MASTER 1 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 + 3
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 1 Algèbre Appliquée et Cryptologie** constitue la première année d'un parcours dédié à l'algèbre moderne, à la géométrie algébrique et à la cryptologie.

Il offre un socle **algèbre avancée, arithmétique, cryptographie, calcul formel et programmation,** permettant aux étudiants d'aborder les enjeux théoriques de l'algèbre appliqué en particulier de ceux concernant la cryptologie.

Ce M1 prépare naturellement à la poursuite en Master 2 Algèbre Appliquée et Cryptologie de l'UVSQ, puis éventuellement à un doctorat ou à une insertion en recherche et développement.

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

Spécificités de la formation

Le volume d'enseignement est constitué de cours magistraux (CM), travaux dirigés (TD) et séances pratiques, auxquels s'ajoute un travail personnel important.

Le programme détaillé (UE, volumes horaires, enseignants, mutualisations) est disponible dans :

- la présentation PDF du master sur le site du DMV : https://www.mathematiques.uvsq.fr/master-1-aa
- le site Paris-Saclay du M1 AA

Compétences développées

Au terme du Master 1 AAC, l'étudiant est capable de :

- modéliser un problème concret à l'aide d'outils algébriques avancés ;
- analyser la complexité d'un algorithme et en comprendre les limites théoriques ;
- utiliser les principaux outils de l'algèbre moderne (groupes, anneaux, corps, modules, courbes algébriques, théorie de Galois…) ;
- comprendre les principes fondamentaux de la cryptographie moderne ;
- implémenter des algorithmes algébriques ou cryptographiques dans un environnement numérique ;
- s'intégrer dans un projet de recherche ou de R&D en sécurité informatique ou en mathématiques appliquées..

Attendus et compétences conseillées

- posséder une solide formation en mathématiques (niveau L3) ;
- maîtriser l'analyse, l'algèbre, les probabilités et l'analyse numérique de base ;
- être capables de suivre des preuves théoriques exigeantes ;
- avoir une appétence pour la modélisation, l'abstraction et les méthodes numériques ;
- pratiquer la programmation scientifique (Python, C, ou équivalent) ; Maîtriser des bases solides en algèbre (groupes, anneaux, corps, algèbre linéaire approfondie).
- faire preuve de capacité de raisonnement abstrait et de démonstration.
- apprécier les mathématiques théoriques et la modélisation rigoureuse.
- manifester un intérêt pour la cryptologie, la sécurité informatique ou la recherche fondamentale.
- faire preuve d'autonomie, de rigueur et d'implication dans leur travail.

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 plateforme de candidature sera à déterminer selon les choix, la situation et le pays du candidat.

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 + 3

Formation(s) requise(s)

Le M1 s’adresse aux étudiants titulaires :

- d’une licence de Mathématiques ;
- d’une licence de Mathématiques appliquées ;
- d’une Licence Mathématiques–Informatique ;
- d’une Licence Mathématiques–Physique ;
- d’une formation équivalente en France ou à l’étranger.

Une solide maîtrise des programmes d’analyse, de probabilités et d’algèbre linéaire est indispensable.

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

Contenu de la formation

Les étudiants suivront des cours approfondis en algèbre commutative, arithmétique, cryptographie et théorie algébrique des systèmes.

- Algèbre commutative (semestre 2, 6 ECTS)
- Algèbre générale (semestre 1, 6 ECTS)
- Analyse d’Algorithmes, Programmation (semestre 2, 5 ECTS)
- Anglais (semestre 1, 3 ECTS)
- Calcul sécurisé (semestre 2, 4 ECTS)
- Cryptographie (semestre 1, 6 ECTS)
- Introduction au calcul formel (semestre 1, 6 ECTS)
- Introduction au calcul scientifique et projet (semestre 2, 6 ECTS)
- Introduction aux courbes elliptiques (semestre 2, 6 ECTS)

- Probabilités (semestre 1, 3 ECTS)
- Théorie de l'information (semestre 2, 3 ECTS)
- Théorie des nombres (semestre 1, 6 ECTS)

Contrôle de connaissances

Contrôle continu et/ou examens terminaux selon les UE.
Stage évalué par rapport écrit et soutenance.

Perspectives professionnelles

Le parcours ouvre sur des métiers à forte valeur scientifique, dont :

- cryptologue / ingénieur en sécurité informatique ;
- ingénieur R&D en cryptographie ou systèmes sécurisés ;
- ingénieur en sécurité des architectures numériques ;
- ingénieur ou analyste en cryptanalyse ;
- mathématicien appliqué (industrie technologique, défense, cybersécurité) ;
- ingénieur algorithmicien ;
- chargé d'études ou consultant en sécurité des données.

Poursuites d'études à l'UVSQ

- Master 2 Algèbre Appliquée et Cryptologie (suite naturelle)
- Master 2 en cryptographie, sécurité informatique ou mathématiques appliquées
- Thèse en cryptologie, algèbre, géométrie ou sécurité informatique
- Préparation aux concours d'enseignement (agrégation, etc.)

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

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

En dix ans, 32 étudiant(es) du Master 2 «Algèbre Appliquée» ont poursuivi par une thèse, dont 24 en cryptographie.

Ils peuvent également s'orienter vers les métiers d'ingénieur(es) en Cryptographie ou Recherche & Développement dans une entreprise liée à la sécurité informatique (Accenture, Bull, Crédit Agricole, CryptoExperts, CS Group, IDEMIA, Ingenico, Orange, Sogeti, Thales, Viaccess-Orca, etc.)

Responsables pédagogiques

- M. BALTHAZAR BAUER

Adresses et coordonnées

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

Contacts Administratifs :
Bâtiment Fermat - bureau 1202
Email : scolarite.sciences.master@uvsq.fr

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

Responsable du M1 AAC
Balthazar BAUER

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