Master 2

ALGÈBRE APPLIQUÉE

Enseignements donnés en français
Formation initiale

université PARIS-SACLAY | GRADUATE SCHOOL Mathématiques

Objectifs

+ Former des scientifiques en calcul formel, géométrie et cryptographie pour la recherche fondamentale et le développement dans l'industrie.

+ Préparer aussi bien à la recherche fondamentale qu'à la R&D dans l'industrie et les services

+ A l'issue de la formation, les étudiant.e.s sont capables de modéliser

algébriquement un problème concret, en estimer la complexité et utiliser des algorithmes récents pour procéder à sa résolution.

Les + de la formation :

+ La formation en cryptologie proposée dans le Master Algèbre Appliquée est une des rares formations complètes à la cryptologie en Ile-de-France, menant à la fois vers des débouchés académiques (thèse, puis enseignement-recherche) et des débouchés dans la recherche appliquée (dans des entreprises de haute technologie liées à la sécurité informatique).

+ Les étudiant.e.s disposent d'un parcours complet allant des aspects les plus théoriques (hypothèses calculatoires en théorie des nombres, preuves de sécurité, techniques de cryptanalyse) jusqu'aux problématiques les plus récentes d'implémentation optimisée ou sécurisée (algorithmique fine sur les corps finis, sur les courbes elliptiques, problématiques d'attaques physiques).

Compétences

+ Modéliser algébriquement un problème concret en estimer la complexité et utiliser des algorithmes récents pour procéder à sa résolution.

+ Maitriser et mettre en oeuvre des outils et méthodes mathématiques de haut niveau.

+ Analyser un document de recherche en vue de sa synthèse et de son exploitation.

+ Maitriser des outils numériques et langages de programmation de référence.

+ Concevoir et rédiger une preuve mathématique rigoureuse.

+ Expliquer clairement une théorie et des résultats mathématiques.

Débouché

Deux types de débouchés :

Poursuite en thèse, le plus souvent dans le laboratoire de recherche où le stage a été effectué.

En entreprise (industrie ou service) pour un emploi en R&D par exemple.

Admission

L'accès se fait après examen du dossier. Le nombre total de places est limité à 20 étudiant.e.s.

Le M2 Algèbre Appliquée s'adresse en particulier aux :

+ Etudiant.e.s du M1 Mathématiques et Interactions, site UVSQ, qui prépare spécifiquement au M2 Algèbre Appliquée.

+ Etudiant.e.s qui ont obtenu une première année de Master en mathématiques

+ Etudiant.e.s ayant une formation solide en algèbre (théorie de Galois, algèbre commutative, ensembles algébriques affines)et des notions d'informatique (complexité, notions de cryptographie, algorithmes de base).

Modalités de candidature

Période de candidature et liste des pièces à fournir :

Enseignements

Semestre 1

Cours de base

Algèbre effective

Courbes algébriques

Algorithmes avancés de la cryptographie, Cryptanalyse

Algorithmique et langage C, I

Semestre 2

Cours avancés

Courbes elliptiques

Complexité algébrique et cryptographie

Algorithmique et langage C, II

Séminaire étudiant

+ Stage ou mémoire

A partir du mois de mars, l'étudiant.e doit faire un stage dans une entreprise ou dans un laboratoire de recherche. Il ou elle aura alors à lire, comprendre et appliquer un ou plusieurs articles de recherche ou développement industriel. Ce stage comporte obligatoirement un mémoire et un projet de programmation, réalisés sous la responsabilité d'un.e enseignant.e-chercheur.euse associé.e au Master.

La soutenance a lieu au mois de septembre de l'année universitaire suivante.

université PARIS-SACLAY
GRADUATE SCHOOL
Mathématiques

Informations pratiques

Responsables pédagogiques

Pierre-Guy PLAMONDON - pierre-guy.plamondon@uvsq.fr

Secrétariat pédagogique

Jennifer PUCHEU – jennifer.pucheu-lashores@uvsq.fr

Adresse courrier

Université de Versailles Saint-Quentin-en-Yvelines
Bâtiment Fermat
45 avenue des États-Unis
78035 Versailles cedex

Lieux de formation

VERSAILLES

université PARIS-SACLAY

Novembre 2024 - Photo Istock - COMPAS - Université Paris-Saclay