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

Cryptographie (3MT2058)

Filières concernées	Nombre d'heures	Validation	Crédits ECTS
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

Professeure: Elisa Gorla
Assistante: Giulia Gaggero

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. A la fin du cours nous aborderons la cryptographie post quantique.

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.

Objectifs d'apprentissage

Au terme de la formation l'étudiant-e doit être capable de :

- Produire examples et contra-exemples
- Générer des nouvelles preuves
- Adapter les arguments et strategies utilisés pendant le cours pour les appliquer à de nouveaux exemples
- Produire des nouvelles strategies pour resoudre des problemes similaires a les problemes vues pendant le cours
- Reproduire les définitions et les preuves vues pendant le cours
- Produire des preuves correctes et complètes
- Analyser les théorèmes du cours et leurs démonstrations
- Illustrer par des exemples les concepts vus durant le cours
- Expliquer les résultats vus durant le cours ainsi que leurs preuves