



ASIGNATURA:	CRIPTOGRAFÍA	CÓDIGO:	
DEPARTAMENTO:	INGENIERÍA EN SISTEMAS DE INFORMACIÓN	DE CLASE:	Cuatrimestral
ÁREA:	INGENIERÍA EN SISTEMAS DE INFORMACIÓN	HORAS SEM.:	6 hs.
BLOQUE:	ELECTIVAS	HORAS / AÑO:	Reloj 72hs./ Catedra 96hs

Fundamentación:

El Ingeniero en Sistemas de Información debe estar formado en las competencias necesarias para desempeñarse, con eficiencia y efectividad, en actividades orientadas a proyectar y dirigir lo referido a seguridad informática, su implementación, operación y mantenimiento, certificando funcionamiento, condición de uso o estado. Del mismo modo, en sus actividades reservadas relacionadas con la especificación, proyección y desarrollo de sistemas de información, de comunicación de datos y de software, las amenazas actuales y tendencias de ciberataques no le dejan margen para soslayar los atributos de confidencialidad, integridad, disponibilidad, autenticidad, no repudio y responsabilidad en las características de calidad de dichos objetos de trabajo.

La mayor parte de los atributos de seguridad se pueden garantizar mediante el uso de los criptosistemas adecuados y el conocimiento de las técnicas criptográficas que emplean. Por ello, resulta necesario que los estudiantes de la carrera de Ingeniería en Sistemas de información conozcan los sistemas criptográficos, sus fortalezas y debilidades, y puedan evaluar e implementar los productos adecuados a cada necesidad o requerimiento de sistemas.

La asignatura tiene como finalidad brindar una visión actualizada de la criptografía moderna, los antecedentes de sus métodos clásicos, y las tecnologías empleadas, para que los futuros profesionales puedan tomar decisiones correctas y usar racionalmente los productos disponibles en el mercado a partir de los conocimientos teóricos básicos y actividades prácticas que se aborden en la asignatura.

Conocer los criptosistemas eficientes, y su aplicación a los negocios y a las operaciones en Internet, será un activo valioso en la formación profesional que nuestros Ingenieros en Sistemas de Información podrán capitalizar en sus competencias como un elemento diferenciador.



*Universidad Tecnológica Nacional
Facultad Regional Buenos Aires*

Objetivos:

Identificar riesgos y amenazas en el almacenamiento y transferencia de la información para realizarlo en forma segura aplicando la criptografía.

Reconocer la identidad, autenticidad y veracidad de la información transmitida y recibida, así como su confidencialidad e integridad.

Utilizar técnicas y herramientas de aplicación, creación y análisis de los criptosistemas actuales y valoración de las nuevas tendencias.

Programa analítico:

Unidad Temática 1: Introducción a la Criptografía.

Conceptos fundamentales, criptología, criptografía, criptoanálisis. Conceptos básicos de seguridad y criptografía. Matemática discreta. Uso de problemas matemáticos en la criptografía. Seguridad de los algoritmos criptográficos. Nociones de teoría de la información. Codificación de la información. Clasificaciones fundamentales. Evolución histórica a través de las ciencias y aplicaciones a lo largo de la historia. Modelos y tipos de ataque a un criptosistema.

Unidad Temática 2: Criptografía clásica.

Funciones. Inversibilidad. Permutación. Sustitución. Transposición. Matrices. Confusión y Difusión. Principios de Kerckhoffs. Cifrado Monoalfabético, monográfico y poligráfico. Cifrado Polialfabético.

Unidad Temática 3: Criptografía moderna de Clave Simétrica

Teoría de números. Congruencias. Clases de equivalencia. Espacio de Claves. Composición de Cifradores. Cifrado de Bloque y de Flujo. Secuencias pseudoaleatorias. Algoritmos de factorización. Generación de números primos. Cifrado Simétrico. 3DES. AES. IDEA. RC4. Blowfish. Problemática de los algoritmos.

Unidad Temática 4: Criptografía moderna de Clave Asimétrica

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

Unidad Temática 5: Criptografía en la seguridad de las redes

Protocolos TLS/Kerberos/y otros. DSS. PGP. SSH. SSL. TLS. Kerberos. IPsec. Implementaciones. Técnicas de Intrusión.

Unidad Temática 6: La criptografía en las redes inalámbricas

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 7: Aplicaciones criptográficas para Integridad, Autenticidad y Firma Digital

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 8: 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 Cuántica. Qubits. Criptografía post-cuántica. Criptografía Ligera. Concepto y principales algoritmos. Criptografía aplicada en las criptomonedas. Criptografía maliciosa.

Distribución de carga horaria entre actividades teóricas y prácticas:

Tipo de actividad	Carga horaria total en hs. reloj	Carga horaria total en hs. cátedra
Teórica	54	72
Formación Práctica	0	0
Formación Experimental	0	0
Resolución de Problemas	0	0
Proyectos de Diseño	18	24
Práctica Supervisada	0	0
Total	72	96

Articulación Horizontal y vertical con otras materias

La asignatura Criptografía se articula en forma vertical con tres (3) asignaturas que la preceden en el plan de estudio, específicamente Diseño de Sistemas, Sistemas Operativos y Gestión de Datos.

El alumno deberá tener cursada cada una de estas asignaturas al momento de comenzar la cursada. En cuanto a la articulación horizontal, Criptografía brinda conocimientos que son compatibles y complementarios con conceptos y contenidos de otras asignaturas del mismo Nivel: Ingeniería de Software, Comunicaciones y Redes de Información, contribuyendo así la interdisciplinariedad.

El equipo docente participa de reuniones inter-cátedras convocadas por el Departamento, a fin de generar acuerdos temáticos y de metodologías que faciliten la articulación horizontal y vertical entre las distintas asignaturas.



Cronograma estimado de clases:

Unidad temática	Duración en horas cátedra
1	12
2	12
3	12
4	16
5	12
6	8
7	12
8	12

Bibliografía:

- Alexander, W. Dent, Y. and Moti, Y. (2010). Practical Signcryption (Information Security and Cryptography). Editorial Springer.
- Hankerson, D. Menezes, A. Vanstone, S. (2004). Guide to Elliptic Curve Cryptography. (1st edition). Editorial Springer.
- Houtven, L. (2016). Crypto 101: the book. CC BY-NC 4.0 license. <https://github.com/crypto101/book>.
- Klein, A. (2013). Stream Ciphers. Editorial Springer
- Menezes, Alfred. (1996). Handbook of Applied Cryptography. Editorial CRC.
- Ramió Aguirre, J. (2018). Curso de Criptografía Aplicada. Criptored. <http://www.criptored.upm.es/download/CursoCriptografiaAplicada2018.pdf>
- Schneier, B. (1996). Applied Cryptography: Protocols, Algorithms, and Source Code in C. (2nd Edition). Editorial John Wiley & Sons.
- Singh, S. (2002). The Code Book: How to Make It, Break It, Hack It, Crack It. Editorial Delacorte Books for Young Readers.
- Stallings, W. (2010). Cryptography and Network Security. Principles and Practice. (5th edition). Editorial Prentice Hall.
- Stinson, D. Paterson, M. (2019). Cryptography, Theory and Practice. (Fourth Edition). CRC Press.
- Van Assche, G. (2006). Quantum Cryptography and Secret-Key Distillation. (1st edition). Editorial Cambridge University Press.
- Wenbo, M. (2003). Modern Cryptography: Theory and Practice. (1st edition). Editorial Prentice Hall PTR.

PÁGINAS WEB DE INTERÉS

- Criptored: <http://www.criptored.upm.es/>
- Digital Currency Initiative: <https://dci.mit.edu/>
- Crypt4you: <http://www.criptored.upm.es/crypt4you/portada.html>
- Cryptocurrency Engineering and Design: <https://ocw.mit.edu/courses/media-arts-and-sciences/mas-s62-cryptocurrency-engineering-and-design-spring-2018/index.htm>
- Cryptomathic. White papers: <https://www.cryptomathic.com/resources/white-papers>
- El Manual de Criptografía: <https://www.electronicdesign.com/technologies/embedded-revolution/whitepaper/21127823/maxim-integrated-the-cryptography-handbook>



Universidad Tecnológica Nacional
Facultad Regional Buenos Aires

- Wikimedia de la categoría
- Intypedia: <https://commons.wikimedia.org/wiki/Category:Cryptography>
- Intypedia: <http://www.criptored.upm.es/intypedia/index.php?lang=es>

Criptografía:

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