MATH-409  
Algebraic curves and cryptography

**Cursus**  
Cybersecurity  MA2, MA4  Opt.  
Informatique  MA2, MA4  Opt.  
Ing.-math  MA2, MA4  Opt.  
Mathématicien  MA2  Opt.  
SC master EPFL  MA2, MA4  Opt.

**Sem.**  
Language  English  
Credits  5  
Session  Summer  
Semester  Spring  
Exam  Written  
Workload  150h  
Weeks  14  
Hours  4 weekly  
Lecture  2 weekly  
Exercises  2 weekly  
Number of positions

**Remarque**  
Cours donnés en alternance tous les deux ans (pas donné en 2019-20)

**Summary**  
The goal of this course is to introduce basic notions from public-key cryptography based on algebraic curves over finite fields. We will introduce basic cryptographic schemes as well as discuss in-depth the discrete logarithm problem for elliptic and Jacobians of higher genus curves.

**Content**  
Topics may include, but are not limited to:  
- Introduction to algebraic curves  
- Elliptic and hyperelliptic curves  
- Jacobians of algebraic curves  
- Cantor arithmetic  
- Elliptic curve discrete logarithm problem  
- Index calculus methods for Jacobians  
- Pairing-based cryptography

**Keywords**  
algebraic curves over finite fields, public key cryptography, discrete logarithms, pairing-based cryptography

**Learning Prerequisites**  
**Required courses**  
Abstract Algebra required (groups theory, rings, fields, field extensions, finite fields)

**Recommended courses**  
- Math 317 (Galois theory)  
- Math 489 (Number Theory in Cryptography)  
- COM-401 (Security and Cryptography)

**Teaching methods**  
Weekly lectures, problem sets and programming assignments.
Assessment methods
written exam

Resources
Bibliography
• P. Griffiths, *Introduction to Algebraic Curves*
• I. Blake, G. Seroussi, and N. Smart, *Elliptic Curves in Cryptography*
• I. Blake, G. Seroussi, N. Smart, *Advances in Elliptic Curve Cryptography*

Ressources en bibliothèque
• *Introduction to Algebraic Curves / Griffiths*
• *Advances in Elliptic Curve Cryptography / Blake & al.*
• (electronic version)
• *Elliptic Curves in Cryptography / Blake & al.*