MAT-377: Criptografía

Identificación

Asignatura:	Criptografía
Sigla:	MAT–377
Area Curricular:	Algebra
Modalidad:	Semestral
Nivel Semestral:	Séptimo Semestre, Ciclo de Orientación
Horas Teóricas:	4 por semana en dos sesiones
Horas Prácticas:	2 por semana en una sesión
Pre–Requisitos Formales:	MAT–141 y MAT-120
Carreras destinatarias:	Matemática y Carreras de FCPN

Objetivos

Los objetivos básicos que se pretenden son: Dotar al alumno de los conceptos básicos, mecanismos y técnicas necesarias para entender, desarrollar y aplicar la criptografía. Adquirir una formación en criptografía simétrica, asimétrica de clave publica.

Competencias

Estudia y fundamenta claves públicas de seguridad de información que se transfiere a través de redes informáticas ya que el uso generalizado de las computadoras y el advenimiento de la Internet lleva a la necesidad de enviar información confidencial financiera y de otro a través de canales públicos. Esto provocó un intenso desarrollo de la criptografía matemática, tanto simétrica y de clave publica. En la actualidad, la criptografía se ha convertido en esencial; como en transacciones bancarios, información de tarjetas de cr édito, etc. se envían a través de canales inseguros.

Objeto de la Materia

El objetivo de la materia es que los alumnos adquieran una formación en Criptografía.

Analiza y demuestra las propiedades locales de curvas y superficies definidas por funciones diferenciables. Aplica los resultados en el desarrollo de la misma teoría y es capaz de generar ejemplos de curvas y superficies regulares, y resuelve problemas teóricos y prácticos de la geometría intrínseca con implementación computacional mediante un razonamiento deductivo, inductivo, por analogías o heurísticas apropiadas.

Programa Sintético

Ideas básicas de criptografía. Criptosistemas Simétricos. Protocolos criptográficas, La criptografía de clave pública. Criptografía de curva elíptica.

Contenidos analíticos

1. *Ideas básicas de criptografía:1.1* Criptografía Matemática *1.2* Criptografía, Criptoanálisis y Criptosistemas *1.3* Breve historia de la criptografía *1.4* Cifrado y Teoría de Nú meros *1.5* Criptografía de claves públicas *1.6* Criptosistemas y el espacio de claves.
2. *Criptosistemas simétricos:2.1* Cifrado Mixto *2.2* Bloques Cifrados *2.3* Secuencias Cifrados *2.4* DES y AES
3. *Protocolos criptográficos:3.1* Funciones Hash Criptográficas *3.2* Esquema de Shamir.
4. *La criptografía de clave pública:4.1* Cifrado ElGamal *4.2* Cifrado por medio de RSA *4.3* Residuos cuadráticas y cifrado Rabin
5. *Criptografía de curva elíptica:5.1* La estructura de grupo de las curvas elípticas *5.2* Curvas elípticas sobre cuerpos finitos *5.3* Criptografía con curvas elípticas

Estructura de Evaluación

La evaluación es la valoración de las competencias de conocimientos (saber), habilidades (saber hacer) y de valores (saber ser) alcanzadas mediante exámenes parciales periódicas (60 %), prácticas e implementaciones de laboratorio (15 %) y una evaluación final (25 %) de todo el contenido de la asignatura. Sobre un total de 100 %, la nota mínima de aprobación en el pregrado es de 51 %. La distribución de temas por parciales, así como el cronograma de los exámenes se presenta en un plan de trabajo al inicio del semestre. También está prevista un examen de recuperación de cualquier examen parcial cuya nota reemplaza a la anterior.

Métodos y Medios Didácticos

Los métodos didácticos aplicados en el proceso de enseñanza y aprendizaje de la materia son las exposiciones magistrales del docente que utiliza recursos educativos y métodos de razonamiento *inductivo*, *deductivo*, *analógico* y *heurístico* para inducir el aprendizaje *por descubrimiento propio, dialogado, programado y demostrativo* que permita al estudiante desarrollar su potencialidad *creativa* con pensamiento crítico capaz de demostrar y presentar los teoremas con rigor lógico utilizando el lenguaje matemático formal. Los medios didácticos que dispone la Carrera son las aulas equipadas con medios audio visuales, laboratorio de computación con internet, aplicaciones computacionales, guías de practicas, material impreso o digital, mapas conceptuales y una Biblioteca especializada que facilita el desarrollo teórico y práctico de la asignatura.

Auxiliatura de docencia

Las materias del ciclo intermedio y de orientación no tienen auxiliatura de docencia. Los trabajos prácticos realizados en la materia son monitoriados por el mismo docente.

Criterios de Evaluación

La evaluación de la asignatura consiste en pruebas escritas u orales, donde se valora la aplicación adecuada de *conceptos*, *teoremas* y *métodos* en la *demostración* o *resolución* de problemas planteados; y, en la calificación de prácticas o trabajos de laboratorios cuyo informe debe estar escrito en un *lenguaje matemático* adecuado con rigor lógico. Se valora de forma adicional la *creatividad* y la *simplicidad* en la presentación de sus resultados.

Cronograma de Avance

Semana	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Capítulos	1				2						3						4			

Bibliografía

[1] Gilbert Baumslag, Benjamin Fine, Martin Kreuzer, Gerhard Rosenberger, *A Course in Mathematical Cryptography*, 2015.

[2] Jeffrey Hoffstein Jill Pipher Joseph H. Silverman, *An Introduction to Mathematical Cryptography*, 2008, Springer.

[3] Ariane M. Masuda Daniel Panario, *Tópicos de Corpos Finitos com Aplicações em Criptografia e Teoria de Códigos*, IMPA, 2007.

[4] Neal Koblitz, *Algebraic Aspects of Cryptography*, Springer-Verlag, 2004.