

UNIDAD	AZCAPOTZALCO	DIVISIÓN	CIENCIAS BÁSICAS E INGENIERÍA	1 / 2
NOMBRE DEL PLAN LIC. INGENIERÍA EN COMPUTACIÓN				
CLAVE	1112036	UNIDAD DE ENSEÑANZA-APRENDIZAJE	CRIPTOGRAFÍA	CRED. 9 TIPO OPT.
H.TEOR.	4.5	SERIACIÓN	1151040	TRIM.
H.PRAC.	0.0			

**OBJETIVO (S):**

Al finalizar el curso el alumno será capaz de:  
 Analizar, diseñar y evaluar formalmente algoritmos y protocolos criptográficos utilizando paquetes computacionales.

**CONTENIDO SINTÉTICO:**

1. Seguridad, privacidad, autenticación 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 números computacional.

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

CLAVE 1112036

CRIPTOGRAFÍA

**MODALIDADES DE EVALUACIÓN:**

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

Admite evaluación de recuperación.

No requiere inscripción previa.

**BIBLIOGRAFÍA 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.