BENEMÉRITA UNIVERSIDAD AUTÓNOMA DE PUEBLA

FACULTAD CIENCIAS DE LA COMPUTACION

PROGRAMA DE LA MATERIA CORRESPONDIENTE A LA INGENIERÍA EN CIENCIAS DE LA COMPUTACIÓN

Coordinación: Área de REDES

NOMBRE DE LA MATERIA:	**Servicios Avanzados en Internet**

Clave: LIC 590
Créditos: 10
Modalidad: Escolarizada

Nivel de Ubicación: Formativa
Tipo de Materia: Optativa

PRE-REQUISITOS:	NIVEL BASICO
MATERIA CONSECUENTE:	LIC 591 Programación de Servicios en Internet
TIEMPO TOTAL ASIGNADO:	96 hrs.

PRIMAVERA – OTOÑO

HRS. TEÓRICAS/SEM: 4	HRS. PRÁCTICAS/SEM: 2

VERANO

HRS. TEÓRICAS/SEM: 8	HRS. PRÁCTICAS/SEM: 4

AUTOR(ES) DEL PROGRAMA:	
Miguel Ángel León Chávez	
Ivo Humberto Pineda Torres	
Apolonio Ata Pérez	

REVISADO POR:	Jorge Jiménez Gonzáles
APROBADO POR:	Academia de Redes
AUTORIZADO POR:	

FECHA DE ELABORACIÓN/REVISIÓN:	24 Noviembre 2006
VIGENCIA:	5 años

JUSTIFICACIÓN:

La sociedad se encuentra en una etapa de desarrollo conocida como "sociedad del conocimiento" la cual se basa tecnológicamente en el uso de redes de computadoras para compartir y difundir el conocimiento, el cual adquiere un valor que en muchos casos debe de protegerse. Por lo cual es vital que los estudiantes de ingeniería en ciencias de la computación conozcan y apliquen los algoritmos y protocolos criptográficos para proteger la información al transmitirse por las redes de computadoras.

OBJETIVO GENERAL DE LA MATERIA:

Que el estudiante adquiera los fundamentos teóricos, conozca las características y las propiedades de los diferentes criptosistemas, así como los algoritmos de cifrado y los protocolos, con el fin de diseñar, administrar e implantar soluciones específicas a cada red de computadoras, en particular al Internet.

CONTRIBUCIÓN DE LA SIGNATURA AL PERFIL DE EGRESO:

En el perfil del egresado se plantea que éste tendrá una visión general de la Ingeniería en Ciencias de la Computación y poseerá conocimientos sólidos para la construcción de soluciones basadas en Sistemas de Software. Un área importante en la computación es la de Redes de Computadoras ya que en la actualidad la mayoría de los Sistemas de Software son distribuidos, es decir interconectados por una Red, por ejemplo la red de redes o Internet. Sin embargo la seguridad de la información es la principal vulnerabilidad del Internet por lo que la asignatura de Sistemas Avanzados de Internet tiene una contribución indispensable en la formación del estudiante.

CONTENIDO TEMÁTICO

MATERIA:

UNIDAD: 1		TÍTULO: Critosistemas de llave privada y públicas				
OBJETIVO ESPECÍFICO: Que el estudiante identifique los principales algoritmos de cifrado de llave privada y pública, así como las funciones Hash						
	CONTENIDO DE LA UNIDAD	Tiempo de impartición (hrs.)		Actividades de Aprendizaje	Técnicas	Recursos Necesarios
		HT	HP			
1.1	Introducción a los criptosistemas	4		Introducción y Motivación; Comprensión y Elicitación de Ideas	Exposición del Profesor; Discusión grupal y lluvia de ideas	Salón, pizarrón, plumones, proyector de acetatos o de video.
1.2	Estándar de cifrado de Datos (DES)	4	2	Comprensión y Elicitación de Ideas. Explicar DES y sus modos de operación	Exposición del Profesor; Discusión grupal y lluvia de ideas	Salón, pizarrón, plumones, proyector de acetatos o de video.
1.3	Estándar Avanzado de Cifrado (AES)	4	2	Comprensión y Elicitación de Ideas. Describir AES.	Exposición del Profesor	Idem.
1.4	Algoritmo RSA	4	2	Comprensión y Elicitación de Ideas. Explicar RSA.	Exposición del Profesor	Idem.
1.5	Función Hash MD5 y SHA1	4	2	Comprensión y Elicitación de Ideas. Describir MD5 y SHA1	Exposición del Profesor	Idem.
	HORAS TOTALES:	20	8			

