Universidad de los Andes
Facultad de Ciencias

DEPARTAMENTO DE MATEMÁTICAS

OFRECIMIENTOS DE CURSOS

2019-10

<table>
<tr><td rowspan="4">Nivel del Curso

4: posgrado X

3: final de carrera X

2: mitad de carrera __

1: inicio de carrera ___</td><td>Nombre completo del curso en español:

Elliptic Curve Cryptography</td></tr>
<tr><td>Nombre completo del curso en inglés:

Elliptic Curve Cryptography</td></tr>
<tr><td>Nombre abreviado en español (Máx. 30 caracteres contando espacios)

Elliptic Curve Cryptography</td></tr>
<tr><td>Profesor: David Karpuk</td></tr>
<tr><td colspan="2">Descripción del curso en español:</td></tr>
<tr><td colspan="2">Descripción del curso en inglés: This course will serve as both an introduction to elliptic curves and their applications to cryptography. Approximately the first 2/3 of the course will establish the basic material concerning elliptic curves, from an algebraic and number theoretic perspective. This will include the basics of the algebraic geometry of elliptic curves and essential results from the theory of elliptic curves over finite fields, such as the Hasse bound. The last 1/3 of the course will be devoted to standard material in public-key cryptography, such as the discrete logarithm problem, key exchanges, digital signatures, hash functions, and hyperelliptic curve cryptography.

No previous knowledge of either elliptic curves or cryptography is assumed.</td></tr>
<tr><td colspan="2">Prerrequisitos: Abstract Algebra 2 OR Algebraic Coding Theory</td></tr>
</table>

Universidad de los Andes
Facultad de Ciencias

Objetivos: By the end of the course, the students will have a firm understanding of the algebra and number theory of elliptic curves, and understand their role in modern-day cryptographic systems. Among the most important objectives are the to understand the following:

1. Computing on elliptic curves: understanding the addition law, algorithms for computing orders of points, calculating the number of points on an elliptic curve, etc.
2. Algebraic geometry of elliptic curves: projective space, coordinate rings, divisors and differentials, and elliptic curves over the complex numbers
3. Elliptic curves over finite fields: the Hasse bound, Schoof's algorithm, supersingular elliptic curves, factorization algorithms, the Weil pairing
4. The Discrete Logarithm Problem: Generic attacks, attacks on specific kinds of curves
5. Public Key Cryptography: Two-party and multi-party key exchanges, Diffie-Hellman key exchange, digital signatures, hash functions, supersingular isogeny cryptography

Contenido: See above

Forma de Evaluación: The course grade will be based entirely on four homework assignments, each worth 20% of the final grade, and a final project, worth the last 20% of the final grade. There are no exams.

Bibliografía: Washington - Elliptic Curves: Number Theory and Cryptography