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

Cryptography (3MT2058)

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

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

Période d'enseignement:

- Semestre Automne

Equipe enseignante

Professeure: Elisa Gorla,
Assistant: Tom Kaiser.

Contenu

Après une introduction à la cryptographie classique, nous nous concentrerons sur les schémas cryptographiques modernes. Nous nous concentrerons sur les techniques et les primitives mathématiques, en particulier dans le cadre de la cryptographie à clé publique. Les principaux sujets que nous traiterons sont les suivants: nombres premiers et RSA, tests de primalité et factorisation d'entiers, échange de clés Diffie-Hellmann, cryptage El Gamal, problème du logarithme discret et algorithmes associés, courbes elliptiques et problème du logarithme discret à courbe elliptique.

Forme de l'évaluation

Examen oral de 30 minutes.

Documentation

D. Stinson, Cryptography: Theory and Practice

Pré-requis

Algèbre linéaire et algèbre.

Forme de l'enseignement

Ex cathedra