1.-DATOS DE LA ASIGNATURA

Nombre de la asignatura:	**TEMAS SELECTOS DE APLICACIONES CRIPTOGRÁFICAS.**
Carrera:	**Ingeniería en Tecnologías de la Información y Comunicaciones.**
Clave de la asignatura:	
SATCA[1]:	**2-3-5**

2.-PRESENTACIÓN

Caracterización de la asignatura

Esta asignatura aporta al perfil del Ingeniero en Tecnologías de la información y comunicaciones la capacidad de utilizar aplicaciones y herramientas, actuales y/ó emergentes, acordes a las necesidades del entorno y de información de los sistemas informáticos para plantear soluciones a problemas específicos de protección de datos y seguridad de la información.

Puesto que esta materia requiere de competencias desarrolladas anteriormente en el adecuado desarrollo profesional, se requiere el amplio conocimiento de algún lenguaje de programación orientado a objetos, matemáticas discretas y los fundamentos de seguridad de redes de computadoras.

Intención didáctica

Estaasignatura se compone de cuatro unidades; cada unidad plantea contenidos específicos que se aplican en el campo laboral.

La unidad I incluye conceptos básicos de la criptografía.

La unidad II plantea el estudio de firmas digitales.

La unidad III aborda un panorama general de los certificados digitales.

En la unidad IV se promueve el uso de una herramienta criptográfica para el cifrado de correo electrónico de nombre PGP.

Finalmente en la unidad V, se muestran algunas aplicaciones de la criptografía a través del planteamiento y análisis de algunos casos prácticos.

[1] **Sistema de Asignación y Transferencia de Créditos Académicos**

3.-COMPETENCIAS A DESARROLLAR

Competencias especificas:	**Competencias genéricas**
Analizar los conceptos y principios de la criptografía. Comprender el esquema de firmas digitales y su aplicación en los sistemas informáticos. Comprender el esquema de certificados digitales y su aplicación en los sistemas informáticos. Implementar técnicas de cifrado en el envío y recepción de correos electrónicos a través de PGP. Entender el la importancia de la criptografía en la protección de datos a través de ejemplos prácticos.	*Competencias instrumentales* • Pensamiento lógico, algorítmico,heurístico, analítico y sintético. • Capacidad de análisis y síntesis. • Capacidad de diseñar modelos abstractos. • Procesar e interpretar datos. • Representar e interpretar conceptos en diferentes formas: Gráfica, escrita y verbal. • Habilidades básicas para elaborar diagramas. • Solución de problemas. • Potenciar las habilidades para implementar las redes en las tecnologías web • Toma de decisiones. • Lectura en idioma inglés. *Competencias interpersonales* • Capacidad crítica y autocrítica. • Trabajo en equipo. • Habilidades interpersonales. • Compromiso ético. *Competencias sistémicas* • Habilidad de planificar como un todoy diseñar nuevos sistemas. • Aplicar conocimientos a la práctica. • Capacidad de aplicar losconocimientos en la práctica. • Habilidades de investigación. • Capacidad de aprender. • Creatividad. • Habilidad para trabajar en formaautónoma. • Búsqueda del logro.

4.-HISTORIA DEL PROGRAMA

Lugar y fecha de elaboración o revisión	Participantes	Evento
Instituto Tecnológico de Tlahuac II	Academia de Ingeniería en Tecnologías de la Información y Comunicaciones	Reunión de docentes de la academia de Ingeniería en TIC´S

5.-OBJETIVO GENERAL DEL CURSO (competenciasespecíficas a desarrollar en el curso)

Comprender el uso de algunas aplicaciones criptográficas y su importancia en problemas específicos de seguridad de la información.

6.-COMPETENCIAS PREVIAS

- Habilidad para el manejo de la computadora.
- Manejo de software de cálculo simbólico.
- Manejo de software de simulación.
- Capacidad de análisis y síntesis.
- Aplicar el uso de comandos y teclas rápidas de algunas herramientas de software.
- Contar con experiencia en solución de problemas informáticos.
- Aplicar la informática en concreto: instalación de aplicaciones, uso de editores de texto, gestión de archivo y directorios.
- Diseño, modelado e instalación de redes de computadoras.
- Aplicar lógica matemática en la solución de problemas informáticos.
- Uso de la programación orientada a objetos y estructural.

