PLAN DE ESTUDIOS (PE): LICENCIATURA EN CIENCIAS DE LA COMPUTACIÓN

AREA: Optativa

ASIGNATURA: Criptografía

CÓDIGO: CCOM-612

CRÉDITOS: 5 créditos

FECHA: 16 de Mayo de 2013

1. DATOS GENERALES

Nivel Educativo:	Licenciatura
Nombre del Plan de Estudios:	Licenciatura en Ciencias de la Computación
Modalidad Académica:	Presencial
Nombre de la Asignatura:	Criptografía
Ubicación:	Formativo
Correlación:	
Asignaturas Precedentes:	Redes de Computadoras
Asignaturas Consecuentes:	Ninguna
Conocimientos, habilidades, actitudes y valores previos:	**Conocimientos** • Diseño de redes LAN y WAN • Protocolos TCP/IP • Programación en red **Habilidades** • Creatividad para establecer algo nuevo a problemas planteados • Innovación para mejorar lo existente en redes • Trabajo en equipo para enfrentar los retos tecnológicos y sociales • Capacidad de investigar y hacer juicios críticos • Aprender por sí mismo • Comunicar lo aprendido • Resolver problemas **Actitudes y valores** • Actitud para aprender los nuevos conocimientos y realizar innovaciones • Búsqueda de la verdad • Trabajar con respeto y empatía con las personas • Honestidad y responsabilidad • Liderazgo y humanismo

	• Actitud participativa

2. CARGA HORARIA DEL ESTUDIANTE

Concepto	Horas por periodo		Total de horas por periodo	Número de créditos
	Teoría	Práctica		
Horas teoría y práctica Actividades bajo la conducción del docente como clases teóricas, prácticas de laboratorio, talleres, cursos por internet, seminarios, etc. **(16 horas = 1 crédito)**	**48**	**32**	**80**	**5**
Total	**48**	**32**	**80**	**5**

3. REVISIONES Y ACTUALIZACIONES

Autores:	Verónica Edith Bautista López Miguel Ángel León Chávez José Esteban Torres León
Fecha de diseño:	1 de Junio de 2009
Fecha de la última actualización:	16 de Mayo de 2013
Fecha de aprobación por parte de la academia de área	*16 de mayo de 2013*
Fecha de aprobación por parte de CDESC-UA	*30 de mayo de 2013*
Fecha de revisión del Secretario Académico	*3 de junio de 2013*
Revisores:	Miguel Ángel León Chávez Bárbara Sánchez Rinza Edna Iliana Tamariz Flores
Sinopsis de la revisión y/o actualización:	1. Se definió una nueva unidad, “Introducción a la teoría de números”, antes de la unidad tres, “Criptografía de llave pública”, debido a la falta de fundamento matemático que existía para el estudio de los algoritmos de llave pública. 2. Se modificó el nombre de la última unidad, antes “Tópicos en criptografía” por “Aplicaciones”, debido a que no sólo la criptografía se implementa en hardware, sino está la aplicación en software. Asimismo el objetivo específico se cambió. 3. Con respecto a la bibliografía, se tomó como base el libro de [Stallings, 2011]

4. PERFIL DESEABLE DEL PROFESOR (A) PARA IMPARTIR LA ASIGNATURA:

Disciplina profesional:	Redes de Computadoras y Tecnologías inalámbricas
Nivel académico:	Maestría
Experiencia docente:	Mínima de 2 años
Experiencia profesional:	Mínima de 1 año

