1. Datos Generales de la asignatura

Nombre de la asignatura:	Criptografía
Clave de la asignatura:	CBD-2412
SATCA[1]:	2-3-5
Carrera:	Ingeniería en Ciberseguridad.

2. Presentación

Caracterización de la asignatura

La Criptografía es el estudio de técnicas matemáticas relacionadas con aspectos de la seguridad de la información. Esta materia se centra en el estudio de los principios y técnicas fundamentales de la criptografía moderna y su aplicación en la seguridad de la información. Esta asignatura abona al perfil de egreso de la carrera de Ingeniería en Ciberseguridad las siguientes competencias:

- 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.
- Propone soluciones para proteger la transmisión y almacenamiento de información sensible dentro de un área funcional o técnica, a partir de marcos de referencia con excelencia, vanguardia e innovación social aplicando mejores prácticas del mercado.

La asignatura es fundamental para la formación de profesionales en Ingeniería en Ciberseguridad, ya que en ella el estudiante explorará los algoritmos de cifrado, métodos de autenticación, protocolos de seguridad y aplicaciones prácticas de la criptografía en entornos digitales.

Intención didáctica

El contenido de esta materia se encuentra distribuido en 4 temas, busca dotar a los estudiantes de conocimientos teóricos y prácticos necesarios para comprender, implementar y utilizar técnicas criptográficas en la protección de la información. Se enfoca en la importancia de la criptografía en el contexto de la ciberseguridad y su aplicación práctica en la industria. Los estudiantes serán capaces de Comprender los fundamentos teóricos y matemáticos de la criptografía, aplicar los diferentes algoritmos criptográficos para proteger información, analizar la seguridad de los sistemas criptográficos y diseñar e implementar soluciones criptográficas para diferentes escenarios.

En el tema 1, el estudiante Introducirá los conceptos básicos de la criptografía, como la terminología, la historia y los diferentes tipos de algoritmos criptográficos. Su objetivo es proporcionar a los estudiantes una comprensión práctica de los principios y técnicas de la criptografía y su aplicación en la seguridad de la información.

[1] Sistema de Asignación y Transferencia de Créditos Académicos

En el tema 2, el estudiante obtendrá conocimiento profundo sobre los algoritmos criptográficos más importantes y su aplicación en la protección de la información. A través de este tema, el estudiante comprenderá los fundamentos de los algoritmos de cifrado simétrico y asimétrico, así como las funciones de hash y las firmas digitales, Adicional a ello, el estudiante adquirirá habilidades prácticas para implementar y utilizar algoritmos criptográficos en la seguridad de sistemas de información y comunicación.

En el tema 3, el estudiante se familiarizará con los protocolos criptográficos utilizados para garantizar la seguridad en la comunicación y el intercambio de información en entornos digitales. En el transcurso de este tema, el estudiante desarrollará la capacidad de evaluar la seguridad y eficacia de estos protocolos, así como de implementarlos correctamente en sistemas y aplicaciones para proteger la confidencialidad, integridad y autenticidad de los datos transmitidos.

Y en el tema 4, el estudiante explotará las diversas aplicaciones prácticas de la criptografía en entornos digitales y de redes. Explorará las diferentes aplicaciones de la criptografía en la vida real, como la seguridad informática, las comunicaciones seguras, las transacciones electrónicas y el blockchain. Durante el desarrollo del tema, el estudiante desarrollará la capacidad de diseñar y desarrollar soluciones criptográficas para garantizar la seguridad de la información en una variedad de contextos y aplicaciones prácticas.

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
• Explica los principios de la criptografía simétrica y asimétrica. • Aplica algoritmos de cifrado y técnicas de autenticación de forma eficiente y segura para proteger la información. • Diseña y desarrolla soluciones criptográficas para garantizar la confidencialidad, integridad y autenticidad de la información.

5. Competencias previas

• Identifica y explica el proceso de comunicación entre dispositivos conectados a una red aplicando normas y estándares vigentes en las redes de datos. • Conoce, comprende y aplica eficientemente estructuras de datos, métodos de ordenamiento y búsqueda para la optimización del rendimiento de soluciones a problemas del mundo real, garantizando la seguridad de la estructura de datos al implementar la validación y el saneamiento de estos. • Explora las tendencias cibernéticas, las amenazas para permanecer seguro en el ciberespacio a fin de proteger los datos personales y empresariales.

6. Temario

No.	Temas	Subtemas
1	Fundamentos de la criptografía.	1.1. Introducción a la criptografía y sus objetivos. 1.2. Conceptos básicos de la criptografía. 1.3. Historia y evolución de la criptografía. 1.4. Tipos de ataques criptográficos y medidas de seguridad.
2	Algoritmos criptográficos.	2.1. Algoritmos de cifrado simétrico. 2.1.1. Algoritmos de cifrado en flujo. 2.1.2. Algoritmos de cifrado en bloque. 2.1.3. Modos de operación. 2.1.4. Seguridad de los algoritmos simétricos. 2.1.5. Problema de la distribución de claves. 2.2. Algoritmos de cifrado asimétrico. 2.2.1. Algoritmos de clave pública. 2.2.2. Intercambio de claves seguras. 2.2.3. Seguridad de los algoritmos asimétricos. 2.3. Funciones de HASH y firmas digitales. 2.4. Certificados digitales y PKI.
3	Protocolos criptográficos	3.1. Protocolos de distribución de clave simétrica. 3.1.1. Protocolo de Needham-Schroeder. 3.1.2. Protocolo Kerberos. 3.2. Protocolos de intercambio de clave pública. 3.2.1. Protocolo de Diffie-Hellman. 3.3. Protocolo SSL/TLS.
4	Aplicaciones de la criptografía	4.1 Criptografía en la seguridad informática. 4.2 Criptografía en sistemas de almacenamiento y transmisión de datos. 4.3 Criptografía en las comunicaciones seguras.

