Carrera INGENIERIA EN INFORMATICA		
Asignatura 3662 – Matemática Aplicada		
Trayecto Ciencias Básicas		
Año académico 2023		
Responsable / Jefe de cátedra Mg. Ing. Jorge Eterovic		
Carga horaria semanal: 6 hs	**Carga horaria total:** 96 hs	**Créditos** ----
Modalidad: Presencial		
Correlativas anteriores: PROBABILIDAD Y ESTADISTICA	**Correlativas posteriores**: ELECTIVA II	
Conocimientos necesarios Matemática Discreta		

Descripción de la asignatura

La asignatura Matemática Aplicada, está planteada como una materia teórico - práctica donde los alumnos conocerán los fundamentos de Matemática que son la base de los sistemas criptográficos modernos. Se estudian los distintos sistemas criptográficos y sus aplicaciones. Dada la dinámica de los contenidos de la materia los temas a tratar en la misma van desde tecnología de base a temas actuales de mercado.

Metodología de enseñanza

La materia adoptará la modalidad “taller”, combinando clases teórico-prácticas con la actividad de seguimiento presencial. De esta manera, se utilizará la modalidad de evaluación continua, a través de la resolución de los diferentes trabajos prácticos que se centrarán en el uso de herramientas de software, utilizando el método de casos y trabajando en equipo con la supervisión de los docentes.

Objetivos de aprendizaje

- Adquirir los conocimientos necesarios para comprender el funcionamiento de los sistemas criptográficos.
- Obtener las técnicas y herramientas para la aplicación, creación y análisis de los criptosistemas actuales y de las nuevas tendencias.
- Lograr una actitud crítica y reflexiva para determinar las mejores técnicas criptográficas en el almacenamiento y transferencia segura de la información.
- Adquirir el deseo de la investigación así como también de la aplicación de nuevas tecnologías relacionadas.

Contenidos mínimos

Teoría y Análisis Numéricos. Complejidad computacional. Teoría de la Información. Primalidad. Criptosistemas simétricos DES e IDEA. Campos de Galois. Criptosistema simétrico AES. Criptografía Ligera. Logaritmo Discreto. Criptosistemas asimétricos Diffie-Hellman y El Gamal. - Factorización. Criptosistema asimétrico RSA. Curvas Elípticas. Criptosistema asimétrico ECDSA. Funciones de Hash MD5, SHA1-2 y SHA3 Keccak . Firma

Digital. Sello de Tiempo. Blockchain. Contratos Inteligentes. Non Fungible Tokens (NFT). Algoritmos Cuánticos. Criptografía Post Cuántica.

Competencias a desarrollar

Genéricas

- Desempeño en equipos de trabajo.
- Comunicación efectiva.
- Actuación profesional ética y responsable.
- Aprendizaje continuo.
- Identificación, formulación y resolución de problemas de ingeniería en sistemas de información/informática.
- Concepción, diseño y desarrollo de proyectos de ingeniería en sistemas de información / informática.
- Utilización de técnicas y herramientas de aplicación en la ingeniería en sistemas de información / informática.
- Generación de desarrollos tecnológicos y/o innovaciones tecnológicas.
- Desarrollo de una actitud profesional emprendedora.

Específicas

- Proyectar y dirigir lo referido a seguridad informática
- Especificación, proyecto y desarrollo de sistemas de información.
- Especificación, proyecto y desarrollo de sistemas de comunicación de datos.
- Especificación, proyecto y desarrollo de software.
- Dirección y control de la implementación, operación y mantenimiento de sistemas de información, sistemas de comunicación de datos, software, seguridad informática y calidad de software.

Programa analítico	
Unidad 1	**Historia de 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 2	**Criptografía clásica** Funciones. Inversibilidad. Cifrado de Bloque y de Flujo. Sustitución. Monoalfabético, monográfico y poligráfico. Polialfabético. Transposición. Composición de Ciphers. Confusión y Difusión.
Unidad 3	**Base matemática de la Criptografía. Criptografía de clave Pública** Base matemática de la Criptografía. Cifrado Asimétrico. Conceptos de criptografía pública. Key Agreement Diffie Hellman. RSA. DSA. El Gamal. Análisis de factorización. Principales aspectos a tener en cuenta.

Unidad 4	**Criptografía de clave Secreta** 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 5	**Criptografía ligera** Introducción a la Criptografía ligera. Principios matemáticos. Algoritmos. Aplicaciones. Seguridad en dispositivos RFID e Internet de las Cosas.
Unidad 6	**Funciones hash Criptográficas** Funciones hash Criptográficas. Message Digest. MD2, MD4, MD5. Sha-1. Tiger. Colisiones. Versiones simplificadas. Implementación de claves en GNU/Linux. Salts. Random Generators.
Unidad 7	**Protocolos criptográficos en redes de datos** Protocolos de seguridad usados en las redes de datos: SSL/TLS, Kerberos, IPSec, SSH. Aplicación en PGP. Implementación de seguridad en Sistemas Operativos GNU/Linux y Windows.
Unidad 8	**Criptografía en 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 9	**Certificados Digitales y Firma Digital** 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 10	**Criptografía basada en Curvas Elípticas** Introducción a las Curvas Elípticas. ECC. Curvas Elípticas. Campos finitos. Teorema de Hasse. DH Elíptico. DSA Elíptico.
Unidad 11	**Criptografía Cuántica y Poscuántica** Teorema de Lagrange. Algoritmo de Schoof. Reducción Rápida. Ataque de canales paralelos. Introducción a la Criptografía Quántica. Introducción a la mecánica quántica. Conceptos de Computación Quántica. Qubits. Infraestructura y Limitaciones. Puntos de aplicación y Costos. Tendencias de utilización. Ventajas y desventajas respecto a la tradicional.
Unidad 12	**Aplicaciones Criptográficas** Blockchain. Contratos inteligentes. NFT: Non-Fungible Tokens. Nuevas tecnologías.

