UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

Licenciatura en Ciencias de la Computación

Facultad de Ciencias

Programa de la asignatura

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

Asignatura con seriación indicativa antecedente: Análisis de Algoritmos; Teoría de los Números I; Álgebra Moderna I

Asignatura con seriación indicativa subsecuente: Ninguna

Objetivo general:

Proporcionar conocimientos generales de la Criptografía a través del estudio de diferentes métodos criptográficos históricos y modernos. Consolidar la importancia del estudio de objetos matemáticos y su aplicación a la Teoría de la Información. Dar al alumno herramientas básicas de análisis criptoanalítico. Presentar a la Criptografía como rama de investigación activa.

Índice temático

Unidad	**Temas**	**Horas**	
		Teóricas	**Prácticas**
I	Introducción	1	1
II	Criptografía clásica	15	20
III	Métodos históricos de llave larga	5	7
IV	Criptografía moderna y de llave pública	15	20
V	Esquemas de Firmas	3	4
VI	Sistemas basados en Curvas Elípticas	6	8
VII	Optativo	3	4
	Total de horas:	**48**	**64**
	Suma total de horas:	**112**	

Contenido temático	
Unidad	**Tema**
I Introducción	
I.1	Motivación y principales problemas de la Criptografía.
I.2	Esquemas básicos de comunicación.
II Criptografía clásica	
II.1	Criptografía de sustitución monoalfabética. • Cifrado de César. • Sustituciones afines. • Alfabetos mezclados.
II.2	Criptoanálisis de sustitución monoalfabética.
II.3	Criptografía de sustitución polialfabética. • Vigenère. • Alberti.
II.4	Criptoanálisis de sustitución polialfabética. • Prueba de Kasiski. • Prueba de Friedman. • Índice de coincidencias.
II.5	Criptografía de sustitución poligráfica. • Álgebra lineal y método de Hill. • Métodos modulares.
II.6	Criptoanálisis de sustitución poligráfica. • Ataques al método de Hill. • Análisis de frecuencias. • Ataque de palabra probable.
III Métodos históricos de llave larga	
III.1	Enigma.
III.2	Púrpura.
III.3	Cifrado de Vernam.
III.4	Seguridad Perfecta. • Cuadrados Latinos.
III.5	Registros de desplazamiento con retroalimentación lineal.
IV Criptografía moderna y de llave pública	
IV.1	DES.
IV.2	Criptoanálisis de DES.
IV.3	Funciones de un sólo sentido.
IV.4	Idea de la Criptografía de llave pública.
IV.5	Intercambio de llaves de Diffie-Hellman.
IV.6	Criptosistema de envío de mensajes Massey Omura.
IV.7	Criptosistemas de Llave pública. • RSA.

	• ElGamal. • Rabino.
IV.8	Criptoanálisis de llave pública. • Ruptura contra ruptura total. • Problemas asociados con el criptoanálisis de llave pública. • Complejidad de operaciones sencillas en Teoría de Números. • Problema del Logaritmo Discreto y algoritmos para solucionarlo. o Búsqueda exhaustiva. o Paso grande, paso chico. o Algoritmo de Pohling Hellman. o Cálculo de índices. • El problema de factorización y algoritmos para solucionarlo. o División. o Algoritmo de factorización Ro de Pollard. o Algoritmo de factorización Ro-1 de Pollard. o Criba Cuadrática. • Ataques al RSA sin factorización del módulo. • Ataque por módulo en común. • Ataques por exponente público y/o privado pequeño. • Ataques de implementación.
V Esquemas de Firmas	
V.1	Proceso de firmas y verificación.
V.2	Algoritmos de firmas. • ElGamal. • RSA.
VI Sistemas basados en Curvas Elípticas	
VI.1	Definición y estructura de grupo de las Curvas Elípticas.
VI.2	Algoritmos para hacer más eficiente la suma de puntos.
VI.3	Criptosistemas basados en Curvas Elípticas.
VI.4	Algoritmos de factorización y primalidad usando Curvas Elípticas.
VII Optativo	
VII.1	Criptografía cuántica.
VII.2	Criptografía Visual.

Bibliografía básica:

1. Bauer, F. L., *Decrypted Secrets, Methods and Maxims of Cryptology*, 2a. ed., Springer Verlag, 2000.
2. Galaviz José, *Introducción a la Criptografía*, Departamento de Matemáticas, Facultad de Ciencias, UNAM, Vínculos Matemáticos #15, 2003.
3. Koblitz, Neal, *A Course in Number Theory and Cryptography*, 2a ed., Springer Verlag, 1994, Graduate Texts in Mathematics.

4. Menezes A. J., P. C. van Oorschot y S. A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1996.
5. Schneier, Bruce, *Applied Cryptography*, 2a. ed., John Wiley and Sons. 1996.
6. Douglas R. Stinson, *Cryptography: Theory and Practice*, CRC Press, Inc., Boca Raton, FL, USA, 1995. ISBN 0849385210.

Bibliografía complementaria:

1. John B. Fraleigh, *A first course in abstract algebra* , (Addison-Wesley series in mathematics), Addison-Wesley Pub. Co, July 1976. ISBN 0201019841.
2. Joseph H. Silverman and John Tate, *Rational Points on Elliptic Curves*, Undergraduate Texts in Mathematics. Springer, 1992.
3. Whitfield Diffie and Martin E. Hellman, *New directions in cryptography*, IEEE Transactions on Information Theory, IT-22(6):644-654, 1976. URL citeseer.ist.psu.edu/diffie76new.html.
4. Neal Koblitz, *A course in number theory and cryptography*, Springer-Verlag New York, Inc., New York, NY, USA, 1987. ISBN 0-387-96576-9.
5. Lawrence C.Washington, *Elliptic Curves: Number Theory and Cryptography*, CRC Press, Inc., Boca Raton, FL, USA, 2003. ISBN 1584883650.
6. Henri Cohen and Gerhard Frey, editores, *Handbook of elliptic and hyperelliptic curve cryptography*, CRC Press, 2005. ISBN 11584885181

Sugerencias didácticas:		**Métodos de evaluación:**	
Exposición oral	**(X)**	**Exámenes parciales**	**(X)**
Exposición audiovisual	**(X)**	**Examen final escrito**	**( )**
Ejercicios dentro de clase	**(X)**	**Trabajos y tareas fuera del aula**	**(X)**
Ejercicios fuera del aula	**( )**	**Prácticas de laboratorio**	**( )**
Seminarios	**(X)**	**Exposición de seminarios por los alumnos**	**( )**
Lecturas obligatorias	**(X)**	**Participación en clase**	**(X)**
Trabajo de investigación	**( )**	**Asistencia**	**( )**
Prácticas de taller o laboratorio	**(X)**	**Proyectos de programación**	**(X)**
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 con amplia experiencia de programación. Es conveniente que posea un posgrado en la disciplina. Con experiencia docente.