UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

Licenciatura en Ciencias de la Computación

Facultad de Ciencias

Programa de la asignatura

Denominación de la asignatura: *Criptografía y Seguridad*					
Clave:	**Semestre:** 8	**Eje temático:** Integración Teoría-Práctica			**No. Créditos:** 10
Carácter: Obligatoria		**Horas**		**Horas por semana**	**Total de Horas**
Tipo: Teórico-Práctica		**Teoría:** 3	**Práctica:** 4	**7**	**112**
Modalidad: Curso		**Duración del programa: Semestral**			

Asignatura con seriación obligatoria antecedente: Computación Distribuida; Análisis de Algoritmos; Organización y Arquitectura de Computadoras

Asignatura con seriación obligatoria subsecuente: Ninguna

Asignatura con seriación indicativa antecedente: Redes de Computadoras; Complejidad Computacional.

Asignatura con seriación indicativa subsecuente: Ninguna

Objetivos generales:

Comprender los algoritmos de cifrado de datos más usuales, tanto simétricos como de llave pública.
Comprender los principales protocolos de autenticación y de intercambio seguro de datos.
Conocer y aplicar las principales fortalezas y debilidades de los distintos algoritmos y protocolos criptográficos.
Conocer los ataques y mecanismos de criptoanálisis más usuales.
Instrumentar medidas básicas de seguridad en sistemas de cómputo.

Índice temático

Unidad	**Temas**	**Horas**	
		Teóricas	**Prácticas**
I	Conceptos de seguridad y criptografía	3	4
II	Sistemas de cifrado clásicos, seguridad perfecta	4	6
III	Redes de Feistel, cifrado de bloques, DES y AES	6	8
IV	Elementos de teoría de números y campos finitos	6	8
V	Criptosistemas de llave pública	6	8

VI	Algoritmos criptográficos de integridad de datos	5	6
VII	Autentificación y firma digital	6	8
VIII	Protocolos de seguridad en Internet	6	8
IX	Seguridad en redes, cortafuegos y políticas	6	8
	Total de horas:	**48**	**64**
	Suma total de horas:	**112**	

Contenido temático	
Unidad	**Tema**
I Conceptos de seguridad y criptografía	
I.1	Esquema general de la comunicación criptográfica.
I.2	Servicios y mecanismos de seguridad, ataques.
I.3	Principios de Kerckhoffs.
I.4	Estándares de seguridad.
II Sistemas de cifrado clásicos, seguridad perfecta	
II.1	Sistemas monoalfabéticos y polialfabéticos.
II.2	Análisis de frecuencias, prueba de Kasiski y de Friedman.
II. 3	Sistemas poligráficos, sistema de Playfair y de Hill.
II.4	Cifrado de Vernam, *one-time pad* y seguridad perfecta.
II.5	Registros de desplazamiento de retroalimentación líneal.
II.6	Cifrados de rotor: Enigma y Púrpura.
III Redes de Feistel, cifrado de bloques, DES y AES	
III.1	Cifrado y teoría de la información: confusión y difusión.
II.2	Redes de Feistel. Lucifer y DES.
III.3	Criptoanálisis diferencial.
III.4	Criptoanálisis lineal.
III.5	Redes de permutación y substitución: AES.
IV Elementos de teoría de números y campos finitos	
IV.1	Repaso de aritmética modular, divisibilidad, algoritmo de Euclides, MCD Y MCM.
IV.2	Teoremas de Fermat y de Euler, teorema chino del residuo.
IV.3	Un poco de estructuras algebraicas: grupos, anillos y campos.
IV.4	Campos finitos, polinomios.
V Criptosistemas de llave pública	
V.1	Motivación, principios de sistemas de llave pública.
V.2	Funciones de un sólo sentido: factorización y logaritmo discreto.
V.3	Algoritmo de Diffie Hellman.
V.4	Algoritmo de RSA.
V.5	Algoritmo de El-Gamal.
V.6	Elementos de criptoanálisis de sistemas de llave pública.
VI Algoritmos criptográficos de integridad de datos	
VI.1	Códigos de autentificación de mensajes.
VI.2	Generadores de números pseudoaleatorios.
VI.3	Funciones de dispersión, características, usos para sintetizar mensajes.

VI.4	Funciones de dispersión basadas en cifrados de bloque.
VI.5	Análisis de diversos algoritmos de dispersión.
VII Autentificación y firma digital	
VII.1	Principios fundamentales de autentificación, factores de autentificación.
VII.2	Distribución de llaves, certificados.
VII.3	Protocolos de autentificación.
VII.4	Autentificación basada en sistemas simétricos y de llave pública.
VIII Protocolos de seguridad en Internet	
VIII.1	Análisis comparativo de sistemas simétricos y de llave pública.
VIII.2	Sistemas criptográficos mixtos.
VIII.3	Seguridad en la web.
VIII.4	Protocolos de seguridad: IPSec, secure shell, TLS, PGP.
VIII.5	Ataques, herramientas de análisis.
IX Seguridad en redes, cortafuegos y políticas	
IX.1	Intrusión, detección de intrusos.
IX.2	Tipos de ataque, tipos de software malicioso.
IX.3	Planeación de la seguridad, políticas de seguridad.
IX.4	Aspectos de seguridad en el diseño de sistemas operativos y de manejadores de bases de datos.
IX.5	Mecanismos de defensa contra intrusión, configuración del sistema, cortafuegos.
IX.6	Herramientas de análisis de intrusión, análisis forense.

Bibliografía básica:

1. Stallings, William, *Cryptography and Network Security: Principles and Practice*, 5a Ed., Prentice Hall, 2010.
2. Forouzan, Behrouz A., *Cryptography and Network Security*, McGraw Hill, 2008. Pfleeger, Charles P. y Shari L.
3. Pfleeger, *Security in Computing*, 4a. Ed., Prentice Hall, 2006.

Bibliografía complementaria:

1. Stallings, William, *Network Security Essentials: Applications and Standards*, 4a Ed., Prentice Hall, 2010.
2. Ferguson, Niels, Bruce Schneier y Tadayoshi Kohno, *Cryptography Engineering: Design Principles and Practical Applications*, Wiley, 2010.
3. Menezes, Alfred, Paul van Oorschot y Scott Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1996.
4. Schneier, Bruce, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*. 2a Ed., Wiley, 1996.

Sugerencias didácticas:		Métodos de evaluación:	
Exposición oral	**(X)**	**Exámenes parciales**	**(X)**
Exposición audiovisual	**(X)**	**Examen final escrito**	**(X)**
Ejercicios dentro de clase	**(X)**	**Trabajos y tareas fuera del aula**	**(X)**
Ejercicios fuera del aula	**(X)**	**Prácticas de laboratorio**	**( )**
Seminarios	**( )**	**Exposición de seminarios por los alumnos**	**( )**
Lecturas obligatorias	**( )**	**Participación en clase**	**( )**
Trabajo de investigación	**( )**	**Asistencia**	**( )**
Prácticas de taller o laboratorio	**(X)**	**Proyectos de programación**	**( )**
Prácticas de campo	**( )**	**Proyecto final**	**( )**
		Seminario	**( )**
Otras: _____		**Otras:** _____	

Perfil profesiográfico:

Egresado preferentemente de la Licenciatura en Ciencias de la Computación o Matemático con especialidad en Computación. Es conveniente que posea un posgrado en la disciplina. Con experiencia docente.