Planificación de actividades					
Semana	*Clase*	*Actividad. Detalle de la actividad a desarrollar*	*Tipo (indicar el tipo de actividad a desarrollar: teoría, práctica, práctica de laboratorio,*	*Duración estimada*	*Unidad*

			trabajo de campo, otra)		
1	1	Presentación de la asignatura. Normas de cátedra. Historia de la Criptografía.	Teórico	4	1
1	2	Práctica métodos clásicos	Práctica	2	1
2	3	Criptografía Moderna.	Teórico	4	2
2	4	Introducción a Cryptohack	Práctica	2	2
3	11	Base matemática de la Criptografía. Criptografía de clave Pública	Teórico	4	3
3	12	Práctica de RSA	Práctica	2	3
4	7	Criptografía de Clave Secreta.	Teórico	4	4
4	8	Práctica de de Diffie Hellman	Práctica	2	4
5	9	Criptografía de Clave Secreta: AES (continuación)	Teórico	4	4
5	10	Práctica de AES	Práctica	2	4
6	5	Criptografía Ligera.	Teórico	4	5
6	6	Presentación TP 2do. Parcial	Práctica	2	5
7	13	Funciones hash Criptográficas	Teórico	4	6
7	14	Práctica de Hash	Práctica	2	6
8	15	Protocolos criptográficos en Redes.	Teórico	4	7
8	16	Práctica de JWT	Práctica	2	7
9	17	Criptografía en Redes Wireless. Certificados Digitales y Firma Digital	Teórico	4	8 9
9	18	Clase de consulta	Práctica	2	
10	19	PRIMER PARCIAL		4	
10	20	Revisión del TP 2do. Parcial	Práctica	2	
11	21	Criptografía de Curvas Elípticas	Teórico	4	10
11	22	Práctica de Curvas Elípticas	Práctica	2	10
12	23	Criptografía Cuántica y Postcuántica	Teórico	4	11
12	24	Práctica de Criptografía Postcuántica	Práctica	2	11
13	25	Aplicaciones Criptográficas	Teórico - Práctica	4	12
13	26	Clase de consulta	Práctica	2	
14	27	SEGUNDO PARCIAL – Presentaciones Trabajos Finales		4	

14	28	SEGUNDO PARCIAL – Presentaciones Trabajos Finales		2	
15	29	RECUPERATORIO		4	
15	30	RECUPERATORIO		2	
16	31	Cierre de la materia		4	

Evaluación			
Descripción del proceso evaluativo desarrollado por la cátedra: La evaluación de los conocimientos adquiridos se llevará a cabo en dos instancias. Mediante la aprobación de un primer parcial teórico-práctico que consistirá en preguntas acerca de los fundamentos de los algoritmos criptográficos y del estado actual de la criptografía y en el segundo se evaluará la implementación práctica de una serie de algoritmos expuestos en la cursada. Se trabajará en equipos y se deberá hacer una presentación teórico-práctica de los productos y resultados obtenidos.			
Primera evaluación	Semana 10	Presencial	2 horas (19 a 21 hs.)
Segunda evaluación	Semana 14; Clases 27 y 28	Presencial	6 horas (19 a 23 hs. Y 19 a 21 hs.)
Recuperatorio	Semana 15; Clases 29 y 30	Presencial	6 horas (19 a 23 hs. Y 19 a 21 hs.)

Bibliografía obligatoria				
Título	**Autor**	**Editorial**	**Edición**	**Año**
Beginning cryptography with Java	Hook, David	Wiley	2005	1ra Ed.
Matemáticos, espías y piratas informáticos	Gómez Urgellés, Joan	RBA	2011	1ra Ed.
Aventuras matemáticas	Cagliero, Leandro; [*et al.*]	Instituto Nacional de Educación Tecnológica	2010	1ra Ed.
Las matemáticas en la criptología	María Isabel González Vasco	Ed. Catarata	2018	1ra Ed.
Manual de criptografía	Francisco José Plaza Martín	Ediciones Universidad Salamanca	2021	1ra Ed.

Bibliografía complementaria recomendada				
Título	**Autor**	**Editorial**	**Edición**	**Año**
Menezes, Alfred	Handbook of Applied Cryptography	CRC Press	2001	5ta Ed.
Pacheco, Federico	Criptografía	RedUsers	2014	1ra Ed.

Scolnik, Hugo	Qué es la seguridad informática	Paidós	2014	1ra Ed.
López Lucena, Manuel	Criptografía y Seguridad en Computadores	Creative Commons	2015	4ta Ed.

Otros recursos obligatorios (videos, enlaces, otros) Incluir una fila por cada recurso	
Nombre	
Material de la cátedra	https://miel.unlam.edu.ar/

Otros recursos complementarios (videos, enlaces, otros) Incluir una fila por cada recurso	
Nombre	