# MASTER 2 ALGÈBRE APPLIQUÉE ET CRYPTOLOGIE (AAC)

**DOMAINE(S) :**
**SCIENCE - TECHNOLOGIE - SANTÉ**

| | |
|---|---|
| **MENTION** | Mathématiques et applications (Université Paris-Saclay) |
| **DISCIPLINE(S)** | Mathématiques |
| **DURÉE DES ÉTUDES** | 1 an |
| **NIVEAU DE RECRUTEMENT** | Bac + 4 |
| **CRÉDITS ECTS** | 60 ECTS |
| **COMPOSANTE(S)** | UFR des sciences |
| **SITE(S) D'ENSEIGNEMENT** | Versailles |
| **FORMATION DIPLÔMANTE** | ✓ |
| **FORMATION INITIALE** | ✓ |
| **FORMATION CONTINUE** | ✓ |
| **LANGUE(S) D'ENSEIGNEMENT** | Français |

Le **Master 2 Algèbre Appliquée et Cryptologie** constitue la spécialisation avancée du parcours en algèbre moderne, géométrie algébrique, calcul formel, algorithmique, cryptologie, et leurs applications.
Il forme des étudiantes et étudiants capables de développer et d'utiliser des méthodes algébriques de pointe pour résoudre des problèmes concrets en cryptologie, sécurité informatique, modélisation ou recherche fondamentale.

**Le descriptif du master se trouve sur le site de l'Université Paris-Saclay.**

## Spécificités de la formation

**Organisation**

Le M2 AAC se déroule sur 1 année, en deux sessions de cours de 7 semaines, suivies d'un stage obligatoire de 6 mois en laboratoire ou en entreprise.

**Les enseignements couvrent :**
- algèbre effective ;
- algorithmique et langage C ;
- complexité algébrique ;

• cryptographie avancée ;
• courbes algébriques et elliptiques ;
• applications modernes en géométrie et sécurité.

## Compétences développées

**Au terme du Master 2 AAC, l'étudiante ou l'étudiant est capable de :**
• modéliser algébriquement un problème concret et en analyser la structure ;
• estimer la complexité et la faisabilité algorithmique des méthodes de résolution ;
• utiliser des algorithmes avancés issus du calcul formel et de la cryptologie ;
• maîtriser des techniques modernes en géométrie algébrique, courbes elliptiques, théorie de Galois ou algèbre commutative ;
• implémenter des algorithmes récents en environnement informatique (C, Sage, Magma, etc.) ;
• conduire un projet de recherche ou de développement en sécurité informatique, en mathématiques appliquées ou en modélisation ;
• intégrer un laboratoire ou un service R&D via un stage long permettant la poursuite en thèse ou l'insertion en entreprise.

## Attendus et compétences conseillées

**Les candidates et candidats doivent :**
• maîtriser les bases de l'algèbre avancée (théorie de Galois, algèbre commutative, arithmétique) ;
• comprendre les principes fondamentaux de la complexité algébrique et des méthodes de résolution algébriques ;
• posséder des notions en cryptologie ou en algorithmique appliquée ;
• être capables de suivre des preuves abstraites et rigoureuses ;
• manifester un intérêt pour la cryptographie, la sécurité informatique ou la recherche fondamentale ;
• faire preuve d'autonomie, d'analyse et de rigueur scientifique.

## Conditions d'admission

**L'admission se fait via :**
- la plateforme de candidature nationale **MON MASTER** (pour les candidats en France) ;
- ou via **plateforme de candidature Paris-Saclay : INCEPTION / Paris-Saclay** (pour candidats internationaux selon pays).

La sélection s'effectue sur dossier (relevés, CV, lettre de motivation, prérequis scientifiques, etc).

Toutes les informations actualisées sont disponibles sur le site d'admission de l'Université Paris-Saclay.

**FAQ** : Ici

**Niveau de recrutement :** Bac + 4

## Formation(s) requise(s)

Master 1 Algèbre Appliquée et Cryptologie (AAC)

**ou aux étudiantes et étudiants titulaires :**

- d'un M1 de Mathématiques,
- ou d'un Master 1 Mathématiques et Applications ;
- ou d'un M1 Algèbre Appliquée et Cryptologie ou équivalent ;
- ou d'une formation équivalente en France ou à l'étranger.

