1. INFORMACIÓN DEL CURSO

Denominación: Criptografía	**Tipo:** Curso-taller	**Nivel**: Superior
Área de formación:	**Obligatorio** ☐ **Optativo** ■	**Prerrequisitos:** Ninguno
Horas: Teoría; 48 Práctica; 16 Totales: 64	**Créditos:** 7	
Elaboró:		**Fecha de actualización o elaboración:** Abril 2017

2. DESCRIPCIÓN

Objetivo general

El alumno conocerá los elementos básicos de un sistema criptográfico, será capaz de analizar e implementar sistemas criptográficos tanto de clave simétrica como de clave abierta y describirá los principales elementos en un sistema de seguridad para redes de computadoras.

Objetivos parciales

Identificar los elementos básicos de un sistema criptográfico
Conocer e implementar técnicas de cifrado de clave simétrica
Conocer e implementar técnicas de cifrado de clave abierta
Conocer técnicas estándar de codificación, como DES, AES, RSA, PGP, etc

Contenido temático sintético

1. Introducción
2. Técnicas clásicas de cifrado
3. DES y AES
4. Aspectos de cifrado simétrico
5. Cifrado de clave abierta
6. Autentificación
7. Aplicaciones

Estructura conceptual

1. Introducción
1.1 Tendencias en la seguridad
1.2 La arquitectura de seguridad OSI
1.3 Ataques, servicios y mecanismos de seguridad
2. Técnicas clásicas de cifrado
2.1 Cifrado simétrico
2.2 Substitución
2.3 Transposición
2.4 Máquinas de cifrado
3. DES y AES
3.1 Cifrado en bloques
3.2 DES
3.3 Análisis de DES
3.4 Elementos básicos de Teoría de números
3.5 AES
3.6 Análisis de AES
4. Aspectos de cifrado simétrico
4.1 Cifrado múltiple y triple DES
4.2 Cifrado de flujo

4.3 Seguridad de los canales de comunicación
4.4 Distribución de ll
5. 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
6. 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
7. Aplicaciones
7.1 Kerberos
7.2 PGP
7.3 S/MIME
7.4 Seguridad en IP
7.5 Aspectos generales de seguridad en WEB

Modalidades del proceso enseñanza aprendizaje

Mixta

Competencias que el alumno deberá adquirir

Capacidad de comprensión, trabajo colaborativo, aplicación de los conocimientos teóricos.

Campo de aplicación profesional de los conocimientos promovidos en la Unidad

En mantener la información segura, entre otras áreas como son: la seguridad de mensajes, negociación clave y administración de claves. En en desarrollo y aplicación de técnicas para la creación de criptografía en los productos.

Modalidad de evaluación y factores de ponderación

Exámenes 40%
Prácticas 40%
Actividades integradoras 20%

3. BIBLIOGRAFÍA

a) Básica:

William Stallings, Cryptography and Network Security: Principles and Practice, 5ª ed, Prentice Hall, 2011
David Hook, Beginning Cryptography with Java, Wrox Press, 2005
Nichols, Randall K. Seguridad para comunicaciones inalámbricas : redes, protocolos, criptografía y soluciones, McGraw-Hill, 2003
Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, Handbook of applied cryptography, 5th ed, CRC Press, 2001