1. Datos Generales de la asignatura

Nombre de la asignatura:	***Criptografía.***
Clave de la asignatura:	***SIG-1602***
SATCA[1]:	***3-3-6***
Carrera:	***Ingeniería en Sistemas Computacionales***

2. Presentación

Caracterización de la asignatura
Aportación al perfil
Esta asignatura aporta al perfil del egresado la capacidad para el desarrollo de proyectos de tecnología de seguridad de la información, en los que se involucran aspectos que influyen en el resguardo, la integridad, fiabilidad y confidencialidad de la información. Así como entender los procesos de cifrado, sus modos de operación y el contexto en que se usan los algoritmos criptográficos.
Intención didáctica
La asignatura se compone de cinco unidades. La unidad uno aborda los antecedentes históricos, evolución y conceptos fundamentales de la criptografía, así, como sus servicios y componentes inmersos en entornos públicos y privados de los sistemas computacionales. *La unidad dos contempla el conocer, comprender y aplicar las técnicas clásicas de cifrado y, los algoritmos que han sentado las bases de la criptografía moderna.* *En la unidad tres se revisan la importancia de las claves de seguridad, así como, los diferentes mecanismos de generación y distribución de las claves para su correcto manejo y administración.* *En la unidad cuatro se trabajan los algoritmos de criptografía simétrica (clave secreta), estudiando sus características, operaciones matemáticas involucradas, procesos de cifrado y descifrado con el fin de poder aplicar los principales algoritmos simétricos de*

[1] Sistema de Asignación y Transferencia de Créditos Académicos

criptografía.

- *En la unidad cinco se realiza un estudio de la criptografía asimétrica (clave pública) y los procedimientos, herramientas matemáticas en las que se basan los algoritmos, verificando el grado de seguridad y los mecanismos para su funcionamiento para comprender su uso y aplicar los algoritmos asimétricos de la criptografía.*

3. Participantes en el diseño y seguimiento curricular del programa

Lugar y fecha de elaboración o revisión	Participantes	Observaciones
Instituto Tecnológico de Tláhuac, México D.F. 18 de Mayo de 2012. Instituto Tecnológico de Tláhuac, CDMX. 11 de Abril de 2016.	Academia de Sistemas y Computación	Revisión y modificación de contenidos temáticos de las asignaturas que conforman la especialidad.

4. Competencia(s) a desarrollar

Competencia(s) específica(s) de la asignatura
El alumno conocerá, explicará y aplicará los diferentes algoritmos criptográficos, metodologías y técnicas de cifrado que le permitan analizar, diseñar, desarrollar y/o seleccionar mecanismos y herramientas de seguridad de manera ética y profesional orientados a brindar seguridad informática, cuidando en todo momento que el trabajo realizado se enfoque en el bienestar social

5. Competencias previas

Identificar los atributos de la información que pueden Identificar las técnicas de ataque hacia los sistemas informáticos Aplicar la sintaxis de un lenguaje de programación Aplicar un lenguaje orientado a objetos para la solución de problemas. Identificar y aplicar las operaciones de matemáticas, operaciones lógicas, corrimientos, sistemas de numeración, teoría de grupos, teoría de campos Identificar y aplicar operaciones del algebra superior

