- Faculté des sciences
- www.unine.ch/sciences

Applied elliptic curves (3MT2084)

Filières concernées	Nombre d'heures	Validation	Crédits ECTS
Bachelor en mathématiques	**Cours: 2 ph** **Exercice: 2 ph**	**Voir ci-dessous**	6
Master en mathématiques	**Cours: 2 ph** **Exercice: 2 ph**	**Voir ci-dessous**	6

ph=période hebdomadaire, pg=période globale, j=jour, dj=demi-jour, h=heure, min=minute

Période d'enseignement:

- Semestre Printemps

Equipe enseignante

CAMINATA Alessio, Maître Assistant (B219, alessio.caminata@unine.ch); LANDOLINA Cristina, Assistant (B207, cristina.landolina@unine.ch)

Contenu

Plane projective curves, plane cubics and their group law, Weierstrass form of an elliptic curve, elliptic curves over finite fields, Discrete Logarithm Problem (DLP), Diffie-Hellman key exchange, El Gamal cryptosystem, attacks to the DLP on elliptic curves, elliptic-curve factorization method. If time permits other topics may be treated.

Forme de l'évaluation

oral exam of 30 minutes on the content of the lectures and exercises

Documentation

L.C. Washington - Elliptic Curves. Number Theory and Cryptography.
J. H. Silverman - The Arithmetic of Elliptic Curves.
J. H. Silverman, J. Tate - Rational Points on Elliptic Curves.
D. Stinson - Cryptography: Theory and Practice.

Pré-requis

Knowledge of linear algebra and basic algebra notions: groups, rings, fields (in particular finite fields).
Basic notions of computational complexity such as polynomial, exponential, subexponential time complexity and the big O notation.

Forme de l'enseignement

Cours: 2h, TP: 2h