



CRIPTOGRAFÍA

Asignatura

Clave

8°, 9°

Semestre

06

Créditos

Ingeniería Eléctrica

División

Ingeniería en Computación

Departamento

Ingeniería en Computación

Carrera en que se imparte

Asignatura:

Obligatoria de elección

Optativa

Horas:

Teóricas

Prácticas

Total (horas):

Semana

16 Semanas

Modalidad: Curso.

Asignatura obligatoria antecedente: Ninguna.

Asignatura obligatoria consecuente: Ninguna.

Objetivo(s) del curso:

El alumno conocerá, explicará y aplicará los diferentes algoritmos criptográficos, etodologías y técnicas de cifrado que le permitan analizar, diseñar, desarrollar y/o seleccionar mecanismos y herramientas de seguridad orientados a brindar seguridad informática.

Temario

NÚM.	NOMBRE	HORAS
1.	Panorama general	6.0
2.	Técnicas clásicas de cifrado	12.0
3.	Gestión de claves	6.0
4.	Criptografía simétrica o de clave secreta	12.0
5.	Criptografía asimétrica o de clave pública	12.0
		48.0
	Prácticas de laboratorio	0.0
	Total	48.0

CRIPTOGRAFÍA

(2 / 5)



1 Panorama general

Objetivo: El alumno conocerá los antecedentes históricos de la criptografía y su evolución a través del tiempo. Asimismo el alumno entenderá los requerimientos de la seguridad de la información dentro del mundo del cómputo y las redes.

Contenido:

- 1.1 Historia de la Criptografía.
- 1.2 Servicios y Mecanismos de Seguridad.
- 1.3 Ataques.
- 1.4 La Arquitectura de Seguridad de OSI.

2 Técnicas clásicas de cifrado

Objetivo: El alumno conocerá, comprenderá y aplicará las técnicas clásicas de la criptografía y los principales algoritmos que han sentado las bases de la criptografía moderna.

Contenido:

- 2.1 Introducción y clasificación de los sistemas de cifrado.
- 2.2 Operaciones utilizadas.
 - 2.2.1 Algoritmos de Sustitución.
 - 2.2.1.1 Monoalfabética: cifrado del César.
 - 2.2.1.2 Polialfabética: cifrado de Desplazamiento, Vigenère y Vernam.
 - 2.2.2 Algoritmos de Transposición.
 - 2.2.2.1 Simple.
 - 2.2.2.2 Doble.
 - 2.2.2.3 Máscaras rotativas.
- 2.3 Números de claves.
 - 2.3.1 Sistemas de una clave.
 - 2.3.1.1 Cifradores simétricos.
 - 2.3.2 Sistemas de dos claves.
 - 2.3.2.1 Cifradores asimétricos.
- 2.4 Formas de procesamiento de datos.
 - 2.4.1 Procesadores seriales o en flujo.
 - 2.4.2 Procesadores por bloques.

3 Gestión de claves

Objetivo: El alumno entenderá la importancia de las claves de seguridad, así como la forma correcta de su manejo, generación, procesamiento y administración.

Contenido:

- 3.1 Políticas de gestión de claves.
 - 3.1.1 Motivos.
 - 3.1.2 Políticas.



- 3.2 Tipos de claves.
 - 3.2.1 Estructural.
 - 3.2.2 Maestra.
 - 3.2.3 Primaria y Secundaria.
 - 3.2.4 De generación de claves.
 - 3.2.5 De sesión o de mensaje.
 - 3.2.6 De cifrado de archivos.
- 3.3 Generadores y distribución de claves.
 - 3.3.1 Generadores pseudoaleatorios.
 - 3.3.1.1 Período.
 - 3.3.1.2 Distribución de uno's y cero's.
 - 3.3.1.3 Imprevisibilidad.
 - 3.3.1.4 Estructuras básicas de generación de claves.
 - 3.3.2 KDC (Key Distribution Center).

4 Criptografía simétrica o de clave secreta

Objetivo: El alumno conocerá, comprenderá y aplicará los principales algoritmos simétricos de la criptografía.

Contenido:

- 4.1 Introducción a la Criptografía Simétrica.
 - 4.1.1 Características de los algoritmos simétricos.
 - 4.1.2 Herramientas matemáticas: operaciones lógicas, corrimientos, sistemas de numeración, teoría de grupos, teoría de campos y otras.
 - 4.1.3 Principales algoritmos simétricos: IDEA (International Data Encryption Algorithm), Blowfish, RC5 (Rivest Cipher), DES(Data Encryption Standard), 3DES y AES (Advanced encryption standard).
- 4.2 Des y 3des (data encryption standard).
 - 4.2.1 Orígenes.
 - 4.2.1.1 Historia.
 - 4.2.1.2 Teoría de la información: técnicas sugeridas por Shannon.
 - 4.2.2 Algoritmos de cifrado y descifrado.
 - 4.2.2.1 Procesamiento y transformación de claves: diagramas de flujo.
 - 4.2.2.2 PROCESO y transformación de los bloques de datos: diagramas de flujo.
 - 4.2.3 Aplicación del algoritmo.
 - 4.2.3.1 Procesamiento y transformación de claves: caso práctico.
 - 4.2.3.2 4.2.3. 2 procesamiento y transformación de claves: caso práctico.
 - 4.2.4 Nivel de seguridad que proporcionan.
 - 4.2.4.1 Análisis de los algoritmos.
- 4.3 AES (Advanced Encryption Standard).
 - 4.3.1 Orígenes.
 - 4.3.1.1 Historia.
 - 4.3.1.2 Campos de Galois.
 - 4.3.2 Algoritmos de cifrado y descifrado (claves de 128, 192 y 256 bits).
 - 4.3.2.1 Procesamiento y transformación de claves: diagramas de flujo.
 - 4.3.2.2 Proceso y transformación de los bloques de datos: diagramas de flujo.
 - 4.3.3 Aplicación de los algoritmos.
 - 4.3.3.1 Procesamiento y transformación de claves: Caso práctico.