6. Temario

No.	Temas	Subtemas
1	Panorama general	1.1 Historia de la Criptografía 1.2 Servicios y mecanismos de seguridad 1.3 Ataques 1.4 La arquitectura de Seguridad de OSI
2	Técnicas clásicas de cifrado	2.1 Introducción y clasificación de los sistemas de cifrado 2.2 Operaciones utilizadas 2.2.1 Algoritmos de sustitución 2.2.1.1 Monoalfabética: Cifrado del César 2.2.1.2 Polialfabética: Cifrado de Desplazamiento, Vigenére y Vernam 2.2.2 Algoritmos de Transposición 2.2.2.1 Simple 2.2.2.2 Doble 2.2.2.3 Máscaras rotativas 2.3 Números de claves 2.3.1 Sistemas de una clave 2.3.1.1 Cifradores simétricos 2.3.2 Sistemas de dos claves 2.3.2.1 Cifradores asimétricos 2.4 Formas de procesamiento de datos 2.4.1 Procesadores seriales o en flujo 2.4.2 Procesadores por bloques
3	Gestión de claves	3.1 Políticas de gestión de claves 3.1.1 Motivos 3.1.2 Políticas 3.2 Tipos de claves 3.2.1 Estructural 3.2.2 Maestra 3.2.3 Primaria y Secundaria 3.2.4 De generación de claves 3.2.5 De sesión o de mensaje 3.2.6 De cifrado de archivos 3.3 Generadores y distribución de claves 3.3.1 Generadores pseudoaleatorios 3.3.1.1 Período 3.3.1.2 Distribución de uno's y cero's 3.3.1.3 Imprevisibilidad 3.3.1.4 Estructuras básicas de Generación de claves 3.3.2 KDC (Key Distribution Center)
4	Criptografía simétrica o de clave secreta	4.1 Introducción a la criptografía simétrica 4.1.1 Características de los algoritmos simétricos 4.1.2 Herramientas matemáticas: operaciones lógicas, corrimientos, sistemas

		de numeración, teoría de grupos, teoría de campos y otras. 4.1.3 Principales algoritmos simétricos: IDEA, Blowfish, RC5, DES, 3DES y AES 4.2 DES y 3DES(Data Encryption Standard) 4.2.1 Orígenes 4.2.1.1 Historia 4.2.1.2 Teoría de la información: Técnicas sugeridas por Shannon 4.2.2 Algoritmos de cifrado y descifrado 4.2.2.1 Procesamiento y transformación de claves: diagramas de flujo. 4.2.2.2 Proceso y transformación de los bloques de datos: diagramas de flujo 4.2.3 Aplicación del algoritmo 4.2.3.1 Procesamiento y transformación de claves: caso práctico 4.2.4 Nivel de seguridad que proporcionan 4.3 AES (AdvancedEncryptionSatandard) 4.3.1 Orígenes 4.3.1.1 Historia 4.3.1.2 Campos de Galois 4.3.2 Algoritmos de cifrado y descifrado (claves de 128, 192 y 256 bits) 4.3.2.1 Procesamiento y transformación de claves: diagramas de flujo 4.3.2.2 Procesamiento y transformación de los bloques de datos: diagramas de flujo 4.3.3 Aplicación de los algoritmos 4.3.3.1 Procesamiento y transformación de claves: Caso práctico 4.3.3.2 Procesamiento y transformación de claves: Caso práctico 4.3.4 Nivel de seguridad que proporciona 4.3.4.1 Análisis de los algoritmos
5	Criptografía asimétrica o de clave pública	5.1 Introducción a la Criptografía Asimétrica 5.1.1 Características de los algoritmos asimétricos 5.1.2 Herramientas matemáticas: Algoritmo de Euclides, Teorema de Euclides, Teorema de la División de Euclides, Algoritmo extendido de Euclides, Anillo de Números Enteros Módulo m, Teorema de Euler, Teorema de Fermat, Logaritmos Discretos, Logaritmos Discretos Elípticos, Teoría de Polinomios y otras. 5.1.3 Principales algoritmos asimétricos: Diffie-Hellman, El Gamal, RSA (RivestShamir-Adelman), DSA (Digital

		Signatu-Ra Algorithm), Funciones Hash y Curvas Elípticas 5.2 Diffie-Hellman 5.2.1 Orígenes 5.2.2 El algoritmo y las matemáticas Modulares. 5.3 RSA (Rivest-Shamir-Adelman) 5.3.1 Orígenes 5.3.2 Algoritmo de cifrado y descifrado 5.3.3 Cálculo de claves (pública y privada) 5.3.4 Aplicación del algoritmo 5.4 Funciones Hash 5.4.1 MD4 (MessageDigestAlgorithm) 5.4.2 MD5 (Message Digest Algorithm) 5.4.3 SHA (Standard High Algorithm) 5.4.4 Firmas digitales 5.5 Curvas Elípticas 5.5.1 Grupos abelianos 5.5.2 Curvas elípticas sobre números reales 5.5.3 Descripción geométrica 5.5.4 Descripción algebraica