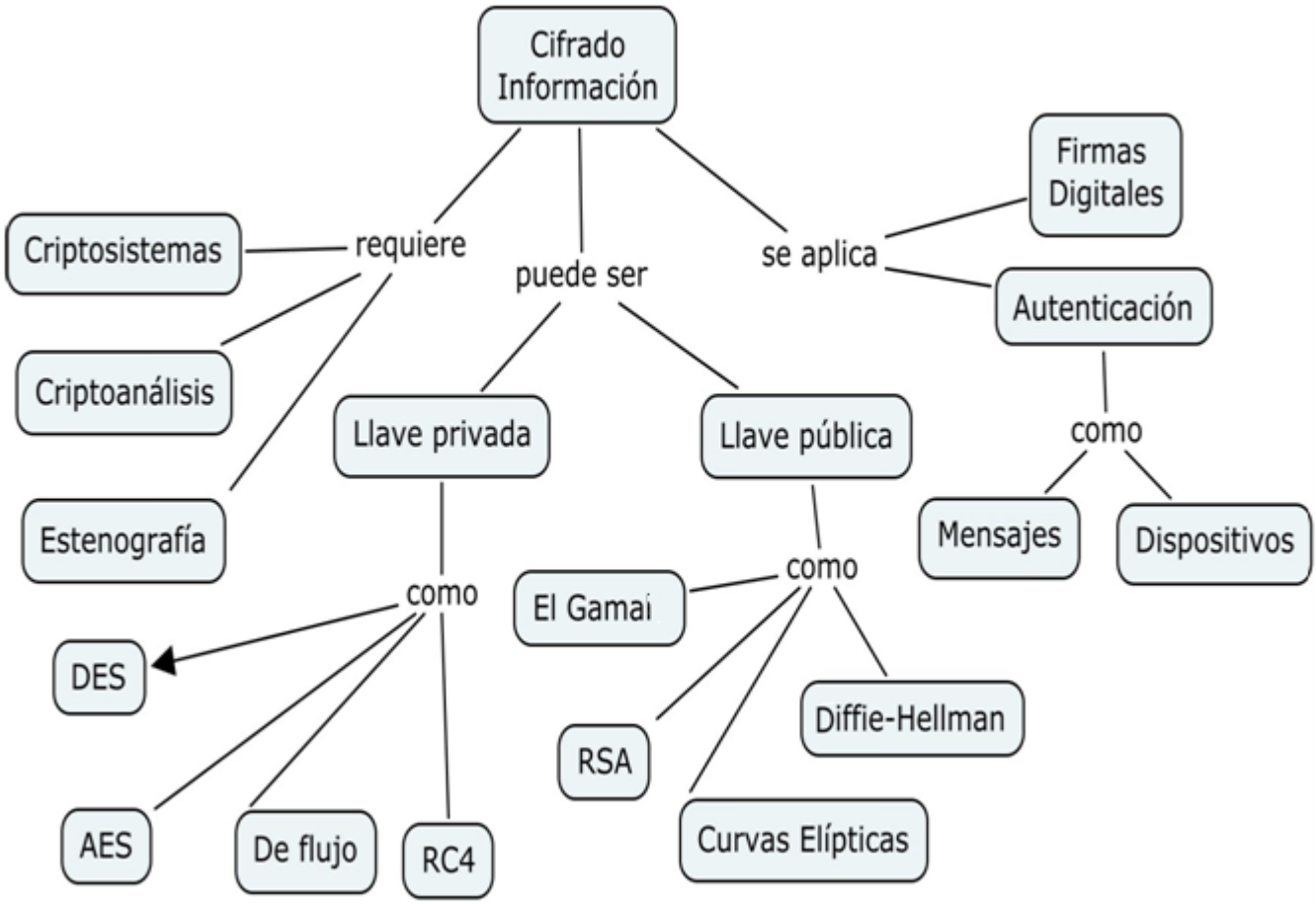
5. OBJETIVOS:

5.1 **General:** Interpretar los diferentes modelos criptográficos que existen, para dar seguridad a la información que fluye en las redes de computadoras, implementando dichos modelos en hardware o software para aplicaciones básicas de redes.

