

Share



Email destinataire :

Vous devez renseigner un email valide

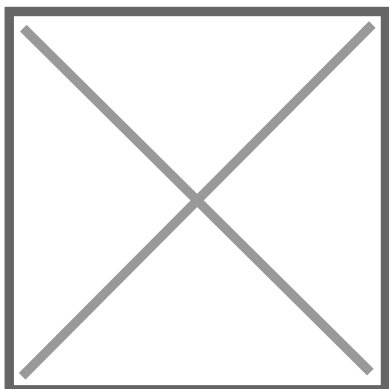
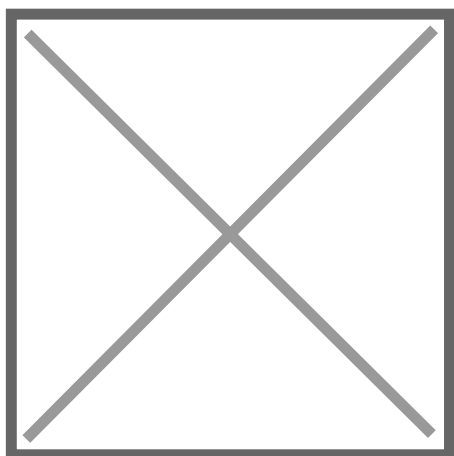
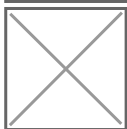
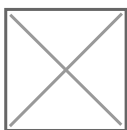
Envoyer

Une erreur est survenue. Merci de réessayer ultérieurement

Le mail de partage a bien été envoyé.

Add to Compare

M2 Algèbre Appliquée et Cryptologie



Master's degree

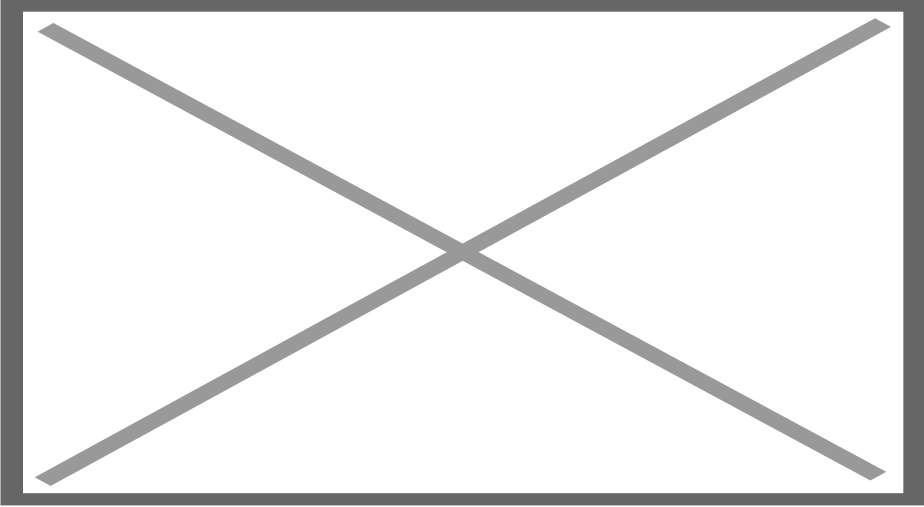
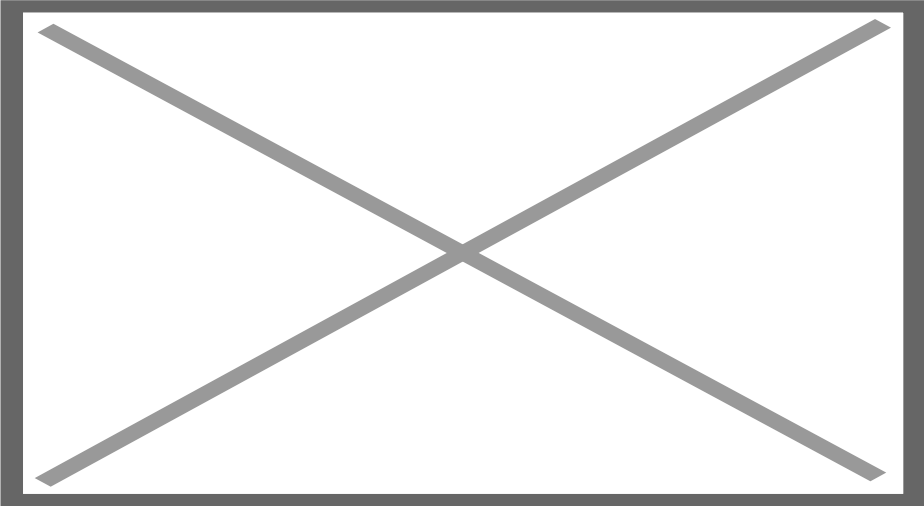
Specialisation Mathematics and applications