7. Actividades de aprendizaje de los temas

Unidad 1: Panorama general.	
Competencias	Actividades de aprendizaje
Específica(s): Conocer los antecedentes históricos de la criptografía y su evolución a través del tiempo. Asimismo el alumno entenderá los requerimientos de la seguridad de la información dentro del mundo del cómputo y las redes. **Genéricas:** **Competencias instrumentales:** • Capacidad de abstracción análisis y síntesis. • Capacidad de aplicar los conocimientos en la práctica. **Competencias interpersonales:** • Capacidad de investigación. • Trabajo en equipo. **Competencias sistémicas:** • Capacidad de aplicar los conocimientos en la práctica. • Habilidades de investigación. • Capacidad de aprender. • Habilidad para trabajar en forma autónoma.	El alumno realizará una investigación sobre la historia de la criptografía y su aplicación en la actualidad.
Unidad 2: Técnicas clásicas de cifrado.	
Competencias	Actividades de aprendizaje
Específica(s): Conocer, comprender y aplicar las técnicas clásicas de la criptografía y los principales algoritmos que han sentado las bases de la criptografía moderna. Analiza y selecciona técnicas de cifrado óptimas para su implementación. Analiza y selecciona algoritmos apropiados para optimizar aplicaciones de software para la gestión de claves. Genéricas: **Competencias instrumentales:** • Capacidad de abstracción análisis y síntesis.	El alumno investigara los diferentes algoritmos criptográficos y debatirá las técnicas clásicas aplicadas en los mismos.

• Capacidad de aplicar los conocimientos en la práctica. **Competencias interpersonales:** • Capacidad de investigación. • Trabajo en equipo. **Competencias sistémicas:** • Capacidad de aplicar los conocimientos en la práctica. • Habilidades de investigación. • Capacidad de aprender. Habilidad para trabajar en forma autónoma.	
Unidad 3: Gestión de claves.	
Competencias	Actividades de aprendizaje
Específica(s): Específica(s): Entender la importancia de las claves de seguridad, así como la forma correcta de su manejo, generación, procesamiento y administración. **Genéricas**: **Competencias instrumentales:** • Capacidad de abstracción análisis y síntesis. • Capacidad de aplicar los conocimientos en la práctica. **Competencias interpersonales:** • Capacidad de investigación. • Trabajo en equipo. **Competencias sistémicas:** • Capacidad de aplicar los conocimientos en la práctica. • Habilidades de investigación. • Capacidad de aprender. Habilidad para trabajar en forma autónoma.	El alumno investigará y analizará las diferentes políticas para la gestión de claves de seguridad y su clasificación.
Unidad 4: Criptografía simétrica o de clave secreta.	
Competencias	Actividades de aprendizaje
Específica(s): Conocer, comprender y aplicar los principales algoritmos simétricos de la criptografía. Analiza la complejidad de los algoritmos para argumentar la selección con el fin de optimizar una aplicación.	El alumno trabajara y observará comportamiento de los diferentes algoritmos simétricos, la transformación de claves y su procesamiento.

Conocer e identificar los diferentes sistemas y equipos en los cuales se implementa la criptografía simétrica. Analizar e identifica donde y cuando aplicar criptografía asimétrica. **Genéricas:** **Competencias instrumentales:** • Capacidad de abstracción análisis y síntesis. • Capacidad de aplicar los conocimientos en la práctica. **Competencias interpersonales:** • Capacidad de investigación. • Trabajo en equipo. **Competencias sistémicas:** • Capacidad de aplicar los conocimientos en la práctica. • Habilidades de investigación. • Capacidad de aprender. Habilidad para trabajar en forma autónoma.	
Unidad 5: Criptografía asimétrica o de clave pública.	
Competencias	Actividades de aprendizaje
Específica(s): Conocer, comprender y aplicar los principales algoritmos asimétricos de la criptografía. Analiza la complejidad de los algoritmos para argumentar la selección con el fin de optimizar una aplicación. Conocer e identificar los diferentes sistemas y equipos en los cuales se implementa la criptografía simétrica. Analizar e identifica donde y cuando aplicar criptografía asimétrica. **Genéricas:** **Competencias instrumentales:** • Capacidad de abstracción análisis y síntesis. • Capacidad de aplicar los conocimientos en la práctica. **Competencias interpersonales:**	El alumno trabajara y observará comportamiento de los diferentes algoritmos asimétricos