7.-TEMARIO

Unidad	Temas	Subtemas
Unidad I	**INTRODUCCIÓN A LA CRIPTOGRAFÍA**	1.1. Panorama general. 1.2. Cifradores de bloque; los principios de confusión y difusión de Shannon. 1.3. Secrecía perfecta, cifradores de flujo, uno a la vez (One -Time pad). 1.4. Funciones Hash. 1.5. Integridad del mensaje usando criptografía simétrica. 1.6. Criptosistemas de llave pública. 1.7. El esquema de intercambio de llave de Diffie-Hellman. 1.8. Criptografía cuántica. 1.9. Gestío de la llave y Kerberos. 1.10. Algoritmo DES. 1.11. Ejercicios prácticos.
UNIDAD II	**FIRMAS DIGITALES**.	2.1. Mecanismos de firmadigitales. 2.2. Esquema de firma RSA. 2.3. Esquemas de firma digital de FIAT SHAMIR. 2.4. Esquema de firma DSA. 2.5. Firmas digitales con funcionalidad adicional.
UNIDAD III	**CERTIFICADOS DIGITALES**	3.1. Autoridad certificarora. 3.2. Certificado digital. 3.3. Componentes de un certificado digital. 3.4. Creación de certificados digitales. 3.5. Lista de certificados revocados. 3.6. Certificados X.509
UNIDAD IV	**PGP**	4.1. Fundamentos e historia de PGP. 4.2. Estructura de PGP. 4.3. Otros PGP. 4.4. Vulnerabilidades de PGP.
UNIDAD V	**APLICACIONES DE LA CRIPTOGRAFÍA**	5.1. Autenticación e identificación. 5.2. Esquemas de compartición de secretos. 5.3. Situaciones de confianza mutua. 5.4. Dinero electrónico. 5.5. Elecciones electrónicas. 5.6. Expectativas a futuro.

8.-SUGERENCIAS DE EVALUACIÓN

- Utilizar software didáctico y software de apoyo.
- Presentar proyectos finales.
- Propiciar el uso de terminología técnica adecuada al programa.

- Definir los lineamientos de documentación que deberán contener las Tareas y prácticas.
- Desarrollar de manera conjunta ejemplos de cada uno de los temas.
- Utilizar el aprendizaje basado en problemas, trabajando en grupos pequeños, para sintetizar y construir el conocimiento necesario para resolver problemas relacionados con situaciones reales.
- Elaboración de las prácticas solicitadas por el profesor.
- Propiciar que el estudiante participe aportando propuestas de problemas reales a resolver y que sean significativas para su aprendizaje.
- Fomentar el trabajo en equipo.
- Elaborar de manera conjunta con el estudiante una guía de ejercicios para actividades extra clase.
- Uso del laboratorio para la elaboración de prácticas que integren los temas estudiados.
- Formar equipos de trabajo para la exposición de investigaciones y tareas.
- Generar problemas prácticos y completos y solicitar la solución de aplicaciones utilizando la computadora.
- Emplear herramientas computacionales para el análisis de algoritmos.
- Uso de un portal de Internet para apoyo didáctico de la materia.

9.-SUGERENCIAS DIDÁCTICAS

Crear actividades de metacognición. Ante la ejecución de una actividad, señalar o identifica el tipo de proceso intelectual que se realizo: una identificación de patrones, un análisis, una síntesis, la creación de un algoritmo de programacion heurístico, etc. Al principio lo hará el profesor, luego será el estudiante quién lo identifique.

Diseñar actividades de observación y experimentación que permitan reconocer el principal funcionamiento de la redes de comunicaciones aplicados al uso de tecnología web.

Construir actividades de búsqueda, selección y análisis de información en distintas fuentes, que permitan reconocer los parámetros de la programación.

Implementar software de programación que actualmente se utilice en el medio productivo referente al Desarrollo de Aplicaciones que funciona en ambiente Web.

Proponer problemas que permitan al estudiante la integración de contenidos de la asignatura y entre distintas asignaturas, para su análisis y solución.

