Centro de Investigación y de Estudios Avanzados
Del Instituto Politécnico Nacional
Secretaría Académica

Registro de Cursos o Asignaturas

Nombre Completo del Programa de Posgrado		**Maestría en Ciencias en Ingeniería Eléctrica**		
Nombre Completo del Curso		**Computación II: Criptografía y Seguridad Informática**		
Tipo de Curso		**Electivo**	**Créditos**	**8**
Número de horas	**Teóricas:**	**60**	**Prácticas:**	**20**
		Presenciales		No presenciales

Profesores que impartirán el curso

Arturo Díaz Pérez

Objetivos del curso:	**General**	El curso tiene como propósito presentar las herramientas criptográficas esenciales para proporcionar servicios de seguridad informática que se requieren en las aplicaciones modernas. Se revisarán las técnicas de ciframeinto y aseguramiento de información estándar en los servicios de seguridad.
	Específicos	En el curso se describirá el proceso de aseguramiento de información en el contexto de los sistemas de información presentes y futuros, se describirán los servicios de seguridad esenciales, confidencialidad, autenticación, integridad, no repudio, que requieren las aplicaciones modernas. Se revisarán también las herramientas útiles para seguridad en datos y en redes.

Contenidos temáticos

1. Aritmética Modular
- 1.1. Introducción a la teoría de números
- 1.2. Campos finitos
- 1.3. Números primos y teorema de Euler
- 1.4. Factorización de enteros.
- 1.5. Teorema chino del residuo.
- 1.6. Algoritmos para aritmética modular

2. Introducción a la criptografía
- 2.1. Arquitectura de seguridad OSI
- 2.2. Técnicas de ciframeinto clásicas
- 2.3. Cifradores de bloque y modos de operación
- 2.4. Cifradores de flujo
- 2.5. Encriptación de llave simétrica
- 2.6. DES y AES

3. Criptografía de llave pública
- 3.1. Introducción a la criptografía de llave pública
- 3.2. Protocolo Diffie-Hellman para intercambio de llaves
- 3.3. El criptosistema de llave pública RSA.
- 3.4. Confidencialidad usando criptografía de llave pública
- 3.5. Criptografía de curvas elípticas

4.	**Autenticación y funciones hash**
4.1.	Requerimientos de autenticación
4.2.	Funciones de autenticación
4.3.	Códigos de autenticación de mensajes (MAC)
4.4.	Funciones Hash y SHA-256
4.5.	Firmas digitales
5.	**Seguridad en redes**
5.1.	Seguridad IPSec
5.2.	Aplicaciones de autenticación: Kerberos
5.3.	X.509 Servicios de autenticación y PKI
5.4.	SSL/TLS
5.5.	Seguridad en los servicios de correo electrónico, PGP
5.6.	Seguridad Web
5.7.	Firewalls, IDS/IPS
5.8.	Control de Accesos, DAC y RBAC
6.	**Software malicioso y seguridad en software**
6.1.	Vulnerabilidades
6.2.	Malware
6.3.	Programación segura
6.4.	OWASP y ataques a aplicaciones más comunes
6.5.	Ataques de inyección SQL
6.6.	Ataques CROSS SITE SCRIPTING (XSS)
6.7.	Cibercrimen y ciberterrorismo

Bibliografía

1. Menezes, A. J, van Oorschot P. C., Vanstone, S. A. “Handbook of Applied Cryptography”, CRC Press, 5th Edition. 2001.
2. Schneier, B. “Applied Cryptography: Protocols, Algorithms, and Source Code in C (inglés). Wiley, 2015.
3. William Stallings, “Cryptography And Network Security – Principles and Practices”, Prentice Hall, Fourth Edition, 2005.
4. Stallings & Brown, “Computer Security: Principles and Practice, 3rd Edition”. Pearson, 2018.

Criterios de evaluación

Tareas	0%
Exámenes (2 parciales y un final)	0%
Proyecto Final	0%
Total	0%

Contribución del curso al perfil de egreso del programa

Conocimientos:

Habilidades:

Actitudes y valores: