



---

ASIGNATURA:	CRIPTOGRAFÍA
DEPARTAMENTO:	ING. EN SIST. DE INFORMACION
AREA:	ELECTIVA
BLOQUE	TECNOLOGÍAS APLICADAS

MODALIDAD:	Cuatrimestral
HORAS SEM.:	6 horas
HORAS/AÑO:	96 horas
HORAS RELOJ	72
NIVEL:	4°
AÑO DE DICTADO:	2018

---

### Objetivos

- Adquirir una actitud crítica y reflexiva en el almacenamiento y transferencia de la información en forma segura aplicando la criptografía.
- Adquirir los conocimientos necesarios para determinar la identidad, autenticidad y veracidad de la información transmitida y recibida.
- Obtener las técnicas y herramientas para la aplicación, creación y análisis de los criptosistemas actuales y presentación de las nuevas tendencias.

### Contenidos Mínimos (Programa Sintético)

Introducción e Historia de la criptografía. Criptografía Clásica. Criptografía Moderna / Criptografía de clave Secreta. Criptografía Moderna / Criptografía de clave Pública. Protocolos TLS/Kerberos/IPSec. Redes Wireless. Funciones Hash Criptográficas. Certificados Digitales y Firmas. Introducción a las Curvas Elípticas. Introducción a la Criptografía Quántica.

### Contenidos Pedagógicos

#### Unidad I: *Introducción a la Criptografía.*

Conceptos fundamentales, criptología, criptografía, criptoanálisis. Categorización. Clasificaciones fundamentales. Historia, orígenes y necesidades a cubrir. Evolución histórica a través de las ciencias. Cronología y aplicaciones militares a lo largo de la historia.



**Unidad II: *Criptografía clásica.***

Funciones. Inversibilidad. Cifrado de Bloque y de Flujo. Sustitución. Monoalfabético, monográfico y poligráfico. Polialfabético. Transposición. Composición de Ciphers. Confusión y Difusión

**Unidad III: *Criptografía moderna. Claves secretas Simétrica***

Teoría de números. Congruencias. Clases de equivalencia. Espacio de Claves. Algoritmos de factorización. Generación de números primos. Cifrado Simétrico. 3DES. AES. IDEA. RC4. Blowfish. Problemática de los algoritmos.

**Unidad IV: *Técnicas avanzadas de criptografía. Claves públicas Asimétrica***

Cifrado Asimétrico. Conceptos de criptografía pública. Key Agreement Diffie Hellman. RSA. DSA. El Gamal. Análisis de factorización. Principales aspectos para tener en cuenta. Esteganografía.

**Unidad V: *La criptografía en la seguridad de las redes. Protocolos***

Protocolos TLS/Kerberos/y otros. DSS. PGP. SSH. SSL. TLS. Kerberos. IPsec. Implementación en GNU/Linux y en Windows. Análisis de Técnicas de Intrusión

**Unidad VI: *La criptografía en las redes inalámbricas. Redes Wireless***

Redes Wireless. Implementación WEP 64 bits y 128 bits. Manejo de Múltiples Claves. Implementación y riesgos de RC4. Scrambling. Implementación de WPA. Análisis de AES sobre Wifi. MAC

**Unidad VII: *Aplicaciones criptográficas. Funciones hash***

Funciones hash Criptográficas. Message Digest. MD2, MD4, MD5. Sha-1. Tiger. Colisiones. Versiones simplificadas. Implementación de claves en GNU/Linux. Salts. Random Generators. Certificados Digitales y Firmas. CA. X.509. Integridad. Identificación Autenticación. Usos y aplicación. Estructura de Certificados. PKI. Revisión de DSA. Generación de CA y Certificados OpenSSL

**Unidad VIII: *Últimas tendencias en criptografía.***

Introducción a las Curvas Elípticas. ECC. Curvas Elípticas. Campos finitos. Teorema de Hasse. DH Elíptico. DSA Elíptico. Teorema de Lagrange. Algoritmo de Schoof. Reducción Rápida. Ataque de canales paralelos. Introducción a la Criptografía Quántica. Introducción a la mecánica cuántica. Conceptos de Computación Quántica. Qubits. Infraestructura y Limitaciones. Puntos de aplicación y Costos. Tendencias de utilización. Ventajas y desventajas respecto a la tradicional. Criptografía Ligera. Concepto y principales algoritmos.



## Bibliografía

- Alfred J. Menezes, 1996, Handbook of Applied Cryptography, Editorial CRC.
- Bruce Schneier, 1996, Applied Cryptography: Protocols, Algorithms, and Source Code in C, 2nd Edition, Editorial John Wiley & Sons.
- Wenbo Mao, 2003, Modern Cryptography: Theory and Practice, 1st edition, Editorial Prentice Hall PTR.
- William Stallings, 2010, Cryptography and Network Security. Principles and Practice, 5th edition, Editorial Prentice Hall.
- Simon Singh, 2002, The Code Book: How to Make It, Break It, Hack It, Crack It. Editorial Delacorte Books for Young Readers.
- Darrel Hankerson, Alfred J. Menezes, Scott Vanstone, 2004, Guide to Elliptic Curve Cryptography, 1st edition, Editorial Springer.
- Gilles Van Assche, 2006, Quantum Cryptography and Secret-Key Distillation, 1st edition, Editorial Cambridge University Press.
- Alexander W. Dent, Yuliang Zheng, and Moti Yung, 2010, Practical Signcryption (Information Security and Cryptography), Editorial Springer.
- Andreas Klein, 2013, Stream Ciphers, Editorial Springer

## Correlativas

### Para Cursar:

Cursadas:

- Diseño de Sistemas
- Sistemas Operativos
- Gestión de Datos

Aprobadas:

- Análisis de Sistemas
- Sintaxis y Semántica del Lenguaje
- Paradigmas de Programación

**Para rendir:**

Aprobadas:

- Diseño de Sistemas
- Sistemas Operativos
- Gestión de Datos