BENÉMERITA UNIVERSIDAD AUTÓNOMA DE PUEBLA
FACULTAD DE CIENCIAS DE LA COMPUTACION

MAESTRIA EN CIENCIAS DE LA COMPUTACION

Área: Sistemas Distribuidos

Programa de Asignatura: Criptografía

Código: MCOM 22214

Tipo: Optativa

Créditos: 9

Fecha: Noviembre 2012

1. DATOS GENERALES

Nombre del Programa Educativo:	Maestría en Ciencias de la Computación
Modalidad Académica:	Escolarizada
Nombre de la Asignatura:	Criptografía
Ubicación:	Segundo o tercer semestre (Optativa)

2. REVISIONES Y ACTUALIZACIONES

Autores:	Dra. Bárbara Sánchez Rinza Dr. Manuel Martín Ortiz Dr. Ivo Pineda Torres Dr. José Luis Carballido Carranza
Fecha de diseño:	Noviembre 2012
Fecha de la última actualización:	Marzo 2019
Revisores:	Dra. Bárbara Sánchez Rinza
Sinopsis de la revisión y/o actualización:	Actualización de referencias

3. OBJETIVOS:

***General*:**

El alumno se familiarizará con métodos, algoritmos y herramientas necesarias para la implementación de aplicaciones criptográficas y de seguridad de datos. Aprenderá a cómo establecer una comunicación segura entre dos o más entidades de manera tal que se garantice un alto grado de confidencialidad, integridad y autenticidad en los datos y documentos intercambiados.

Específicos:

1.- El estudiante aprende a entender y distinguir los problemas de comunicación en presencia de un adversario. Aprende también a evaluar y construir protocolos para resolver dichos problemas.

2.- Aprenderá la importancia de las funciones One Way en la protección de passwords.

3.- Entenderá la relación entre generadores de bits aleatorios, la teoría de la complejidad y el diseño de algoritmos.

4.- Entenderá el papel central de las funciones y permutaciones pseudo-aleatorias en la creación de protocolos.

5.- Aprenderá a usar los algoritmos de cifrado para procesar texto.

4. CONTENIDO

Unidad	Contenido Temático/Actividades de aprendizaje
1. Introducción	1.1 Introducción a la criptografía 1.2 Encriptación Moderna: Una teoría basada en complejidad computacional 1.3 Lista de candidatos One Way Functions 1.4 Definiciones de seguridad 1.5 El modelo del adversario
2. Funciones	2.1 Funciones SHA-0 y SHA-1 2.2 Funciones HMAC 2.3 Función RIPEMD-160 2.3 La función Logaritmo discreto 2.4 La función RSA 2.5 Función CRC32
3. Generadores de Bits Aleatorios	3.1 Generación de sucesiones pseudo-aleatorias de bits y de números 3.2 Existencia de un generador pseudo-aleatorio 3.3 Ejemplos de generadores aleatorios
4. Cifras Block	4.1 Definición 4.2 Encriptación estándar de datos (DES) 4.3 Construcción 4.4 Rapidez 4.5 DES iterados y DESX 4.6 Encriptación Estándar Avanzada (AES) 4.7 Limitaciones de seguridad basada en Key recovery
5. Funciones Pseudo Aleatorias	5.1 Familias de funciones 5.2 Funciones aleatorias y permutaciones 5.3 Funciones y permutaciones pseudo-aleatorias 5.4 Modelo arquitectónico 5.5 El lema de intercambio PRPPRF 5.6 Sucesiones de familias de PRP's y PRF's
6. Encriptación de Llave Privada	6.1 Esquemas simétricos de encriptación 6.2 Ejemplos 6.3 Otros ejemplos de encriptación simétrica
7. Encriptación de Llave Pública	7.1 Ejemplos 7.2 Definición de seguridad 7.3 Encriptación probabilística de la llave pública

Unidad	Contenido Temático/Actividades de aprendizaje
8. Cifrado con curvas algebraicas	8.1 Criptosistema de curvas elípticas 8.2 Acuerdo de clave con curvas elípticas 8.3 Criptosistema de curvas elípticas: ECC 8.4 Criptosistema de curvas hiperelípticas

Bibliografía	
Básica	**Complementaria**
I. - W. Trappe y L.C. Washington. Introduction to Cryptography with Coding Theory, Prentice Hall, 2 Ed. 2006. 2.- W. Stallings. Cryptography and Network Security, Principles and Practice. Prentice-Hall. 6 Ed. 2013. 3.- Simon Singh. The Code Book, The Secret History of Codes and Code Breaking. Anchor 2000. 4.- Víctor Shoup. A Computational Introduction to Number Theory and Algebra. Cambridge University Press 2008. 5.- Bruce Schneier. Applied Criptography Protocols, Algorithms, and Source Code in C. Second Edition. John Wiley & Sons.	1.- Luis Espino , Criptografia, primera edición, editorial Kindle, 2016 2.- Federico Pacheco, Crtiptografia, editorial Ursers, 2015

5. CRITERIOS DE EVALUACIÓN

Criterios	Porcentaje
• Exámenes	40%
• Participación en clase	5%
• Tareas	20%
• Exposiciones	
• Simulaciones	5%
• Trabajo de investigación y/o de intervención	
• Prácticas de laboratorio	15%
• Reporte de actividades académicas y culturales	
• Mapas conceptuales	
• Proyecto final	15%
Total	100%