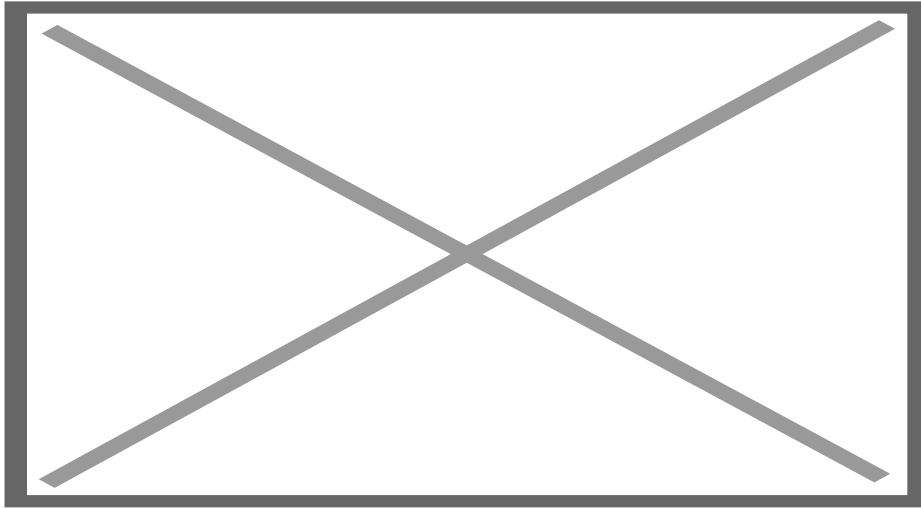
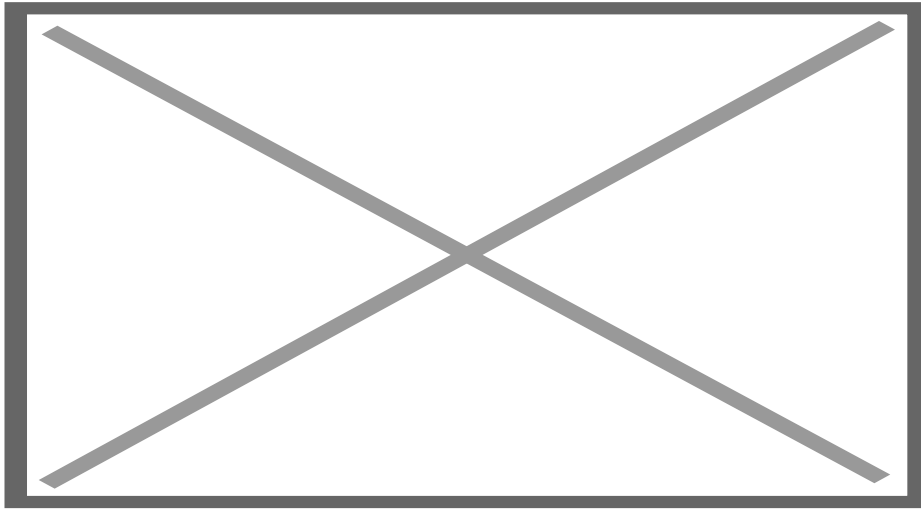
Language(s) of instruction

French

Le parcours Algèbre Appliquée et Cryptologie allie les mathématiques fondamentales, telles l'algèbre et la géométrie, aux applications à la cryptologie.