5.2 Específicos:

- Definir una comunicación segura, así como los diferentes ataques que existen a la información y las técnicas clásicas para proteger u ocultar información respecto de observadores no autorizados.
- Identificar los métodos de cifrado de llave privada o algoritmos simétricos que existen: por bloque o por flujo, considerando la implementación de ellos en plataformas de hardware o software.
- Estudiar la teoría de números para el diseño de los algoritmos criptográficos de llave pública.
- Identificar los métodos de cifrado de llave pública o algoritmos asimétricos que hay en la actualidad. De cómo estos se utilizan para cifrar información en redes inseguras y cómo se utilizan para la autentificación.
- Identificar los métodos de autenticación existentes para mensajes, usuarios o dispositivos, para comprobar de manera segura una característica de un objeto utilizando algoritmos asimétricos para crear firmas digitales.
- Identificar nuevas técnicas de aplicación en software así como en hardware.

6. REPRESENTACIÓN GRÁFICA DE LA ASIGNATURA:



7. CONTENIDO

Unidad	Objetivo Específico	Contenido Temático/Actividades de aprendizaje	Bibliografía	
			Básica	**Complementaria**
1. Fundamentos criptográficos y criptografía clásica	Definir una comunicación segura así como los diferentes ataques que existen a la información y las técnicas clásicas para proteger u ocultar información respecto de observadores no autorizados.	1.1 Introducción 1.1.1 Criptografía 1.1.2 Criptosistema 1.1.3 Esteganografía 1.1.4 Criptoanálisis 1.1.5 Criptosistema y Criptoanálisis 1.1.6 Seguridad 1.2 Definición de comunicación segura. 1.3 Ataques a criptosistemas. 1.4 Técnicas y algoritmos clásicos de cifrado.	1. Stallings, W. (2011). Cryptography and Network Security (5th edition). USA: Pearson Education. 2. Menezes, A., van Oorschot, P., & Vanstone, S. (1996). Handbook of Applied Cryptography. (1st edition). USA: CRC Press. 3. Schneier, B. (1996). Applied Cryptography (2nd edition). USA: John Wiley & sons.	1. Lucena, M. (2003) Criptografía y Seguridad en Computadores (4ª edición). España. 2. Seberry, J., Pieprzyk, J. (1989). Cryptography. An Introduction to Computer Security. Australia: Prentice Hall. 3. Rodriguez, F. Saqib, A., Diaz, A. (2006) Cryptographic Algorithms on Reconfigurable Hardware. USA: Springer.
2. Criptografía de llave	Identificar los métodos de cifrado	2.1 Introducción al cifrado por bloques y por flujo.	1. Stallings, W. (2011). Cryptography and	1. Lucena, M. (2003)

Unidad	Objetivo Específico	Contenido Temático/Actividades de aprendizaje	Bibliografía	
			Básica	**Complementaria**
privada	de llave privada o algoritmos simétricos que existen: por bloque o por flujo, considerando la implementación de ellos en plataformas de hardware o software.	2.2 Cifrados por bloques. 2.2.1 Cifrado de producto. 2.2.2 Algoritmo DES y variantes. 2.2.3 Algoritmo IDEA. 2.2.4 Algoritmo AES y variantes. 2.3 Cifrado por flujo 2.3.1 Secuencias pseudoaleatorias. 2.3.2 Generadores de secuencias. 2.3.3 Registros de desplazamientos retroalimentados. 2.3.4 Otros generadores de secuencia. Algoritmos RC4 y SEAL.	Network Security (5th edition). USA: Pearson Education. 2. Menezes, A., van Oorschot, P., & Vanstone, S. (1996). Handbook of Applied Cryptography. (1st edition). USA: CRC Press. 3. Schneier, B. (1996). Applied Cryptography (2nd edition). USA: John Wiley & sons.	Criptografía y Seguridad en Computadores (4ª edición). España. 2. Seberry, J., Pieprzyk, J. (1989). Cryptography. An Introduction to Computer Security. Australia: Prentice Hall. 3. Rodriguez, F. Saqib, A., Diaz, A. (2006) Cryptographic Algorithms on Reconfigurable Hardware. USA: Springer.
3.Introducción a la teoría de números	Estudiar la teoría de números para el diseño de los algoritmos criptográficos de llave pública.	3.1 Números Primos. 3.2 Teoremas de Fermat y Euler. 3.3 Pruebas de primalidad. 3.4 Álgebra modular.	1. Stallings, W. (2011). Cryptography and Network Security (5th edition). USA: Pearson Education. 2. Menezes, A., van	1. Lucena, M. (2003) Criptografía y Seguridad en Computadores (4ª edición).

