UNIVERSIDAD AUTONOMA METROPOLITANA

Casa abierta al tiempo

PROGRAMA DE ESTUDIOS

UNIDAD **AZCAPOTZALCO**	DIVISION **CIENCIAS BASICAS E INGENIERIA**	1 / 2
NOMBRE DEL PLAN **LICENCIATURA EN INGENIERIA EN COMPUTACION**		
CLAVE	UNIDAD DE ENSEÑANZA-APRENDIZAJE	CRED. 9
1112036	**CRIPTOGRAFIA**	TIPO **OPT.**
H.TEOR. **4.5**		
H.PRAC. **0.0**	SERIACION **1151040**	

OBJETIVO(S):

General:

Al final de la UEA el alumno será capaz de:

Analizar, diseñar y evaluar formalmente algoritmos y protocolos criptográficos utilizando paquetes computacionales.

CONTENIDO SINTETICO:

1. Seguridad, privacidad, autentificación y adversarios.
2. Criptografía clásica. One-time pad y seguridad perfecta.
3. Criptografía simétrica.
4. Criptografía asimétrica y firmas digitales.
5. Criptografía en la práctica.
6. Software de criptografía y teoría de numeros computacional.

MODALIDADES DE CONDUCCION DEL PROCESO DE ENSEÑANZA-APRENDIZAJE:

Clase teórica y práctica con apoyos de medios audiovisuales y computacionales.. Alternativamente modalidad de SAI.

Como parte de las modalidades de conducción del proceso de enseñanza-aprendizaje será requisito que los alumnos con apoyo del profesor, participen en la revisión y análisis de al menos un texto técnico, científico o de difusión escrito en idioma inglés y que contribuya a alcanzar los objetivos del programa de estudios.

Se procurará que como parte de las modalidades de conducción del proceso de

UNIVERSIDAD AUTONOMA METROPOLITANA

Casa abierta al tiempo

APROBADO POR EL COLEGIO ACADEMICO
EN SU SESION NUM. 355

EL SECRETARIO DEL COLEGIO

enseñanza-aprendizaje los alumnos participen en la presentación oral de sus trabajos, tareas u otras actividades académicas desarrolladas durante el curso.

MODALIDADES DE EVALUACION:

Evaluación Global:

Al menos dos evaluaciones periódicas consistentes en preguntas conceptuales, resolución de problemas, tareas y elaboración de programas.

Evaluación de Recuperación:

Admite evaluación de recuperación.

No requiere inscripción previa.

BIBLIOGRAFIA NECESARIA O RECOMENDABLE:

1. Menezes A. J., Van Oorschot P. C., Vanstone S. A., "Handbook of applied cryptography", CRC Press, 2001.
2. Giblin P., "Primes and Programming", Cambridge University Press, 1993.

Revistas de divulgación, técnicas o científicas en inglés, relacionadas con el contenido de la UEA.

Casa abierta al tiempo

UNIVERSIDAD AUTONOMA METROPOLITANA

APROBADO POR EL COLEGIO ACADEMICO
EN SU SESION NUM. 335

EL SECRETARIO DEL COLEGIO