



UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO  
FACULTAD DE INGENIERÍA



PROGRAMA DE ESTUDIO

**CRIPTOGRAFÍA**

**2930**

**9,10**

**8**

Asignatura

Clave

Semestre

Créditos

**INGENIERÍA ELÉCTRICA**

**INGENIERÍA  
EN COMPUTACIÓN**

**INGENIERÍA  
EN COMPUTACIÓN**

División

Departamento

Licenciatura

**Asignatura:**

Obligatoria

Optativa

**Horas/semana:**

Teóricas

Prácticas

Total

**Horas/semestre:**

Teóricas

Prácticas

Total

**Modalidad:** Curso teórico

**Seriación obligatoria antecedente:** Ninguna

**Seriación obligatoria consecuente:** Ninguna

**Objetivo(s) del curso:**

El alumno decidirá los diferentes algoritmos criptográficos, metodologías y técnicas de cifrado que le permitan analizar, diseñar, desarrollar y elegir 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	10.0
4.	Criptografía simétrica o de clave secreta	12.0
5.	Criptografía asimétrica o de clave pública	12.0
6.	Aplicaciones criptográficas	12.0
		64.0
	Actividades prácticas	0.0
	Total	64.0

## 1 Panorama general

**Objetivo:** El alumno identificará los antecedentes históricos de la criptografía y su evolución a través del tiempo, entendiendo los requerimientos de la seguridad de la información dentro del mundo del cómputo y las redes.

**Contenido:**

### 1.1 Historia de la criptografía.

#### 1.1.1 Criptografía en el mundo.

#### 1.1.2 Criptografía en México.

### 1.2 Servicios y mecanismos de seguridad.

## 2 Técnicas clásicas de cifrado

**Objetivo:** El alumno aplicará las técnicas clásicas de la criptografía y los principales algoritmos para conocer las bases de la criptografía moderna.

**Contenido:**

### 2.1 Introducción y clasificación de los sistemas de cifrado.

#### 2.1.1 Número de claves: algoritmos simétricos y asimétricos.

#### 2.1.2 Formas de procesar datos: algoritmos en flujo y en bloque.

#### 2.1.3 Operaciones utilizadas: sustitución y transposición.

### 2.2 Algoritmos de sustitución.

#### 2.2.1 Monoalfabética: Polybios, César, Afin, Playfair y Hill.

#### 2.2.2 Polilfabética: Alberti, Vigenére , Beaufort, Vernam y Enigma.

### 2.3 Algoritmos de transposición.

#### 2.3.1 Inversa, simple y doble.

#### 2.3.2 Grupos y series.

#### 2.3.3 Filas y columnas.

#### 2.3.4 Máscaras rotativas.

## 3 Gestión de claves

**Objetivo:** El alumno interpretará 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.
- 3.3.2 Postulados de Golomb y pruebas estadísticas.
- 3.3.3 KDC (Key Distribution Center) y KTC (Key Translation Center).

#### 4 Criptografía simétrica o de clave secreta

**Objetivo:** El alumno aplicará los principales algoritmos simétricos de la criptografía para su desarrollo.

**Contenido:**

- 4.1 Introducción a la criptografía simétrica.
  - 4.1.1 Características de los algoritmos simétricos.
  - 4.1.2 Principales algoritmos simétricos: RC4 (Rivest Cipher 4), A5 (Algoritmo de comunicaciones móviles), IDEA (International Data Encryption Algorithm), Blowfish, Twofish, DES (Data Encryption Standard), 3DES, AES (Advanced Encryption Standard), GOST (Algoritmo soviético de cifrado), y RC6 (Rivest Cipher 6).
- 4.2 DES y 3DES (Data Encryption Standard).
  - 4.2.1 Orígenes.
  - 4.2.2 Algoritmos de cifrado y descifrado.
  - 4.2.3 Aplicación del algoritmo.
  - 4.2.4 Nivel de seguridad.
- 4.3 AES (Advanced Encryption Standard).
  - 4.3.1 Orígenes.
  - 4.3.2 Algoritmos de cifrado y descifrado (claves de 128, 192 y 256 bits).
  - 4.3.3 Aplicación de los algoritmos.
  - 4.3.4 Nivel de seguridad.

#### 5 Criptografía asimétrica o de clave pública

**Objetivo:** El alumno aplicará los principales algoritmos asimétricos de la criptografía para su desarrollo.

**Contenido:**

- 5.1 Introducción a la criptografía asimétrica.
  - 5.1.1 Características de los algoritmos asimétricos.
  - 5.1.2 Principales algoritmos asimétricos: Diffie-Hellman, El Gamal, RSA (Rivest-Shamir-Adelman), DSA (Digital signature Algorithm), Funciones Hash y Curvas elípticas.
- 5.2 Diffie-Hellman y El Gamal.
  - 5.2.1 Orígenes.
  - 5.2.2 Algoritmo Diffie-Hellman y el problema del logaritmo discreto.
  - 5.2.3 Algoritmo El Gamal y el problema del logaritmo discreto.
  - 5.2.4 Fortaleza de los algoritmos.
- 5.3 RSA (Rivest-Shamir-Adelman).
  - 5.3.1 Orígenes.
  - 5.3.2 Algoritmo de cifrado y descifrado.
  - 5.3.3 Cálculo de claves (pública y privada).
  - 5.3.4 Aplicación del algoritmo.