Unidad	Objetivo Específico	Contenido Temático/Actividades de aprendizaje	Bibliografía	
			Básica	**Complementaria**
		3.5 El teorema del residuo chino. 3.6 Logaritmos discretos.	Oorschot, P., & Vanstone, S. (1996). Handbook of Applied Cryptography. (1st edition). USA: CRC Press. 3. Schneier, B. (1996). Applied Cryptography (2nd edition). USA: John Wiley & sons.	España. 2. Seberry, J., Pieprzyk, J. (1989). Cryptography. An Introduction to Computer Security. Australia: Prentice Hall. 3. Rodriguez, F. Saqib, A., Diaz, A. (2006) Cryptographic Algorithms on Reconfigurable Hardware. USA: Springer.
4. Criptografía de llave pública	Identificar los métodos de cifrado de llave pública o algoritmos asimétricos que hay en la actualidad. De cómo estos se utilizan para cifrar información en	4.1 Introducción a los algoritmos asimétricos. 4.2 Aplicaciones de los algoritmos asimétricos. 4.2.1 Protección de la información. 4.2.2 Autentificación. 4.3 Algoritmos asimétricos. 4.3.1 Algoritmo RSA. 4.3.2 Algoritmo Diffie-	1. Stallings, W. (2011). Cryptography and Network Security (5th edition). USA: Pearson Education. 2. Menezes, A., van Oorschot, P., & Vanstone, S. (1996). Handbook of Applied Cryptography. (1st	1. Lucena, M. (2003) Criptografía y Seguridad en Computadores (4ª edición). España. 2. Seberry, J., Pieprzyk, J.

Unidad	Objetivo Específico	Contenido Temático/Actividades de aprendizaje	Bibliografía	
			Básica	**Complementaria**
	redes inseguras y cómo se utilizan para la autentificación.	Hellman. 4.3.3 Algoritmo El Gamal. 4.3.4 Algoritmo Rabin. 4.3.5 Algoritmo DSA. 4.3.6 Algoritmo Curvas Elípticas. 4.3.7 Protocolos SSL y TLS.	edition). USA: CRC Press. 3. Schneier, B. (1996). Applied Cryptography (2nd edition). USA: John Wiley & sons.	(1989). Cryptography. An Introduction to Computer Security. Australia: Prentice Hall. 3. Rodriguez, F. Saqib, A., Diaz, A. (2006) Cryptographic Algorithms on Reconfigurable Hardware. USA: Springer.
5.Autenticación y Firmas digitales	Identificar los métodos de autenticación existentes para mensajes, usuarios o dispositivos, para comprobar de manera segura una característica de un objeto utilizando algoritmos asimétricos para crear firmas digitales.	5.1 Funciones de autentificación de mensajes (Funciones Hash). 5.2 Autentificación de dispositivos. 5.3 Autentificación de usuario mediante contraseña. 5.3.1 Ataques mediante diccionarios. 5.3.2 Dinero digital. 5.3.3 Esteganografía.	1. Stallings, W. (2011). Cryptography and Network Security (5th edition). USA: Pearson Education. 2. Menezes, A., van Oorschot, P., & Vanstone, S. (1996). Handbook of Applied Cryptography. (1st edition). USA: CRC Press. 3. Schneier, B. (1996). Applied Cryptography	1. Lucena, M. (2003) Criptografía y Seguridad en Computadores (4ª edición). España. 2. Seberry, J., Pieprzyk, J. (1989). Cryptography. An Introduction to Computer

