1. IDENTIFICACIÓN DEL CURSO

Nombre de la materia

Encriptación de datos

Clave de la materia:	Horas de teoría:	Horas de práctica:	Total de Horas:	Valor en créditos:
IC466	**40**	**40**	**80**	**8**

Tipo de curso: (Marque con una X)															
C= curso		P= practica		**CT = curso–taller**	**X**	M= módulo		C= clínica		S= seminario	

Nivel en que ubica: (Marque con una X)			
L=Licenciatura	**X**	P=Posgrado	

Prerrequisitos formales (Materias previas establecidas en el Plan de Estudios)	Prerrequisitos recomendados (Materias sugeridas en la ruta académica aprobada)
IC465 Hackeo ético y pruebas de seguridad	

Departamento:

Ciencias Exactas y Tecnología (DCET)

Carrera:

Licenciatura en Tecnologías de la información

Área de formación:

Área de formación básica común obligatoria.		Área de formación básica particular obligatoria.		Área de formación básica particular selectiva.		Área de formación especializante obligatoria.		**Área de formación especializante selectiva**	**X**

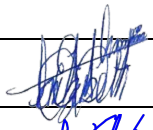
Historial de revisiones:

Acción: Revisión, Elaboración	Fecha:	Responsable
Elaboración	**16/08/2018**	**Mtro. Víctor Becerra Córdoba**
Revisión	**15/01/2019**	**Mtro. Víctor Becerra Córdoba**
Revisión	**15/01/2020**	**Dr. Héctor Alfonso Juárez López**
Revisión	**Enero 2021**	**Mtra. María del Rocío Ramírez Jiménez**
Revisión	**Enero 2023**	**Mtra. María del Rocío Ramírez Jiménez**

Academia:

Cómputo

Aval de la Academia:

Marzo 2023		
Nombre	**Cargo** Presidente, Secretario, Vocales	**Firma**
Mtra. Larisa Elizabeth Lara Ramírez	**Presidente**	
Dra. Auria Lucia Jiménez Gutiérrez	**Secretario**	

2. PRESENTACIÓN

La criptografía se encarga de cifrar o codificar mensajes para evitar que su contenido pueda ser leído por un tercero no autorizado; es decir, la generación de códigos y algoritmos de cifrado que buscan ofuscar la información y protegerla de "ojos curiosos" es el cometido principal de esta disciplina.
La criptografía es una de las áreas que componen la criptología; su misión es mucho más amplia y también se ocupa del criptoanálisis, es decir, romper las codificaciones realizadas por terceros (como ejemplo podemos tomar a la NSA o los descifradores de códigos de la Segunda Guerra Mundial), la esteganografía (la ocultación de mensajes dentro de canales inseguros de manera que pasen desapercibidos) y el estegoanálisis, que busca, precisamente, detectar los mensajes ocultos mediante esteganografía.

3. OBJETIVO GENERAL

El alumno comprenderá y aplicará tipos y métodos de criptografía y será capaz de implementarlos en diferentes lenguajes y plataformas

4. OBJETIVOS ESPECÍFICOS

- El alumno conocerá los elementos básicos de una arquitectura de seguridad
- El alumno conocerá e implementará algunos algoritmos clásicos de cifrado (transposición)
- El alumno conocerá los principios básicos del cifrado por bloques
- El alumno conocerá los principios básicos del cifrado de clave abierta
- El alumno conocerá los principios básicos de la autentificación digital

5. CONTENIDO

Temas y Subtemas

Módulo I. Introducción a la seguridad informática

1.1 Tendencias en la seguridad
1.2 El modelo OSI
1.3 Ataques servicios y mecanismos de seguridad

Módulo II. Técnicas clásicas de cifrado

2.1 Cifrado simétrico
2.2 Sustitución
2.3 Transposición

2.4 Máquinas de cifrado

Módulo III. DES y AES

3.1 Cifrado en bloques
3.2 DES
3.3 Análisis de DES
3.4 AES
3.5 Análisis de AES

Módulo IV. Aspectos de cifrado simétrico

4.1 Cifrado múltiple y triple DES
4.2 Cifrado de flujo
4.3 Seguridad en los canales de comunicación
4.4 Distribución y generación de llaves

Módulo V. Cifrado de clave abierta

5.1 Algoritmos de teoría de números
5.2 Principios de un sistema de clave abierta
5.3 RSA
5.4 Cifrado con curvas elípticas

Módulo VI. Autentificación

6.1 Funciones de autentificación
6.2 Códigos de autentificación
6.3 Funciones resumen
6.4 Algoritmos HASH y MAC
6.5 Firmas digitales
6.6 Protocolos de autentificación

Módulo VII. Aplicaciones

7.1 Kerberos
7.2 PGP
7.3 S/MIME
7.4 Seguridad en IP
7.5 Aspectos generales de la seguridad en web

6. TAREAS, ACCIONES Y/O PRÁCTICAS DE LABORATORIO

a) Aprendizaje grupal y autogestivo.
b) Investigación grupal e individual.
c) Integración individual de productos de aprendizaje (reportes de lectura, ensayos, trabajos de investigación, exposición de temas, prácticas de algunos temas, portafolio, entre otros).
d) Exposición por parte del maestro sobre los temas (pizarrón, diapositivas, etc.).

7. BIBLIOGRAFÍA BÁSICA (Preferentemente ediciones recientes, 5 años)

1	William Stallings, Cryptography and Network security; Principles and Practice, 7th ed, Prentice Hall, 2016
2	Al Sweigart, Hacking Secret Ciphers with Python: A beginner's guide to cryptography

	and computer programming with Python, CreateSpace Independent Publishing Platform, 2013
3	Scott A. Vanstone, A. J. Menezes, Paul C. van Oorschot, Handbook of Applied Cryptography, 5th de, CRC Press, 2001

8. BIBLIOGRAFÍA COMPLEMENTARIA (Preferentemente ediciones recientes, 5 años)

1	Jean-Philippe Aumasson, Serious Cryptography: A Practical Introduction to Modern Encryption, No Starch Press, 2017
2	Keith Martin, Everyday Cryptography: Fundamental Principles and Applications, 2nd Ed, Oxford University Press, 2017
3	Kratikal Academy, Cryptography: Data and Application Security, Independently published, ISBN-10: 15220728102017

9. CRITERIOS Y MECANISMOS PARA LA ACREDITACIÓN

- Aprendizaje grupal y autogestión.
- Integración de equipos para la solución de problemas
- Integración individual de productos de aprendizaje (reportes de lectura, ensayos, formatos de intervención, trabajos de investigación, presentaciones, entre otros).

10. EVALUACIÓN Y CALIFICACIÓN

Unidad de Competencia	Porcentaje
Proyecto final	25%
Tareas	15%
Prácticas	25%
Exámenes Parciales	20%
Formalidad	15%
Total	**100%**

Cambios (revisión y/o actualización)	
Descripción del cambio o actualización	**Realizó**
Se adecuó la cantidad de tópicos yel orden de los mismos	Dr. Héctor Alfonso JuárezLópez
Se revisó el contenido y no hubo cambios	Mtra. María del Rocío Ramírez Jiménez