[Télécharger la fiche détaillée](#)
[Apply Now](#)





■ ■

Information

- [Overview](#)
- [Application requirements](#)
- [Schedule](#)

Présentation

Objectives

Les objectifs du parcours "Algèbre Appliquée et Cryptologie" sont d'acquérir une formation moderne et solide au calcul formel, à la géométrie et la cryptographie et de préparer aussi bien à la recherche fondamentale qu'à la recherche et au développement dans l'industrie et les services. A l'issue de la formation, les étudiants doivent être capable de modéliser algébriquement un problème concret en estimer la complexité et utiliser des algorithmes récents pour procéder à sa résolution.

Débouchés

Further Study Opportunities

R&D researcher or data modelling and analysis expert in leading-edge companies or laboratories.

PhD

PhD thesis

Calendar

Start of programme (indicative date)

06/09/2026

End of programme (indicative date)

30/09/2027

Admission

Admission Route

Mathematics

Capacity

Available Places

20

Target Audience and Entry Requirements

Les étudiants doivent avoir obtenu une première année de Master en mathématiques. Une formation solide en algèbre est particulièrement recommandée : théorie de Galois, algèbre commutative, ensembles algébriques affines. Il est préférable d'avoir quelques notions d'informatique : complexité, notions de cryptographie, algorithmes de base. Voir le programme du M1 Mathématiques et interactions, Site UVSQ qui prépare spécifiquement au M2 Algèbre Appliquée.

Période(s) de candidature

Inception Platform

From 01/04/2026 to 30/06/2026

Supporting documents

Compulsory supporting documents

Motivation letter.

All transcripts of the years / semesters validated since the high school diploma at the date of application.

Certificate of French (compulsory for non-French speakers).

Curriculum Vitae.

Detailed description and hourly volume of courses taken since the beginning of the university program.

VAP file (obligatory for all persons requesting a valuation of the assets to enter the diploma).

Document indicating the list of local M2 choices available here : <https://urlz.fr/i3Lo>.

Additional supporting documents

Supporting documents :

- Residence permit stating the country of residence of the first country
- Or receipt of request stating the country of first asylum
- Or document from the UNHCR granting refugee status
- Or receipt of refugee status request delivered in France
- Or residence permit stating the refugee status delivered in France
- Or document stating subsidiary protection in France or abroad
- Or document stating temporary protection in France or abroad.

Programme

Partie théorique (Informatique)

Subjects	ECTS	Semester	Lecture	directed study	practical class	Lecture/directed study	Lecture/practical class	directed study/practical class	d
Algorithmique et Langage C	6	Semestre 1	21	21					

Algorithmique et Langage C

ECTS : 6

Semester: Semestre 1

Detail

Lecture: 21

Directed study: 21

Language(s) of instruction

Français

Remote teaching

non

Prerequisites

Bases d'algèbre, d'algorithmique et de programmation

Programme/contents

- Multiplication de matrices 32×32 dans $GF(2)$.
- Éléments de base de calcul dans $GF(p)$, avec les opérateurs C d'abord (limite à 16 puis 32 bits environ), avec la librairie GMP ensuite. Illustration sur RSA. Calcul de racines carrées.
- Calcul sur les polynômes à une et plusieurs variables.
- Algorithmes de Tri. Algorithmes de tri à base d'arbres équilibrés.
- Applications en cryptographie et théorie des nombres des algorithmes de tri. « Collisions généralisées » entre 4 listes.
- Courbes elliptiques. Comptage de points par pas de bébé – pas de géant.
- Compléments sur les courbes elliptiques : diviseurs, fonctions, couplage de Weil–Tate. Algorithmes pour les couplages. Applications cryptographiques : Diffie–Hellman tripartite, chiffrement basé sur l'identité, signatures courtes.
- Transformées de Fourier et applications. Multiplication de polynômes, recherche d'approximation linéaires.
- Problématique des accès en mémoire et des effets de cache. Application au crible d'Eratostène.
- Algèbre linéaire et calcul de base de Gröbner sur $GF(2)$.

