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

Cryptography (3MT2058)

Filières concernées	Nombre d'heures	Validation	Crédits ECTS
Master en mathématiques	**Cours: 2 ph** **Exercice: 2 ph**	**oral: 30 min**	6

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

Période d'enseignement:

- Semestre Printemps

Equipe enseignante:

Elisa Gorla and Alberto Ravagnani

Objectifs:

Cryptography is the study of mathematical techniques for secure communication in the presence of third parties (called adversaries). More generally, it is about constructing and analyzing protocols that overcome the influence of adversaries and which are related to various aspects in information security such as data confidentiality, data integrity, and authentication. Cryptography has applications to many aspects of our everyday life, e.g., ATM cards, computer passwords, and electronic commerce.

Contenu:

After an introduction to classical cryptography, we will concentrate on modern cryptographic schemes. Our focus will be on the mathematical primitives and techniques, especially within public-key cryptography. Main topics that we will treat are: prime numbers and RSA, primality testing and integer factoring, Diffie-Hellmann key exchange, El Gamal encryption, the Discrete Logarithm Problem and related algorithms, elliptic curves and the Elliptic Curve Discrete Logarithm Problem.

Forme de l'évaluation:

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

Pré-requis:

Linear algebra and a basic algebra course (e.g., modular arithmetic, Euclidean algorithm, polynomials, finite fields).

Forme de l'enseignement:

ex cathedra