UNIDAD: 2				TÍTULO: Administración de llaves públicas		
OBJETIVO ESPECÍFICO: Que el estudiante identifique los protocolos de intercambio de llave pública						
	CONTENIDO DE LA UNIDAD	Tiempo de impartición (hrs.)		Actividades de Aprendizaje	Técnicas	Recursos Necesarios
		HT	HP			
2.1	Administración de llaves	2		Introducción y Motivación; Comprensión y Elicitación de Ideas	Exposición del Profesor; Discusión grupal y lluvia de ideas	Salón, pizarrón, plumones, proyector de acetatos o de video.
2.2	Protocolo de intercambio de llaves públicas de Diffie-Hellman	4	2	Comprensión y Elicitación de Ideas. Describir y modelar el protocolo Diffie-Hellman	Exposición del Profesor.	Idem.
2.3	Criptosistema de llave pública ElGamal	4	2	Comprensión y Elicitación de Ideas. Describir y modelar el protocolo ElGamal	Exposición del Profesor .	Idem.
	HORAS TOTALES:	10	4			

UNIDAD: 3				TÍTULO: Arquitecturas de Seguridad IP		
OBJETIVO ESPECÍFICO: Que el estudiante identifique los servicios de seguridad definidos por los Modelo de Referencia OSI y TCP/IP						
	CONTENIDO DE LA UNIDAD	Tiempo de impartición (hrs.) HT	HP	Actividades de Aprendizaje	Técnicas	Recursos Necesarios
3.1	Arquitectura de seguridad del Modelo de Referencia OSI	2		Introducción y Motivación; Comprensión y Elicitación de Ideas	Exposición del Profesor; Discusión grupal y lluvia de ideas	Salón, pizarrón, plumones, proyector de acetatos o de video.
3.2	Arquitectura de seguridad del Modelo TCP/IP	2		Introducción y Motivación; Comprensión y Elicitación de Ideas	Exposición del Profesor; Discusión grupal y lluvia de ideas	Salón, pizarrón, plumones, proyector de acetatos o de video.
3.3	Seguridad IP (IPSec): Encabezados de extensión AH, ESP e ISAKMP	6		Comprensión y Elicitación de Ideas	Exposición del Profesor	Idem.
	HORAS TOTALES:	10				

UNIDAD: 4				TÍTULO: Aplicaciones de Autenticación		
OBJETIVO ESPECÍFICO: Que el estudiante identifique los servicios de autenticación que existen a nivel de aplicación						
	CONTENIDO DE LA UNIDAD	Tiempo de impartición (hrs.)		Actividades de Aprendizaje	Técnicas	Recursos Necesarios
		HT	HP			
4.1	Kerberos	4	2	Introducción y Motivación; Comprensión y Elicitación de Ideas	Exposición del Profesor; Discusión grupal y lluvia de ideas	Salón, pizarrón, plumones, proyector de acetatos o de video.
4.2	Servicio de Autenticación X.509	4		Comprensión y Elicitación de Ideas	Exposición del Profesor	Idem.
	HORAS TOTALES:	8	2			