Learning objectives

Le but de ce cours est l'apprentissage de

Subjects	ECTS	Semester	Lecture	directed study	practical class	Lecture/directed study	Lecture/practical class	directed study/practical class	d
Algorithmes avancés de la cryptographie, Cryptanalyse	6	Semestre 2	21	21					

Subjects	ECTS	Semester	Lecture	directed study	practical class	Lecture/directed study	Lecture/practical class	directed study/practical class	d
----------	------	----------	---------	----------------	-----------------	------------------------	-------------------------	--------------------------------	---

Algorithmes avancés de la cryptographie, Cryptanalyse

ECTS : 6

Semester: Semestre 2

Detail

Lecture: 21

Directed study: 21

Language(s) of instruction

Français

Remote teaching

non

Prerequisites

Bases en algèbre et en cryptographie.

Programme/contents

- Le RSA revisité : diverses attaques de protocoles RSA, les normes actuelles, programmation rapide du RSA.
- Les techniques de cryptanalyse à clé secrète : cryptanalyse différentielle, cryptanalyse linéaire, cryptanalyse multivariable (algébrique), autres techniques.
- Cartes à puce : présentation des cartes à puces, les attaques physiques (SPA, DPA, DFA, etc.) et contre-mesures, exemples de protocoles pour certaines applications (cartes bancaires, de téléphone, de sécurité sociale, de télévision, etc.).
- Courbes elliptiques et cryptographie : ECC (Elliptic Curve Cryptography).
- La recherche actuelle en cryptographie : les grandes conférences annuelles, les revues et les ouvrages de recherche, les principaux articles récents.

Learning objectives

L'objectif est ici d'une part de donner aux étudiants une réelle expertise sur les grands algorithmes cryptographiques (la façon de les générer, et de les utiliser pour des applications réelles de l'industrie), et d'autre part d'introduire les principaux axes de recherche en cryptographie actuellement. On met ainsi l'accent sur les diverses techniques modernes de cryptanalyse, sur les contre-mesures de sécurité, sur les techniques de programmation efficaces des algorithmes, et sur divers problèmes ouverts.

Subjects	ECTS	Semester	Lecture	directed study	practical class	Lecture/directed study	Lecture/practical class	directed study/practical class	d
Complexité algébrique et cryptographie	6	Semestre 1	21	21					

Subjects	ECTS	Semester	Lecture	directed study	practical class	Lecture/directed study	Lecture/practical class	directed study/practical class	d
----------	------	----------	---------	----------------	-----------------	------------------------	-------------------------	--------------------------------	---

■

Complexité algébrique et cryptographie

ECTS : 6

Semester: Semestre 1

Detail

Lecture: 21

Directed study: 21

Language(s) of instruction

Français

Remote teaching

non

Prerequisites

Bases d'algèbre et de cryptographie.

Programme/contents

À partir de résultats de théorie algorithmique des nombres, on étudiera la sécurité des algorithmes de chiffrement et de signature qui s'appuient sur la factorisation (RSA), le logarithme discret sur le groupe multiplicatif des entiers modulo p (ElGamal, Schnorr, DSA...), ou encore la réduction de réseaux (Merkle–Hellman, Chor–Rivest, NTRU...). Une autre partie du cours sera consacrée aux cryptosystèmes « multivariables », qui s'appuient sur le problème MQ de résolution des systèmes d'équations polynomiales quadratiques à plusieurs variables, sur la notion d'isomorphismes de polynômes (IP), et sur la détermination d'une combinaison linéaire de matrices ayant un petit rang (MinRank).

