PROGRAMA DE ASIGNATURA

ELECTIVO: Curvas elípticas y criptografía
Profesor: Nicolas Thériault

Departamento	Departamento de Matemática y Ciencia de la Computación
Código Plan	
TEL	T = 6 E= 0 L= 0
SCT	
Requisitos	Álgebra abstracta
Descripción del curso	Introducción a las curvas elípticas sobre cuerpos finitos, su estructura de grupo, algunas de sus aplicaciones prácticas y estudio de algunas de las herramientas esenciales para llegar a estas aplicaciones.
Objetivos	1. Conocer el grupo de una curva elíptica y su estructura 2. Conocer algunas de las aplicaciones prácticas de las curvas elípticas sobre cuerpos finitos 3. Entender la teoría detrás de algunas de las herramientas esenciales para el uso práctico de las curvas elípticas
Contenidos	1. Definiciones de las curvas elípticas 2. Curvas elípticas sobre los complejos y estructura de grupo 3. Curvas elípticas sobre cuerpos finitos y operaciones de grupo 4. Aplicaciones criptográficas de las curvas elípticas 5. Conteo de puntos 6. Tests de primalidad
Metodología	Clases teóricas a cargo del profesor, listado de ejercicios que deben resolver los estudiantes, laboratorios computacionales a desarrollar por los estudiantes. Desarrollar tareas (ejercicios sobre la materia), laboratorios (computacionales) y/o exposición sobre materia relacionada al curso.
Evaluación	Opción entre: • 2 tareas y 2 laboratorios sobre la materia del curso. o • 1 tarea, 1 laboratorio y 1 presentación en clase (resumen) de un articulo relacionado a la materia del curso.
Bibliografía	1. I.F. Blake, G. Seroussi, N.P. Smart, Elliptic Curves in Cryptography, Cambridge University Press, 1999. 2. I.F. Blake, G. Seroussi, N.P. Smart, Advances in Elliptic Curve

	Cryptography, Cambridge University Press, 2008. 3. H. Cohen, G. Frey, Hanbook of Elliptic and Hyperelliptic Curve Cryptography, Chapman & Hall / CRC, 2006. 4. L.C. Washington, Elliptic Curves: Number Theory and Cryptography, Second Edition, CRC Press, 2008.