Unidad	Objetivo Específico	Contenido Temático/Actividades de aprendizaje	Bibliografía	
			Básica	**Complementaria**
			(2nd edition). USA: John Wiley & sons.	Security. Australia: Prentice Hall. 3. Rodriguez, F. Saqib, A., Diaz, A. (2006) Cryptographic Algorithms on Reconfigurable Hardware. USA: Springer.
6.Aplicaciones	Identificar nuevas técnicas de aplicación en software así como en hardware.	6.1 Algoritmos implementados en FPGAs. 6.2 Aplicaciones en Software. 6.2.1 Voto electrónico. 6.2.2 Dinero electrónico.	1. Stallings, W. (2011). Cryptography and Network Security (5th edition). USA: Pearson Education. 2. Menezes, A., van Oorschot, P., & Vanstone, S. (1996). Handbook of Applied Cryptography. (1st edition). USA: CRC Press. 3. Schneier, B. (1996). Applied Cryptography (2nd edition). USA: John Wiley & sons.	1. Lucena, M. (2003) Criptografía y Seguridad en Computadores (4ª edición). España. 2. Seberry, J., Pieprzyk, J. (1989). Cryptography. An Introduction to Computer Security. Australia: Prentice Hall.

Unidad	Objetivo Específico	Contenido Temático/Actividades de aprendizaje	Bibliografía	
			Básica	**Complementaria**
				3. Rodriguez, F. Saqib, A., Diaz, A. (2006) Cryptographic Algorithms on Reconfigurable Hardware. USA: Springer.

8. CONTRIBUCIÓN DEL PROGRAMA DE ASIGNATURA AL PERFIL DE EGRESO

Asignatura	Perfil de egreso (anotar en las siguientes tres columnas, cómo contribuye la asignatura al perfil de egreso)		
	Conocimientos	**Habilidades**	**Actitudes y valores**
	Identificar los criptosistemas, los ataques que existen a los criptosistemas. Las técnicas y algoritmos clásicos que existen para cifrar.	Crear o establecer un nuevo sistema criptográfico. Cuestionar la información y encontrar las respuestas respecto a los sistemas criptográficos y ataques a la información. Trabajar en equipo. Resolver problemas.	Buscar el bien común al trabajar en equipo. Ser responsable y ético. Apertura al diálogo. Responsabilidad y solidaridad.
	Identificar los principios y métodos de cifrado en la criptografía de llave privada o algoritmos simétricos. Implementar los algoritmos de cifrado por bloque o por flujo en plataformas de hardware o	Trabajar en equipo y comunicar puntos de vista sobre los métodos simétricos para cifrado de información que hay. Resolver problemas.	Buscar el bien común al trabajar en equipo. Ser responsable y ético. Apertura al dialogo. Responsabilidad y solidaridad.

Asignatura	Perfil de egreso (anotar en las siguientes tres columnas, cómo contribuye la asignatura al perfil de egreso)		
	Conocimientos	**Habilidades**	**Actitudes y valores**
	software.		
Criptografía	Estudiar los teoremas que sirven de base para los algoritmos de llave pública.	Trabajar en equipo y comunicar puntos de vista sobre los métodos simétricos para cifrado de información que hay. Resolver problemas.	Buscar el bien común al trabajar en equipo. Ser responsable y ético. Apertura al dialogo. Responsabilidad y solidaridad.
	Identificar los principios y métodos de cifrado que hay para la criptografía de llave pública o algoritmos asimétricos. Implementar algoritmos asimétricos en plataformas hardware o software.	Crear o establecer un nuevo algoritmo de cifrado asimétrico. Cuestionar la información y encontrar respuestas respecto a los algoritmos asimétricos aplicados a la criptografía Trabajar en equipo Resolver problemas	Buscar el bien común al trabajar en equipo. Ser responsable y ético. Apertura al dialogo. Responsabilidad y solidaridad.
	Identifica los principios y métodos para autentificar mensajes, usuarios y dispositivos Aplicar la autentificación para crear firmas digitales.	Cuestionar la información y encontrar respuestas respecto a la autentificación y firmas digitales Trabajar en equipo Resolver problemas	Buscar el bien común al trabajar en equipo. Ser responsable y ético. Apertura al dialogo. Responsabilidad y solidaridad.
	Identificar los principios y técnicas actuales que existen para implementar en hardware y aplicar en software algoritmos criptográficos.	Crear o establecer un nuevo algoritmo criptográfico en una FPGA. Aplicar los métodos criptográficos en software. Cuestionar la información y encontrar respuestas respecto a criptosistemas implementados en hardware.	Buscar el bien común al trabajar en equipo. Ser responsable y ético. Apertura al dialogo. Responsabilidad y solidaridad.

