UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO
PROGRAMA DE MAESTRÍA Y DOCTORADO EN INGENIERÍA
Programa de actividad académica

Denominación: Temas Selectos de Telecomunicaciones: CRIPTOGRAFÍA				
Clave:	**Semestre (s): 1, 2 ó 3**	**Campo de conocimiento:** Ingeniería Eléctrica		**No. Créditos: 6**
Carácter: Optativa de elección		**Horas**	**Horas por semana**	**Horas al semestre**
Tipo: Teórica		**Teoría:** 3	**Práctica:** 0	3	48
Modalidad: Curso		**Duración del programa:** Semestral		

Seriación: Sin seriación (X) Obligatoria ( ) Indicativa ( )

Actividad académica antecedente: Álgebra Lineal

Actividad académica subsecuente: Ninguna

Objetivo general:
Se presentarán las definiciones, conceptos, terminología y principios básicos de la criptografía moderna comercial. El estudiante entenderá la diferencia entre los sistemas de cifrado (criptosistemas) simétricos o de llave secreta y los asimétricos o de llave pública, entenderá también la problemática fundamental que conlleva su uso y la solución que se le da a dicha problemática. Desde un punto de vista algorítmico, y para ambos tipos de sistemas, se estudiarán los principales sistemas de cifrado modernos comerciales así como los principales estándares de firma digital.

Índice Temático

Unidad	Tema	Horas	
		Teóricas	Prácticas
1	Introducción a la Criptografía	3	0
2	Criptografía Simétrica	21	0
3	Criptografía Asimétrica	24	0
	Total de horas:	48	0
	Suma total de horas:	48	

Contenido Temático

Unidad	Temas y subtemas
1	Introducción a la Criptografía
1.1	Definiciones y conceptos básicos
2	Criptografía Simétrica
2.1	DES, Triple DES y Modos de Cifrado (ECB, CBC, CFB y OFB)
2.2	IDEA, RC5 y RC2
2.3	Una introducción a los campos finitos y el AES
3	Criptografía Asimétrica
3.1	Construcción de un criptosistema de llave pública a través de un grupo
3.2	Problema del Logaritmo Discreto
3.3	Criptosistemas de llave pública basados en curvas elípticas
3.4	Firma digital usando ECDSA
3.5	Criptosistema ElGamal
3.6	Criptosistema RSA
3.6.1	Algo de Teoría de Números
3.6.2	Teorema de Fermat
3.6.3	Teorema Chino del Residuo en el contexto de RSA
3.7	Firmas Digitales
3.8	El PKCS #1
3.9	Firma digital usando RSA
3.10	El estándar mexicano para la conservación de mensajes de datos digitales NOM-151

Bibliografía Básica:

- Handbook of Applied Cryptography, Alfred J. Menezes et al. CRC Press, 1997. (disponible gratuitamente en http://www.cacr.math.uwaterloo.ca/hac/)
- Bruce Schneier, Applied Cryptography, 2nd edition, John Wiley & Sons, 1996.
- Neal Koblitz, A Course in Number Theory and Cryptography (Springer, New York,. 1987).
- Cryptography and Data Security, Dorothy Elizabeth Robling Denning. Addison-Wesley Pub, 1982.

- Differential Cryptanalysis of the Data Encryption Standard, Eli Biham, Adi Shamir. Springer-Verlag, 1993.

Bibliografía complementaria:

- Finite Fiels, Lidl R. Niederreiter H. Cambridge Univ. Press, 1983.
- The Theory of Error-Correcting Codes, F.J. MacWilliams, N.J.A. Sloane. North-Holland, Amsterdam, The Netherlands, 1977.

Sugerencias didácticas:		**Mecanismos de evaluación del aprendizaje de los alumnos:**	
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)	Exposición de seminarios por los alumnos	( )
Seminarios	( )	Participación en clase	(X)
Lecturas obligatorias	(X)	Asistencia	(X)
Trabajo de investigación	(X)	Seminario	( )
Prácticas de taller o laboratorio	(X)	Otras:	( )
Prácticas de campo	( )		
Otras:	( )		

Línea de investigación:
Telecomunicaciones

Perfil profesiográfico:
Tener grado de Doctor o Maestro con experiencia como docente en el campo de conocimiento de la actividad académica.