- 5.4 Funciones Hash.

- 5.4.1 MD5 (Message Digest Algorithm).
- 5.4.2 SHA-1 y SHA-2 (Standard High Algorithm).
- 5.4.3 RIPEMD-160.

## 5.5 Curvas elípticas.

- 5.5.1 Curvas elípticas sobre números reales.
- 5.5.2 Descripción geométrica.
- 5.5.3 Descripción algebraica.

## 5.6 Introducción a la criptografía cuántica.

- 5.6.1 Introducción y entrelazamiento cuántico.
- 5.6.2 Propiedades y protocolos.
- 5.6.3 Conjunción de criptografía cuántica y moderna.

## 5.7 Ataques y vulnerabilidades.

## 6 Aplicaciones criptográficas

**Objetivo:** El alumno evaluará aplicaciones reales de criptografía para la aplicación de algoritmos criptográficos a protocolos de comunicación; relacionando la criptografía con aplicaciones y herramientas de seguridad.

**Contenido:**

### 6.1 Firmas digitales.

- 6.1.1 El Gamal.
- 6.1.2 DSA.
- 6.1.3 RSA.

### 6.2 Certificados.

- 6.2.1 Autoridades certificadoras.
- 6.2.2 Estándares para certificados.
- 6.2.3 Tipos de certificados.

### 6.3 Aplicaciones a redes.

- 6.3.1 IPsec: Diffie-Hellman y AES.
- 6.3.2 Redes inalámbricas: WEP, WPA y WPA2.
- 6.3.3 Aplicaciones de Hash: MAC y HMAC.
- 6.3.4 Suites de herramientas para transacciones seguras: TLS, SSL, PGP, tokens.

### Bibliografía básica

FERGUSON, Niels, SCHNEIER, Bruce  
*Practical Cryptography*  
 Indiana  
 John Wiley & Sons, 2003

FERGUSON, Niels, SCHNEIER, Bruce, et al.  
*Cryptography Engineering*  
 Indianapolis

### Temas para los que se recomienda:

2, 3, 4, 5, 6

Todos

John Wiley & Sons, 2010

LÓPEZ, Jaquelina

*Criptografía*

Todos

México

Universidad Nacional Autónoma de México, Facultad de Ingeniería, 2009

MAIORANO, Ariel

*Criptografía*

1, 2, 4, 5, 6

Argentina

Alfaomega, 2009

MENEZES, Alfred, VAN OORSCHOT, Paul, et al.

*Handbook of Applied Cryptography*

Todos

5th edition

Canada

CRC Press, 2001

OPPIGER, Rolf

*Sistemas de Autenticación para Seguridad en Redes*

1, 3, 6

España

Alfaomega, 1998

STALLINGS, William

*Cryptography and Network Security: Principles and Practices*

Todos

3th edition

Pearson Education, 2003

### **Bibliografía complementaria**

### **Temas para los que se recomienda:**

FUSTER, Amparo, DE LA GUÍA, Dolores, et al.

*Técnicas Criptográficas de Protección de Datos*

1, 2, 3, 4, 5, 6

España

Ra-Ma editorial, 1997

SCHNEIER, Bruce

*Applied Cryptography*

2, 3, 4, 5, 6

John Wiley & Sons, 1996

**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"/>
Uso de software especializado	<input type="checkbox"/>
Uso de plataformas educativas	<input type="checkbox"/>

Lecturas obligatorias	<input checked="" type="checkbox"/>
Trabajos de investigación	<input checked="" type="checkbox"/>
Prácticas de taller o laboratorio	<input type="checkbox"/>
Prácticas de campo	<input type="checkbox"/>
Búsqueda especializada en internet	<input type="checkbox"/>
Uso de redes sociales con fines académicos	<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"/>
Asistencia a prácticas	<input checked="" type="checkbox"/>

**Perfil profesiográfico de quienes pueden impartir la asignatura**

Licenciatura en Ingeniería en Computación, Ciencias de Computación, Ingeniería Eléctrica Electrónica, Ingeniería en Telecomunicaciones, Matemáticas Aplicadas o una carrera similar. Deseable haber realizado estudios de posgrado, contar con conocimientos y experiencia en el área de Seguridad y/o Tecnologías de la Información especialidad en criptografía, contar con experiencia docente o haber participado en cursos o seminario de iniciación en la práctica docente.