Casa abierta al tiempo
UNIVERSIDAD AUTÓNOMA METROPOLITANA

PROGRAMA DE ESTUDIOS

1/D

UNIDAD:	DIVISIÓN	
IZTAPALAPA	**CIENCIAS BÁSICAS E INGENIERÍA**	
NIVEL: **MAESTRÍA**	EN **POSGRADO EN CIENCIAS Y TECNOLOGÍAS DE LA INFORMACIÓN**	
CLAVE: **xxxxxx**	UNIDAD DE ENSEÑANZA - APRENDIZAJE: **CRIPTOGRAFÍA CUÁNTICA**	TRIM: **III o IV**
HORAS TEORÍA: **4.5**	SERIACIÓN **AUTORIZACIÓN**	CRÉDITOS: **9**
HORAS PRÁCTICA: **0**		OPT/OBL: **OPT.**

OBJETIVO(S): Que el alumnado sea capaz de comprender, formular y aplicar las técnicas y protocolos criptográficos actuales en escenarios prácticos de redes de comunicación, evaluando su eficacia y vulnerabilidades; los principios de la criptografía cuántica y su superioridad en seguridad; y la implementación básica de protocolos cuánticos, aplicando los principios de Distribución Cuántica de Claves (QKD) en entornos simulados.

CONTENIDO SINTÉTICO:

1. **Fundamentos de criptografía.**
   - 1.1. Historia y conceptos básicos iniciales.
   - 1.2. Cifrados simétricos y sus aplicaciones.
   - 1.3. Criptografía asimétrica y protocolos seguros.
   - 1.4. Implementación en redes de comunicación.
2. **Computación cuántica y amenazas.**
   - 2.1. Principios de mecánica cuántica aplicada.
   - 2.2. Computación cuántica versus computación clásica.
   - 2.3. Algoritmos cuánticos y su impacto.
   - 2.4. Vulnerabilidades de sistemas criptográficos actuales.
3. **Criptografía cuántica y aplicaciones.**
   - 3.1. Protocolos de distribución cuántica de claves.
   - 3.2. Criptografía basada en entrelazamiento cuántico.
   - 3.3. Redes cuánticas y desafíos tecnológicos.
   - 3.4. Aplicaciones prácticas y proyectos finales.

MODALIDADES DE CONDUCCIÓN DEL PROCESO DE ENSEÑANZA-APRENDIZAJE:
Exposición que realizará la persona docente en la que enfatizará los aspectos más importantes de cada tema, haciendo ver que existe una unidad dentro de cada uno de ellos.

MODALIDADES DE EVALUACIÓN:
Evaluaciones periódicas, tareas y ejercicios a juicio del personal académico responsable. La modalidad particular de evaluación se le comunicará al alumnado al inicio del curso en forma detallada.

Evaluación de recuperación:

1. La UEA no tiene evaluación de recuperación.

BIBLIOGRAFÍA NECESARIA O RECOMENDABLE:

1. Katz, J. y Lindell, Y. Introduction to Modern Cryptography. Chapman and Hall/CRC, Boca Raton, 2015.
2. Lo, H-K. y Lütkenhaus, N. Quantum Cryptography: from Theory to Practice, arXiv 0702202 (2007).
3. Rieffel, E. y Polak, W. Quantum Computing: A Gentle Introduction. MIT Press, Massachusetts, 2014.
4. Schneier, B. Applied Cryptography: Protocols, Algorithms, and Source Code in C, Hoboken, Wiley, 2015.
5. Stallings, W. Cryptography and Network Security: Principles and Practice. Prentice Hall, New York, 2011.
6. Van Assche, G. Quantum Cryptography and Secret-Key Distillation. Cambridge University Press, Cambridge (2010).