PLAN DE ESTUDIOS (PE): Licenciatura en Ciencias de la Computación

ÁREA: Optativa

ASIGNATURA: Criptografía

CÓDIGO: CCOS-604

CRÉDITOS: 6 créditos

FECHA: 9 de mayo de 2017

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:	Nivel Optativa
Correlación:	
Asignaturas Precedentes:	Redes de Computadoras
Asignaturas Consecuentes:	Ninguna

2. CARGA HORARIA DEL ESTUDIANTE

Concepto	Horas por semana		Total de horas por periodo	Total de créditos por periodo
	Teoría	Práctica		
Horas teoría y práctica (16 horas = 1 crédito)	**3**	**2**	**90**	**6**

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:	9 de mayo de 2017
Fecha de aprobación por parte de la academia de área, departamento u otro.	9 de mayo de 2017
Revisores:	Bárbara Emma Sánchez Rinza Ana Claudia Zenteno Vázquez Miguel Ángel León Chávez Luis Enrique Colmenares Guillén Apolonio Ata Pérez Edna Iliana Tamariz Flores Adriana Hernández Beristain Yeiny Romero Hernández
Sinopsis de la revisión y/o actualización:	1. Se modificó el programa a competencias con justificación para semestres. 2. Se actualizó la unidad 2.2 Cifrados por bloques, eliminando el cifrado de producto, IDEA y agregando 3DEA y como 2.5 Algoritmo e-CIPHER. 3. Se actualizó la bibliografía de acuerdo a las necesidades actuales.

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

Disciplina profesional:	Ciencias de la computación, ciencias de la electrónica y áreas afines.
Nivel académico:	Maestría
Experiencia docente:	Mínima de 2 años
Experiencia profesional:	Mínima de 1 año

5. PROPÓSITO: 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.

.

6. COMPETENCIAS PROFESIONALES:

Esta materia se basa en la competencia definida en el Programa de Estudios de la Licenciatura en Ciencias de la Computación, la cual se cita a continuación:

"Diseña e implementa redes de cómputo con la finalidad de hacerlas efectivas y eficientes en la comunicación de datos, mediante el estudio y análisis de nuevos estándares que ayudan a definir un mejor direccionamiento en el diseño de redes, aplicando además, estrategias de seguridad para ajustarse al crecimiento de la red que se tiene hoy en día, debido al incremento de dispositivos conectados a la Internet y a la exigencia de más ancho de banda para las transmisiones."

De acuerdo a lo que se estudia en esta materia se cumple la competencia al resaltar la importancia de la seguridad de las redes hoy en día para que, de esta manera, se puedan diseñar modelos de seguridad para la transmisión de la información.

7. CONTENIDOS TEMÁTICOS

Unidad de Aprendizaje	Contenido Temático	Referencias
1. Fundamentos criptográficos y criptografía clásica	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. Schneier, B. (2015). Applied Cryptography: Protocols, Algorithms and Source Code in C. (1st Edition). USA: Wiley. 2. Stallings, W. (2016). Cryptography and Network Security: Principles and Practice. (7th Edition). USA: Pearson. 3. Katz, J. (2014). Introduction to Modern Cryptography. (2nd Edition). USA: Chapman and Hall/CRC.

		4. Azad, S. (2014). Practical Cryptography: Algorithms and Implementations Using C++. (1st Edition). USA: Auebach Publications.
2. Criptografía de llave privada	2.1 Introducción al cifrado por bloques y por flujo. 2.2 Cifrados por bloques. 2.2.1 Algoritmo DES y 3DEA. 2.2.2 Algoritmo AES y variantes. 2.3 Modos de operación 2.4 Cifrado por flujo	1. Schneier, B. (2015). Applied Cryptography: Protocols, Algorithms and Source Code in C. (1st Edition). USA: Wiley. 2. Stallings, W. (2016). Cryptography and

Unidad de Aprendizaje	Contenido Temático	Referencias
	2.4.1 Secuencias pseudoaleatorias. 2.4.2 Generadores de secuencias. 2.4.3 Registros de desplazamientos retroalimentados. 2.4.4 Otros generadores de secuencia. 2.5 Algoritmos e-CIPHER.	Network Security: Principles and Practice. (7th Edition). USA: Pearson. 3. Katz, J. (2014). Introduction to Modern Cryptography. (2nd Edition). USA: Chapman and Hall/CRC. 4. Azad, S. (2014). Practical Cryptography: Algorithms and Implementations Using C++. (1st Edition). USA: Auebach Publications.