Cuando los temas lo requieran, utilizar tutoriales y videos para una mejor comprensión del tema.

Propiciar el uso de las nuevas tecnologías en el desarrollo e implantación de sistemas.

10.-UNIDADES DE APRENDIZAJE

Unidad1:Introducción a la criptografía.

Competencia especifica a desarrollar	Actividades de Aprendizaje
Analizar los conceptos y principios de la criptografía.	Consultar fuentes de informacion que permitan conocer los fundamentos de la criptografía Consultar fuentes de información sobre los conceptos básicos de seguridad de la información. Buscar y seleccionar información sobre protocolos criptográficos. Buscar, discutir y seleccionar los protocolos de criptografía simétrica y asimétrica. Conocer los principios de Shannon respecto a la seguridad de lainformación. Realizar ejercicios práctica que permitan entender la idea general de la criptografía.

Unidad 2:Firmas digitales.

Competencia especifica a desarrollar	Actividades de Aprendizaje
Comprender el esquema de firmas digitales y su aplicación en los sistemas informáticos.	• Realizar un estudio del esquemade firma digital. • Buscar y seleccionar información sobrelos tipos de firma digital. • Buscar información referente a la aplicación de firmas digitales. • Buscar y seleccionar información sobre la configuración del soporte de un esquema de firma digital. • Elaborar un mapa conceptual sobre lainteracción de las aplicaciones de firma digital.

Unidad 3:Certificados digitales.

Competencia especifica a desarrollar	Actividades de Aprendizaje
Comprender el esquema de certificados digitales y su aplicación en los sistemas informáticos.	•Buscar y seleccionar información para comprender el concepto de certificados digitales. • Investigar sobre los diferentes tipos de certificados digitales. • Entender el concepto de unidad certificadora. • Utilizar una aplicación que integre el uso del esquema de certificados digitales.

Unidad 4:PGP.

Competencia especifica a desarrollar	Actividades de Aprendizaje
Implementar técnicas de cifrado en el envío y recepción de correos electrónicos a través de PGP.	• Buscar y seleccionar información sobre PGP. •Realizar pruebas de cifrado con PGP.

Unidad 5:Aplicaciones de la criptografía

Competencia especifica a desarrollar	Actividades de Aprendizaje
Entender el la importancia de la criptografía en la protección de datos a través de ejemplos prácticos.	• Hacer uso de aplicaciones que permitan aplicar técnicas criptográficas sobre casos específicos. • Realizar pruebas de cifrado /descifrado.

11.-FUENTES DE INFORMACIÓN

1. Konheim A. G, *Computer Security and Cryptography*, Wiley-Interscience, 2007

2. Forouzan B. A, Cryptography and Network Security, McGraw-Hill Science/Engineering/Math; 1st Edition, 2007.

3. Delfs H, Knebl H, Introduction to Cryptography: Principles and Applications (Information Security and Cryptography), Springer; 2nd Edition, 2007

4. Stallings W, *Cryptography and Network Security*, 4th Edition, 2005

5. Henk C.A. van Tilborg, *Enciclopedya of Cryptography and Security*, Springer, 2005

6. Mao W, *Modern Cryptography: Theory and Practice,* Prentice Hall PTR, 1st Edition, 2003.
7. Ferguson N, Schneier B, *Practical Cryptography,* Wiley, 2003

8. Menezes, P. Van, Oorschot, and S. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1996.

9. Bruce Schneier, *Applied Cryptography: Protocols Algorithms and Source Code in C*, Second Edition, John Wiley & Sons, INC, 1996.

10. Douglas R Stinson, *Cryptography Theory and Practice*, CRC, 1995.

12.-PRÁCTICAS PROPUESTAS

- Desarrollar ejercicios prácticos sobre seguridad de la información.
- Configurar una sesión de PGP para envío y recepción de correo electrónico seguro.
- Visualizar un esquema de firma digital de manera práctica.
- Aplicar el esquema de certificado digital en una sesión cliente servidor.
- Implementar técnicas criptográficas para la protección de datos.
- Implementar algoritmos criptográficos en las bases de datos.