		4.4 Criptografía en dispositivos móviles y redes inalámbricas. 4.5 Criptografía en las transacciones electrónicas. 4.6 Criptografía en blockchain y criptomonedas.

7. Actividades de aprendizaje de los temas

1. Fundamentos de la criptografía	
Competencias	Actividades de aprendizaje
Específica(s): • Comprender los conceptos básicos y la terminología fundamental de la criptografía. • Conocer la historia y evolución de la criptografía. • Identificar y analizar los diferentes tipos de ataques criptográficos *Genérica(s):* ● Capacidad de análisis y síntesis. ● Capacidad de organizar y planificar. ● Habilidad para buscar y analizar información proveniente de fuentes diversas. ● Capacidad de aplicar los conocimientos. ● Capacidad de investigación y autoaprendizaje. *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.	• Lectura de capítulos seleccionados sobre la historia y evolución de la criptografía, seguida de una discusión en clase para profundizar en los conceptos. • Análisis de casos históricos de criptografía, como el Enigma alemán durante la Segunda Guerra Mundial. • Investigación sobre diferentes tipos de ataques criptográficos y sus mecanismos

2. Algoritmos criptográficos	
Competencias	Actividades de aprendizaje
Específica(s): • Entender los principios y aplicaciones de los algoritmos de cifrado simétrico y asimétrico. • Conocer y aplicar funciones hash y firmas digitales *Genérica(s):* • Desarrollar la capacidad de aplicar conocimientos teóricos a situaciones prácticas. • Fomentar el trabajo en equipo y la colaboración. • Desarrollar habilidades técnicas y analíticas *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.	• Implementación de algoritmos de cifrado simétrico (como AES) y asimétrico (como RSA) en un lenguaje de programación. • Realización de prácticas de laboratorio para implementar y utilizar funciones hash (como SHA-256) y firmas digitales. • Comparar y contrastar diferentes algoritmos de cifrado en términos de seguridad y eficiencia.
3. Protocolos criptográficos	
Competencias	Actividades de aprendizaje
Específica(s): • Comprender y aplicar protocolos de autenticación y de cambio de clave.	• Implementación y simulación de protocolos de autenticación y cambio de clave en un entorno controlado. • Configuración práctica de protocolos como SSL/TLS y SSH en servidores y clientes.

• Conocer y utilizar protocolos de seguridad como SSL/TLS, SSH, PGP y otros protocolos de seguridad web. *Genérica(s):* • Desarrollar habilidades de comunicación técnica y presentación. • Fomentar el pensamiento crítico y la resolución de problemas. • Promover la capacidad de análisis y síntesis de información *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.	• Estudio y análisis de cómo funcionan los protocolos de seguridad en la web, como PGP y otros.

4. Aplicaciones de la criptografía	
Competencias	Actividades de aprendizaje
Específica(s): • Aplicar criptografía en diversas áreas de la seguridad informática, almacenamiento, comunicaciones, dispositivos inalámbricos y transacciones electrónicas.	• Desarrollo de proyectos que integren criptografía en la seguridad informática y sistemas de almacenamiento. • Configuración y prueba de sistemas de comunicación segura utilizando criptografía.

• Entender el uso de criptografía en blockchain y criptomonedas. *Genéricas:* • Desarrollar habilidades prácticas y técnicas avanzadas. • Fomentar la innovación y la creatividad en la solución de problemas. • Promover la responsabilidad ética y social en el uso de la criptografía. *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.	• Investigación y análisis del uso de criptografía en blockchain y criptomonedas. • Simulación de transacciones electrónicas seguras utilizando criptografía.

8. Práctica(s)

• Implementación de algoritmos criptográficos en lenguajes de programación
• Implementación de algoritmos de cifrado simétrico y asimétrico
• Análisis de vulnerabilidades en sistemas criptográficos existentes
• Simulación de ataques criptográficos y pruebas de penetración controladas

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 conceptuales, ensayos, reporte de investigación y/o revisiones bibliográficas, reportes de prácticas, estudio de casos, exposiciones en clase, portafolio de evidencias.
- Para verificar el nivel del logro de las competencias del estudiante se recomienda utilizar: listas de cotejo, listas de verificación, matrices de valoración, guías de observación, rúbricas, entre otros.

11. Fuentes de Información

1. Análisis de casos históricos de criptografía, como el Enigma alemán durante la Segunda Guerra Mundial.
2. Stallings, W. (2017). Cryptography and Network Security: Principles and Practice (7th ed.). Pearson.
3. Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (1996). Handbook of Applied Cryptography. CRC Press.
4. Schneier, B. (2015). Applied Cryptography: Protocols, Algorithms, and Source Code in C (20th Anniversary ed.). Wiley.
5. Ferguson, N., Schneier, B., & Kohno, T. (2010). Cryptography Engineering: Design Principles and Practical Applications. Wiley.
6. National Institute of Standards and Technology (NIST). (n.d.). Computer Security Resource Center. Retrieved from https://csrc.nist.gov
7. OWASP Foundation. (n.d.). OWASP Cryptography Cheat Sheet. Retrieved from https://cheatsheetseries.owasp.org/cheatsheets/Cryptographic_Storage_Cheat_Sheet.html
8. Asociación Nacional de Instituciones de Educación en Tecnologías de Información A.C. (2024). Modelo curricular por competencias. ANIEI.