• Capacidad de investigación. • Trabajo en equipo. **Competencias sistémicas:** • Capacidad de aplicar los conocimientos en la práctica. • Habilidades de investigación. • Capacidad de aprender. Habilidad para trabajar en forma autónoma.	

8. Práctica(s)

PRÁCTICA 1.

1. Defina la criptografía.
2. Defina criptoanálisis.
3. Defina la criptología.
4. ¿Qué es la criptografía de clave privada?
5. ¿Qué es la criptografía de clave pública?
6. ¿Qué es la criptografía clásica y la moderna?
7. ¿Qué es un cifrador?
8. Explique con sus propias palabras el funcionamiento de las dos clases de cifradores.
9. ¿A qué nos referimos con confidencialidad?
10. ¿A qué nos referimos con integridad?

PRÁCTICA 2.

1. Una clave de sesión de Internet para proteger una operación de cifra dura 45 segundos. Si alguien intercepta el criptograma, ¿debemos preocuparnos si sabemos que la próxima vez la clave será otra?
2. Si se prueban todas las combinaciones posibles de una clave para romper un criptograma, ¿qué tipo de ataque estamos realizando?
3. Si protegemos una clave en el extremo emisor, ¿qué buscamos, la confidencialidad o la integridad? ¿Y si en el extremo receptor?
4. ¿Por qué en un sistema simétrico se obtiene la confidencialidad y la integridad al mismo tiempo protegiendo la clave?
5. Explique qué significa que en un sistema de cifra simétrica se obtengan la confidencialidad y la integridad por separado.
6. Si se cifra un mensaje con la clave privada del emisor, ¿qué se obtiene? ¿y si el emisor cifra con la clave pública del receptor?
7. ¿Tiene sentido qué el emisor cifre de forma asimétrica con su clave pública? ¿Qué logramos con ello? ¿Para qué serviría?
8. Queremos comunicarnos 10 usuarios con un sistema de cifra de clave secreta única entre cada dos miembros. ¿Cuántas claves serán necesarias? ¿Es eficiente el sistema? ¿Y si hay un usuario más?

9. Proyecto de asignatura

El objetivo del proyecto que planteé el docente que imparta esta asignatura, es demostrar el desarrollo y alcance de la(s) competencia(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 las competencias genéricas y especificas 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”, la metacognición, el desarrollo del pensamiento crítico y reflexivo en los estudiantes.

10. Evaluación por competencias

Son las técnicas, instrumentos y herramientas sugeridas para constatar los desempeños académicos de las actividades de aprendizaje.

11. Fuentes de información

1. DE LA GUÍA, M. Dolores, et al. Técnicas Criptográficas de Protección de Datos España, Ra-Ma, 1997 2. MENEZES, Alfred J., et al Handbook of Applied Cryptography 5th edition, Canadá, CRC, 2001 3. STALLINGS, William Cryptography and Network Security: Principles and Practices 3rd edition, U.S.A., Pearson Education, 2003 4. MAIORANO, Ariel Horacio Criptografía: técnicas de desarrollo para profesionales 1a edición – Buenos Aires, - Alfaomega Grupo Editor 5. STALLINGS, William Fundamentos de seguridad en redes. Aplicaciones y estándares. 2da edición, Pearson Educación, S.A. Madrid, 2004 6. STINSON, Douglas Cryptography: Theory and Practice Chapman & Hall / CRC, Taylor & Francis Group