Learning objectives

L'objectif du cours est d'aborder les notions modernes de sécurité pour les algorithmes cryptographiques, en particulier dans le cas asymétrique.

Bibliography

Douglas Stinson, Cryptographie – Théorie et Pratique (Vuibert, 2003) Gilles Zemor : Cours de Cryptographie (Cassini, 2000) Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone, Handbook of Applied Cryptography (CRC Press, 1997) Oded Goldreich, Foundations of Cryptography – Volume I : Basic Tools (Cambridge University Press, 2001) Oded Goldreich, Foundations of Cryptography – Volume II : Modern Complexity Theory (Cambridge University Press, 2002)

Stage et séminaire

Subjects	ECTS	Semester	Lecture	directed study	practical class	Lecture/directed study	Lecture/practical class	directed study/practical class	distance learning
----------	------	----------	---------	----------------	-----------------	------------------------	-------------------------	--------------------------------	-------------------

[Stage](#) 21 Semestre 2



Stage

ECTS : 21

Semester: Semestre 2

Language(s) of instruction

Français

Remote teaching

non

Type of assessment

Evaluation Continue non Intégrale

[Séminaire étudiant](#) 3 Semestre 2



Séminaire étudiant

ECTS : 3

Semester: Semestre 2

Language(s) of instruction

Français

Remote teaching

non

Type of assessment

Evaluation Continue non Intégrale

Partie théorique (Mathématiques)

Subjects	ECTS	Semester	Lecture	directed study	practical class	Lecture/directed study	Lecture/practical class	directed study/practical class	distance learning
----------	------	----------	---------	----------------	-----------------	------------------------	-------------------------	--------------------------------	-------------------

[Courbes algébriques](#) 6 Semestre 1 21 21



Courbes algébriques

ECTS : 6
Semester: Semestre 1
Detail
Lecture: 21
Directed study: 21
Language(s) of instruction
Français
Remote teaching
non
Prerequisites

Algèbre commutative et Théorie de Galois.

Programme/contents

- Topologie de Zariski.
- Variétés projectives, courbes projectives planes.
- Corps de fonctions.
- Morphisme de variétés projectives.
- Diviseurs, diviseurs sur les courbes, degré.
- Groupe de Picard.
- Cas des courbes elliptiques

Bibliography

W. Fulton, Algebraic curves, Benjamin 1969.
R. Hartshorne, Algebraic Geometry, Springer 1977.
R.J. Walker, Algebraic curves, Princeton University Press

Type of assessment
Evaluation Continue non Intégrale

Courbes elliptiques	6	Semestre 1	21	21
-------------------------------------	---	------------	----	----



Courbes elliptiques

ECTS : 6
Semester: Semestre 1
Detail
Lecture: 21
Directed study: 21
Language(s) of instruction
Français
Remote teaching
non
Prerequisites

Algèbre commutative, théorie de Galois, courbes algébriques.

Programme/contents

- Courbes planes affines et projectives : propriétés locales, diviseurs.
- Courbes elliptiques : généralités, forme de Weierstraß, loi de groupe, couplage de Weil.
- Courbes elliptiques sur les corps finis
- Courbes elliptiques sur le corps des nombres rationnels
- Applications des courbes elliptiques

Learning objectives

Ce cours est consacré à l'étude des courbes elliptiques en vue de leurs utilisations en cryptographie

Bibliography

D. Perrin, Géométrie Algébrique, Une introduction, Savoirs Actuels, 1995. W. Fulton, Algebraic Curves, Benjamin, 1969. J. H.Silverman, The Arithmetic of Elliptic Curves, Springer, Graduate Texts in Math. 106, 1986.