UNIDAD: 5				TÍTULO: Seguridad del Correo Electrónico		
OBJETIVO ESPECÍFICO: Que el estudiante identifique y aplique los servicios de seguridad al correo electrónico						
	CONTENIDO DE LA UNIDAD	Tiempo de impartición (hrs.)		Actividades de Aprendizaje	Técnicas	Recursos Necesarios
		HT	HP			
5.1	S/MIME	4		Introducción y Motivación; Comprensión y Elicitación de Ideas	Exposición del Profesor; Discusión grupal y lluvia de ideas	Salón, pizarrón, plumones, proyector de acetatos o de video.
5.2	PGP (Pretty Good Privacy)		2	Aplicación del Conocimiento.	Exposición del Profesor; Solución de preguntas y/o problemas.	Software PGP
	HORAS TOTALES:	4	2			

UNIDAD: 6		TÍTULO: Seguridad en la Web				
OBJETIVO ESPECÍFICO: Que el estudiante identifique los principales protocolos de seguridad en la Web						
	CONTENIDO DE LA UNIDAD	Tiempo de impartición (hrs.)		Actividades de Aprendizaje	Técnicas	Recursos Necesarios
		HT	HP			
6.1	Requerimientos de seguridad en la Web	2		Introducción y Motivación; Comprensión y Elicitación de Ideas	Exposición del Profesor; Discusión grupal y lluvia de ideas	Salón, pizarrón, plumones, proyector de acetatos o de video.
6.2	Capa de Socket Seguro (Secure Socket Layer, SSL) y Seguridad en la Capa de Transporte (Transport Layer Security, TLS)	4	2	Comprensión y Elicitación de Ideas. Explicar y modelar SSL/TLS	Exposición del Profesor. Solución de preguntas y/o problemas.	Idem.
6.3	Transacciones Electrónicas Seguras (Secure Electronic Transaction, SET)	4		Comprensión y Elicitación de Ideas. Explicar y modelar SET	Exposición del Profesor. Solución de preguntas y/o problemas.	Idem.
	HORAS TOTALES:	10	2			

	HT	HP
HORAS TOTALES DE LA MATERIA:	62	18

PRACTICAS			
UNIDAD	NOMBRE DE LA PRACTICA	OBJETIVO	HORAS
1	Diseño e implementación de DES	Que el estudiante aplique los conocimientos adquiridos en clase	2
1	Diseño e implementación de AES	Idem.	2
1	Diseño e implementación de RSA	Idem.	2
1	Diseño e implementación de MD5 y SHA1	Idem.	2
2	Diseño e implementación del protocolo de Diffie-Hellman	Idem.	2
2	Diseño e implementación del protocolo ElGamal	Idem.	2
4	Identificación de los servicios ofrecidos por Kerberos	Idem.	2
5	Instalación y uso de PGP	Idem.	2
6	Identificación de los servicios ofrecidos por SSL/TLS	Idem.	2

CRITERIOS DE EVALUACIÓN

EXÁMENES PARCIALES		
Parcial	Contenido a evaluar	Periodos
1	Unidad 1	5ª Semana del Curso

2	Unidad 2 y 3	9ª Semana del Curso
3	Unidad 4, 5 y 6	16ª Semana del Curso

	%
Asistencias y participación:	0
Exámenes parciales:	40
Tareas:	0
Trabajos de Investigación y exposición en clase:	20
Prácticas de Laboratorio o Proyecto de curso:	40
TOTAL:	100

REQUISITOS DE ACREDITACIÓN:

Tener una calificación promedio de los exámenes parciales, exposición en clase y proyecto igual o mayor a seis.

FOMENTO DE VALORES:

Se inculcará en el estudiante el hábito de analizar los requerimientos de seguridad del sistema de software y a seleccionar el mejor criptosistema para proveer los servicios de seguridad.

BIBLIOGRAFÍA:

1.- Tanenbaum, A. S. "Redes de Computadoras ". Prentice Hall, 3ª edición

2.- Stallings, W., "Data & Computer Communication ", Prentice Hall, 6a edición

3.- Stallings, W., “Cryptography and Network Security, Principles and Practice”. Prentice Hall, 3ª edition, 2003.

4.- Trappe, W. and L. C. Washington. “Introduction to Cryptography with Coding Theory”. Prentice Hall, 2002.

5.- Artículos varios.