3	Introducción a la teoría de números	3.1 Números Primos. 3.2 Teoremas de Fermat y Euler. 3.3 Pruebas de primalidad. 3.4 Álgebra modular. 3.5 El teorema del residuo chino. 3.6 Logaritmos discretos.	1. Schneier, B. (2015). Applied Cryptography: Protocols, Algorithms and Source Code in C. (1st Edition). USA: Wiley. 2. Stallings, W. (2016). Cryptography and Network Security: Principles and Practice. (7th Edition). USA: Pearson. 3. Katz, J. (2014). Introduction to Modern Cryptography. (2nd Edition). USA: Chapman and Hall/CRC. 4. Azad, S. (2014). Practical Cryptography: Algorithms and Implementations Using C++. (1st Edition). USA: Auebach Publications.
4	Criptografía de llave pública	4.1 Introducción a los algoritmos asimétricos. 4.2 Aplicaciones de los algoritn asimétricos.	1. Schneier, B. (2015). Applied Cryptography: Protocols, Algorithms and

Unidad de Aprendizaje	Contenido Temático	Referencias

	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-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.	2. Source Code in C. (1st Edition). USA: Wiley. 3. Stallings, W. (2016). Cryptography and Network Security: Principles and Practice. (7th Edition). USA: Pearson. Katz, J. (2014). Introduction to Modern Cryptography. (2nd Edition). USA: Chapman and Hall/CRC. 4. Azad, S. (2014). Practical Cryptography: Algorithms and Implementations Using C++. (1st Edition). USA: Auebach Publications.
5 Autenticación y 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. Schneier, B. (2015). Applied Cryptography: Protocols, Algorithms and Source Code in C. (1st Edition). USA: Wiley. 2. Stallings, W. (2016). Cryptography and Network Security: Principles and Practice. (7th Edition). USA: Pearson. 3. Katz, J. (2014). Introduction to Modern Cryptography. (2nd Edition). USA: Chapman and Hall/CRC.

		4. Azad, S. (2014). Practical Cryptography: Algorithms and Implementations Using C++. (1st Edition). USA: Auebach
Unidad de Aprendizaje	**Contenido Temático**	**Referencias**
		Publications.
6 Aplicaciones	6.1 Aplicaciones en Software. 6.1.1 Voto electrónico. 6.1.2 Dinero electrónico.	1. Schneier, B. (2015). Applied Cryptography: Protocols, Algorithms and Source Code in C. (1st Edition). USA: Wiley. 2. Stallings, W. (2016). Cryptography and Network Security: Principles and Practice. (7th Edition). USA: Pearson. 3. Katz, J. (2014). Introduction to Modern Cryptography. (2nd Edition). USA: Chapman and Hall/CRC. 4. Azad, S. (2014). Practical Cryptography: Algorithms and Implementations Using C++. (1st Edition). USA: Auebach Publications.

8. ESTRATEGIAS, TÉCNICAS Y RECURSOS DIDÁCTICOS

Estrategias y técnicas didácticas	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 en inglés • Equipo de laboratorio

9. EJES TRANSVERSALES

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. CRITERIOS DE EVALUACIÓN

Criterios	Porcentaje
▪ Exámenes	**30%**
▪ Trabajos de investigación y/o de intervención	10%
▪ Prácticas de laboratorio	50%
▪ Proyecto final	10%
Total	100%

11. REQUISITOS DE ACREDITACIÓN

Estar inscrito como alumno en la Unidad Académica en la BUAP

Asistir como mínimo al 80% de las sesiones para tener derecho a exentar por evaluación continua y/o presentar el examen final en ordinario o extraordinario
Asistir como mínimo al 70%delas sesiones para tener derecho al examen extraordinario
Cumplir con las actividades académicas y cargas de estudio asignadas que señale el PE
La calificación mínima para considerar un curso acreditado será de 6

Notas:

a) La entrega del programa de asignatura con sus respectivas actas de aprobación, deberá realizarse en formato electrónico, vía oficio emitido por la Dirección o Secretaría Académica a la Dirección General de Educación Superior.

b) La planeación didáctica deberá ser entregada a la coordinación de la licenciatura en los tiempos y formas acordados por la Unidad Académica.