Asignatura	Perfil de egreso (anotar en las siguientes tres columnas, cómo contribuye la asignatura al perfil de egreso)		
	Conocimientos	Habilidades	Actitudes y valores
		Trabajar en equipo Resolver problemas	

9. Describa cómo el eje o los ejes transversales contribuyen al desarrollo de la asignatura

Eje (s) transversales	Contribución con la asignatura
Formación Humana y Social	Desarrollo del análisis y la reflexión de los casos de estudio, así como el pensamiento crítico en la participación en clase.
Desarrollo de Habilidades en el uso de las Tecnologías de la Información y la Comunicación	Análisis de los sistemas criptográficos y ataques a la información que existen en las diversas tecnologías de la actualidad a partir de las prácticas de laboratorio.
Desarrollo de Habilidades del Pensamiento Complejo	Aplicación de los diferentes métodos de cifrado y de autenticación en diversas situaciones de la vida real.
Lengua Extranjera	Bibliografía en el idioma inglés.
Innovación y Talento Universitario	Capacidad para implementar nuevas mejoras de seguridad en los sistemas actuales a partir del modelo matemático.
Educación para la Investigación	Propuesta del proyecto de fin de curso de un caso real.

10. ORIENTACIÓN DIDÁCTICO-PEDAGÓGICA.

Estrategias y Técnicas de aprendizaje-enseñanza	Recursos didácticos
Estrategias de aprendizaje: • Lectura y comprensión, • Reflexión, • Comparación, • Resumen. Estrategias de enseñanza: • ABP, • Aprendizaje activo, • Aprendizaje cooperativo, • Aprendizaje colaborativo, • Basado en el descubrimiento. Ambientes de aprendizaje: • Aula, • Laboratorio, • Simuladores. Actividades y experiencias de aprendizaje: • Visita a empresas. Técnicas • grupales, • de debate, • del diálogo, • de problemas, • de estudio de casos, • cuadros sinópticos, • mapas conceptuales, • para el análisis, • comparación, • síntesis, • mapas mentales, • lluvia de ideas, • analogías, • portafolio, • exposición.	Materiales: • Proyectores • TICs • Plumón y pizarrón • Libros, fotocopias y artículos • Equipo de laboratorio

11. CRITERIOS DE EVALUACIÓN

Criterios	Porcentaje
▪ Exámenes	40%
▪ Participación en clase	10%
▪ Tareas	10%
▪ Trabajos de investigación y/o de intervención	10%
▪ Prácticas de laboratorio	10%
▪ Proyecto final	20%
Total	100%

Nota: Los porcentajes de los rubros mencionados serán establecidos por la academia, de acuerdo a los objetivos de cada asignatura.

12. REQUISITOS DE ACREDITACIÓN

Estar inscrito como alumno en la Unidad Académica en la BUAP
Asistir como mínimo al 80% de las sesiones
La calificación mínima para considerar un curso acreditado será de 6
Cumplir con las actividades académicas y cargas de estudio asignadas que señale el PE

13. Anexar (copia del acta de la Academia y de la CDESC- UA con el Vo. Bo. del Secretario Académico)