar si una proposición compuesta es tautología, contradicción o contingencia.
- Realizar ejercicios en donde se apliquen las leyes de inferencia para la solución de problemas.
- Demostrar formalmente la validez de proposiciones.
- Mediante software disponible para el estudiante, determinar características, propiedades y recorridos importantes en un grafo.
- Desarrollar el algoritmo del camino más corto.
- Realizar el recorrido de un árbol que represente una expresión matemática y obtener su valor usando para ello el concepto de pila para almacenar resultados.
- Crear un árbol binario a partir de una lista de números aleatorios y llevar a cabo búsquedas y ordenamiento de dichos datos.
- Usar software disponible para el estudiante, con el cual se simule el recorrido, búsqueda de información, representación y evaluación de un árbol.
- Utilizar software para realizar factorización de enteros en número primos.
- Aplicar la factorización de primos para el rompimiento de claves públicas.

9. Proyecto de asignatura

El objetivo del proyecto que planteé el docente que imparta esta asignatura, es demostrar el desarrollo y alcance del(los) logro(s) formativo(s) de la asignatura, considerando las siguientes fases:

- **Fundamentación:** marco referencial (teórico, conceptual, contextual, legal) en el cual se fundamenta el proyecto de acuerdo con un diagnóstico realizado, mismo que permite a los estudiantes lograr la comprensión de la realidad o situación objeto de estudio para definir un proceso de intervención o hacer el diseño de un modelo.
- **Planeación:** con base en el diagnóstico en esta fase se realiza el diseño del proyecto por parte de los estudiantes con asesoría del docente; implica planificar un proceso: de intervención empresarial, social o comunitario, el diseño de un modelo, entre otros, según el tipo de proyecto, las actividades a realizar los recursos requeridos y el cronograma de trabajo.
- **Ejecución:** consiste en el desarrollo de la planeación del proyecto realizada por parte de los estudiantes con asesoría del docente, es decir en la intervención (social, empresarial), o construcción del modelo propuesto según el tipo de proyecto, es la fase de mayor duración que implica el desempeño de los saberes, habilidades y destrezas a desarrollar.
- **Evaluación:** es la fase final que aplica un juicio de valor en el contexto laboral-profesión, social e investigativo, ésta se debe realizar a través del reconocimiento de logros y aspectos a mejorar se estará promoviendo el concepto de “evaluación para la mejora continua”, el desarrollo del pensamiento crítico y reflexivo en los estudiantes.

10. Evaluación de saberes, habilidades y destrezas

Para evaluar las actividades de aprendizaje se recomienda solicitar: mapas mentales o conceptuales, reportes de prácticas, tablas comparativas, exposiciones en clase, portafolio de evidencias entre otros. Para verificar el nivel de logro de las competencias del estudiante se recomienda utilizar: listas de cotejo, listas de verificación, matrices de evaluación, guías de observación, rubricas, exámenes prácticos entre otros.

11. Fuentes de Información

1. Koblitz, N. (2014) A Course in Number Theory and Cryptography, 2nd Ed., Springer-Verlag
2. Huertas S. M Lógica y álgebra de Boole Operadores booleanos y tablas de verdad
3. Martín, F., Sánchez, J.L., Paniagua, E. (2003). Lógica computacional. Paraninfo.
4. Roth, C.H. (2005). Fundamentos de diseño lógico. Thomson.
5. Rosen, K. (2018) Discrete Mathematics and Its Applications, 8th ed., McGraw-Hill.
6. Epp, S.S. (2019) Discrete Mathematics with Applications, 5th Ed., Cencage Learning.
7. Asociación Nacional de Instituciones de Educación en Tecnologías de Información A.C. (2024). Modelo curricular por competencias. ANIEI