- 4.3.3.2 Procesamiento y transformación de claves: Caso práctico.
- 4.3.4 Nivel de seguridad que proporciona.
 - 4.3.4.1 Análisis de los algoritmos.

5 Criptografía asimétrica o de clave pública

Objetivo: El alumno conocerá, comprenderá y aplicará los principales algoritmos asimétricos de la criptografía.

Contenido:

- 5.1 Introducción a la Criptografía Asimétrica.
 - 5.1.1 Características de los algoritmos asimétricos.
 - 5.1.2 Herramientas matemáticas: Algoritmo de Euclides, Teorema de Euclides, Teorema de la División de Euclides, Algoritmo Extendido de Euclides, Anillo de Números Enteros Módulo m, Teorema de Euler, Teorema de Fermat, Logaritmos Discretos, Logaritmos Discretos Elípticos, Teoría de Polinomios y otras.
 - 5.1.3 Principales algoritmos asimétricos: Diffie-Hellman, El Gamal, RSA (Rivest-Shamir-Adelman), DSA (Digital signature Algorithm), Funciones Hash y Curvas Elípticas.
- 5.2 Diffie-Hellman.
 - 5.2.1 Orígenes.
 - 5.2.2 El algoritmo y las matemáticas modulares.
 - 5.2.3 RSA (Rivest-Shamir-Adelman).
 - 5.2.4 Orígenes.
 - 5.2.5 Algoritmo de cifrado y descifrado.
 - 5.2.6 Cálculo de claves (pública y privada).
 - 5.2.7 Aplicación del algoritmo.
- 5.3 Funciones Hash.
 - 5.3.1 MD4 (Message Digest Algorithm).
 - 5.3.2 MD5 (Message Digest Algorithm).
 - 5.3.3 SHA (Standard High Algorithm).
 - 5.3.4 Firmas digitales.
- 5.4 Curvas Elípticas.
 - 5.4.1 Grupos abelianos.
 - 5.4.2 Curvas elípticas sobre números reales.
 - 5.4.3 Descripción geométrica.
 - 5.4.4 Descripción algebraica.

Bibliografía básica:

DE LA GUÍA, M. Dolores, et al.
Técnicas Criptográficas de Protección de Datos
 España
 Ra-Ma, 1997

Temas para los que se recomienda:

Todos



MENEZES, Alfred J., et al
Handbook of Applied Cryptography
 5th edition
 Canada
 CRC, 2001

Todos

Bibliografía complementaria:

STALLINGS, William
Cryptography and Network Security: Principles and Practices
 3rd edition
 U.S.A.
 Pearson Education, 2003

Todos

Sugerencias didácticas:

Exposición oral	<input checked="" type="checkbox"/>
Exposición audiovisual	<input checked="" type="checkbox"/>
Ejercicios dentro de clase	<input checked="" type="checkbox"/>
Ejercicios fuera del aula	<input checked="" type="checkbox"/>
Seminarios	<input checked="" type="checkbox"/>

Lecturas obligatorias	<input checked="" type="checkbox"/>
Trabajos de investigación	<input checked="" type="checkbox"/>
Prácticas de taller o laboratorio	<input checked="" type="checkbox"/>
Prácticas de campo	<input type="checkbox"/>
Otras	<input type="checkbox"/>

Forma de evaluar:

Exámenes parciales	<input checked="" type="checkbox"/>
Exámenes finales	<input checked="" type="checkbox"/>
Trabajos y tareas fuera del aula	<input checked="" type="checkbox"/>

Participación en clase	<input checked="" type="checkbox"/>
Asistencias a prácticas	<input checked="" type="checkbox"/>
Otras	<input type="checkbox"/>

Perfil profesiográfico de quienes pueden impartir la asignatura

El profesor deberá contar con licenciatura, preferentemente de las carreras: Ingeniero en Computación, Ingeniero en Electrónica, Ingeniero en Telecomunicaciones, Licenciado en Ciencias Computacionales o formación equivalente y contar con amplia experiencia en seguridad en informática, mecanismos y herramientas de seguridad y especialmente en manejo de algoritmos criptográficos.