

Informations pratiques

Responsables pédagogiques

Pour le M1
Balthazar Bauer - balthazar.bauer2@uvsq.fr

Pour le M2
Pierre-Guy PLAMONDON - pierre-guy.plamondon@uvsq.fr

Secrétariat pédagogique

scolarite.sciences.master@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



Master M1 +M2

ALGÈBRE APPLIQUÉE ET CRYPTOLOGIE

Enseignements donnés en français
Formation initiale

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-es 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 et Cryptologie 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-es 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 algorithmique 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.
- + Expliquer clairement une théorie et des résultats mathématiques.
- + Se familiariser avec les principales méthodes cryptographiques modernes concernant la confidentialité et l'authentification des données.

Débouchés

- 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 18 étudiant-es pour le M1 et 20 étudiant-es pour le M2. Une admission directement en M2 (sans avoir suivi le M1 Algèbre Appliquée et Cryptologie au préalable) est possible.
- Le M1 et M2 Algèbre Appliquée et Cryptologie s'adressent en particulier aux :
- + Etudiant-es 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).
 - + Etudiant-es ayant obtenu une L3 de Mathématiques ou LDD3 Math-Informatique ou LDD3 Math-Physique, puis une première année de master en mathématiques.

Modalités de candidature

Période de candidature et liste des pièces à fournir :

Pour le M1



Pour le M2



Présentation de la formation en vidéo



Enseignements

Master 1

Semestre 1
Algèbre générale
Théorie des nombres et cryptographie
Cryptographie
Introduction au calcul formel
Probabilités
Anglais
Semestre 2
Algèbre commutative
Introduction aux courbes elliptiques
Calcul sécurisé
Analyse d'algorithmes, programmation
Introduction au calcul scientifique et modélisation
Théorie de l'information

Master 2

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/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.