Une solide formation préalable en **algèbre, géométrie, arithmétique, complexité et cryptologie** est recommandée.

## Inscription

**Inscription administrative et pédagogique**

- Les candidats admis reçoivent un courriel indiquant la procédure d'inscription.
- Les inscriptions administratives puis pédagogiques sont effectuées à l'UVSQ.

## Inscription en formation continue

**Pour les reprises d'études** :
Public concerné : salariés, agents publics, travailleurs indépendants, demandeurs d'emploi, contrat de professionnalisation.

- Si vous ne répondez pas aux Conditions d'Admission définies dans la fiche en ligne sur le site de l'Université Paris-Saclay :
Téléchargez le complément de dossier VAPP

- Dans tous les cas :
1. Candidatez en ligne sur le site de l'Université Paris-Saclay
2. Téléchargez la fiche de liaison et retournez-la par e-mail au format PDF au contact "reprise d'études"

- Tarif et financements

- Dispositif d'accompagnement à la reprise d'études

- Obtenir ce diplôme par la Validation des Acquis de l'Expériencehttps://www.universite-paris-saclay.fr/formation/formation-continue-validation-des-acquis

## Contenu de la formation

Le M2 comporte 60 ECTS, répartis en :

**Enseignements (S1 – 7 semaines + S2 – 7 semaines)**

- Algèbre effective
- Algorithmique – langage C
- Complexité algébrique et cryptographie
- Courbes algébriques
- Courbes elliptiques

- Algorithmes avancés de la cryptographie

**Stage obligatoire (21 ECTS)**
Durée : 6 mois
Lieu : laboratoire de mathématiques / informatique, organisme public, entreprise de sécurité ou R&D.

## Contrôle de connaissances

Examens ou projets, selon les UE.
Soutenance de stage en fin d'année.

## Perspectives professionnelles

Le M2 AAC ouvre sur des métiers scientifiques à haut niveau :

- Cryptographe / cryptanalyste
- Ingénieur·e R&D en sécurité informatique
- Ingénieur·e en calcul formel
- Analyste en sécurité
- Développeur·euse bas niveau / systèmes sécurisés
- Ingénieur·e en méthodes formelles
- Chercheur·euse / Enseignant·e-chercheur·euse
- Ingénieur·e d'étude (industrie, défense, télécom, banque)

Exemples d'entreprises ou organismes associés : Thales, Orange Cyberdéfense, IDEMIA, CryptoExperts, INIA, CEA, Airbus, Dassault Systèmes…

## Poursuites d'études à l'UVSQ

- Doctorat (algèbre, géométrie, cryptologie, calcul formel, sécurité informatique)
- Thèse en partenariat industriel (CIFRE)
- Préparation de concours (agrégation …)

Les étudiantes et étudiants bénéficient de nombreux partenariats académiques (CEA, École polytechnique, ENS Ulm, IRMAR, INRIA, LORIA, UPMC, etc.).

Ils et elles peuvent s'orienter vers une thèse universitaire, éventuellement en partenariat avec l'industrie, puis vers un poste de Maître ou Maîtresse de conférences à l'université, de Chargé ou Chargée de recherche au CNRS ou à l'INRIA, etc.

En dix ans, 32 étudiantes et étudiants du Master 2 «Algèbre Appliquée et Cryptologie» ont poursuivi par une thèse, dont 24 en cryptographie.

## Responsables pédagogiques

» M. PIERRE-GUY PLAMONDON

## Adresses et coordonnées

UFR de Sciences - Département de Mathématiques de Versailles
45 avenue des Etats-Unis
78035 Versailles Cedex

**Département de Mathématiques de Versailles (DMV)**
Assistante du DMV : 01 39 25 46 46
Email : contact-dmv@sympa.uvsq.fr

**Responsable du M2 AAC**
Pierre-Guy PLAMONDON
PR

## Contacts administratifs

**Service de scolarité de l'UFR des sciences :**

- **Gestionnaire de scolarité :** Samia BOUBEKEUR - Tél. : 01 39 25 40 09 – samia.boubekeur@uvsq.fr
- **Responsable du pôle master :** Isabel LUBATTI - Tél. : 01 39 25 40 97 - isabel.lubatti@uvsq.fr

## Contacts formation continue

**Reprise d'études - Formation Continue**
Tél. : 01 39 25 46 40
contact.fc@uvsq.fr