



UASLP
Universidad Autónoma
de San Luis Potosí



**FACULTAD DE
INGENIERÍA**
Área de Ciencias
de la Computación

Clave de la materia: 2826
Clave Facultad: 2826
Clave U.A.S.L.P.: ----
Nivel del Plan de Estudios: I.S.I.: 7
Horas/Clase/Semana: 4
Horas/Práctica (y/o Laboratorio): 0
Prácticas complementarias: 0
Trabajo extra-clase Horas/Semana: 4
Carrera/Tipo de materia: I.S.I./ Electiva de Área de Énfasis
No. de créditos aprobados: 200 créditos del Núcleo Básico
Fecha última de Revisión Curricular: 27-noviembre-2020
Materia y clave de la materia requisito: 2822 – Redes de Computadoras y Seguridad

Clave CACEI: IA
No. de créditos: 8
Horas totales/Semestre: 64

OBJETIVO DEL CURSO

Analizar y aplicar los elementos fundamentales y los sistemas de seguridad. protocolos básicos que permiten construir los actuales

CONTENIDO TEMÁTICO

1. FUNDAMENTOS E HISTORIA DE LA CRIPTOGRAFÍA

Tiempo Estimado: 16 hrs.

Objetivo: Analizar los conceptos esenciales y clásicos de los sistemas de seguridad, incluyendo los sistemas clásicos de cifrado y las correspondientes técnicas criptoanalíticas que los vencieron.

- 1.1. Principios de seguridad informática
- 1.2. Hitos en la criptografía y definición
- 1.3. Las matemáticas en la criptografía
- 1.4. Historia de la criptografía
- 1.5. Algoritmos criptográficos clásicos

2. INTRODUCCIÓN A LA CRIPTOGRAFÍA MODERNA

Tiempo Estimado: 4 hrs.

Objetivo: Analizar los aspectos del cifrado clásico al cifrado moderno.

- 2.1. Del cifrado clásico al moderno
- 2.2. Clasificación del cifrado moderno
- 2.3. Usos de sistemas de cifra híbridos

3. CRIPTOGRAFÍA SIMÉTRICA

Tiempo estimado: 12 hrs.

Objetivo: Conocer y aplicar las propiedades de la criptografía de llave secreta o simétrica; además de analizar sus aplicaciones, técnicas y los algoritmos que la usan.

- 3.1. Cifrado simétrico en flujo
- 3.2. Algoritmos de cifrado simétrico en flujo
- 3.3. Algoritmos de cifrado simétrico en bloque

4. CRIPTOGRAFÍA ASIMÉTRICA

Tiempo estimado: 16 hrs.

Objetivo: Conocer y aplicar las propiedades de la criptografía de llave pública o asimétrica; además de sus aplicaciones, técnicas y los algoritmos que la usan.

- 4.1. Introducción al cifrado asimétrico
- 4.2. Algoritmo RSA
- 4.3. Algoritmo ElGamal
- 4.4. Algoritmo de curva elíptica
- 4.5. Funciones Hash

5. ESTEGANOGRAFÍA Y ESTEGOANÁLISIS

Tiempo estimado: 16 hrs.

Objetivo: Analizar y aplicar las técnicas de esteganografía y el estegoanálisis.

- 5.1. Limitaciones de la criptografía
- 5.2. Historia de la esteganografía
- 5.3. Esteganografía en la actualidad
- 5.4. Usos de esteganografía
- 5.5. Estegoanálisis

METODOLOGÍA

Desarrollo del tema por parte del profesor siguiendo el método de aprendizaje basado en problemas. Se espera que el alumno investigue ciertos temas, siguiendo el

método de aula invertida. Implementar estrategias de trabajo en equipo cuando sea conveniente (aprendizaje colaborativo).

EVALUACIÓN

Se realizarán cuatro exámenes parciales de forma colegiada en las fechas establecidas por la Facultad, de acuerdo con el Reglamento de Exámenes. La calificación de los exámenes parciales estará compuesta por la evaluación del examen parcial (80%) y por otras

actividades (20%), como: tareas, investigaciones, resolución de problemas, ejercicios, etc. La calificación del examen ordinario es el promedio de los cuatro parciales.

BIBLIOGRAFÍA

Bibliografía Básica

Whitman, M., Mattord H., *Principles of Information Security*. 6ª Ed., Cengage Learning, 2017.

Helfrich, J. *Security for Software Engineers*. CRC Press, 2019.

House, N., *The Complete Cyber Security Course*. StationX Ltd, 2017.

Mollin, R. *An Introduction to Cryptography*. 2nd Edition, Chapman, 2007.

Bibliografía Complementaria

Grime, R. *Hacking the Hacker: Learn from the Experts Who Take Down Hackers*. Wiley, 2017.

Bass, L., Clements, P., Kazman, R. *Software Architecture in Practice*. 2nd Edition, Addison-Wesley, 2003.

Wayner, P. *Disappearing Cryptography: Information Hiding: Steganography and Watermarking*. 3rd Edition, Morgan-Kaufmann, 2009.