Type of assessment
Evaluation Continue non Intégrale

Algèbre effective	6	Semestre 1	21	21
-----------------------------------	---	------------	----	----

Algèbre effective

ECTS : 6

Semester: Semestre 1

Detail

Lecture: 21

Directed study: 21

Language(s) of instruction

Français

Remote teaching

non

Prerequisites

Il est nécessaire d'avoir une bonne formation en algèbre commutative et théorie de Galois ainsi que des bases en calcul formel. Les étudiants travaillerons sur SAGE.

Programme/contents

- Bases de Gröbner, algorithme de Buchberger.
- Théorie de l'élimination.
- Résultants.
- Applications.

Bibliography

D. Cox, J. Little et D. O'Shea, Ideal, varieties and algorithms, Springer, 1997. D. Cox, J. Little et D. O'Shea, Using algebraic geometry, Springer, 1998. T. Becker et V. Weispfenning, Gröbner Bases : A Computational Approach to Commutative Algebra, Springer-Verlag, 1993. D. Eisenbud, Commutative Algebra with a View toward Algebraic Geometry, Springer-Verlag, 1995. Computations in algebraic geometry with Macaulay 2, édité par D. Eisenbud, D. R. Grayson, M. E. Stillman, and B. Sturmfels, Springer, 2001.

Type of assessment

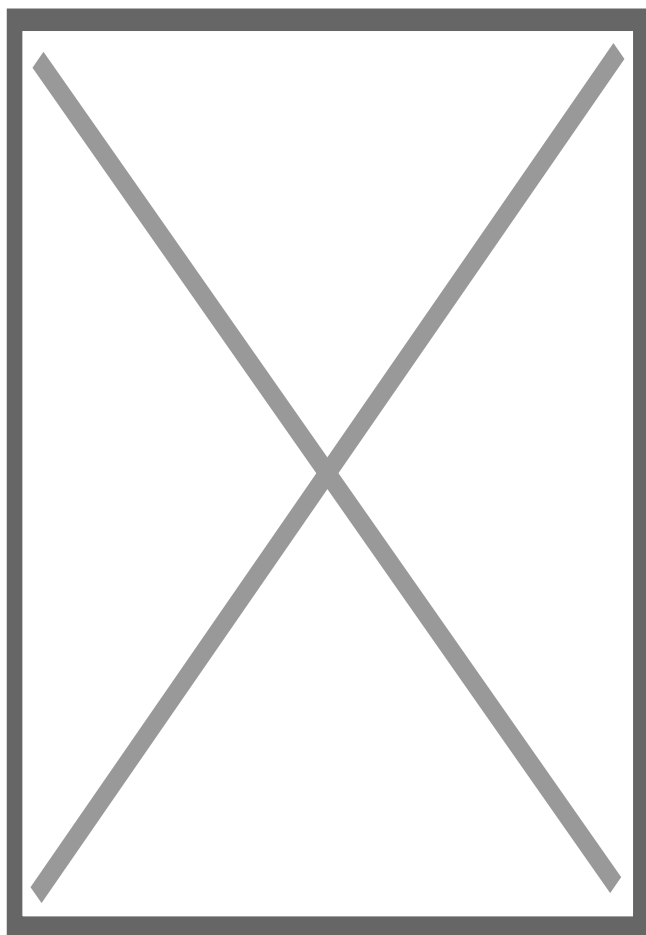
Evaluation Continue non Intégrale

Teaching Location(s)

VERSAILLES

Training campus

Javascript est requis pour visualiser cette carte.



Versailles

Versailles

Bus 8 - 10 - 13 - 105 - 108 - 471

Versailles Rive Droite - Ligne L

RER C Versailles Château Rive gauche

[Voir](#)

Student restaurant (CROUS)

Library

Student residence

Contact

- **Pierre-Guy PLAMONDON**

<http://www.universite-paris-saclay.fr/formation/master/mathematiques-et-applications/m2-algebre-appliquee-et-cryptologie>