

Partager



Email destinataire :

Vous devez renseigner un email valide

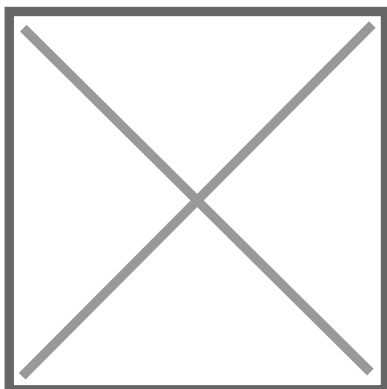
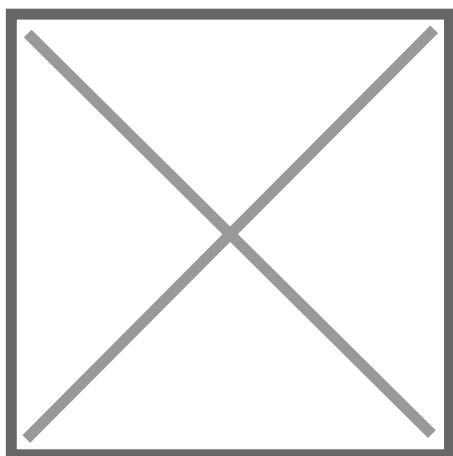
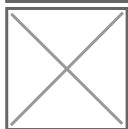
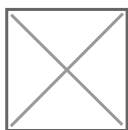
Envoyer

Une erreur est survenue. Merci de réessayer ultérieurement

Le mail de partage a bien été envoyé.

Ajouter au comparateur

M2 Algèbre Appliquée et Cryptologie



Master

Mention Mathématiques et applications

Régime(s) d'inscription

Formation initiale

Langue(s) d'enseignement

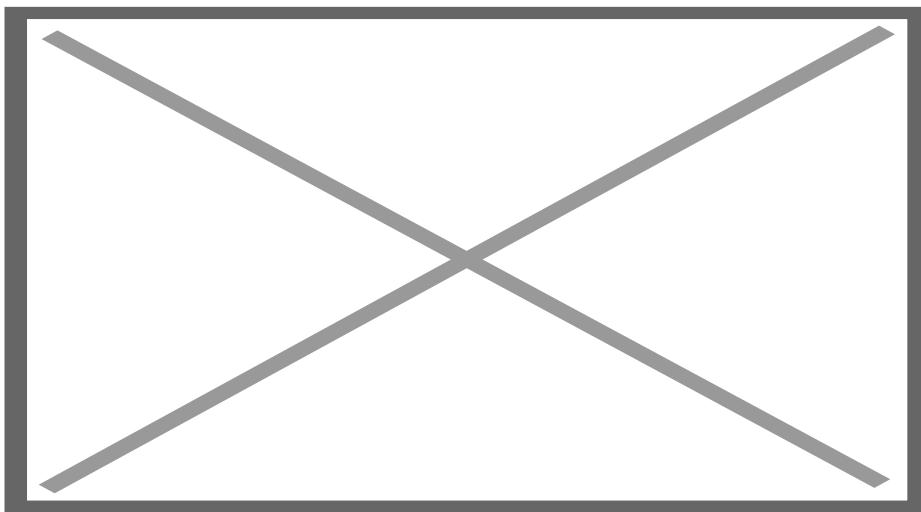
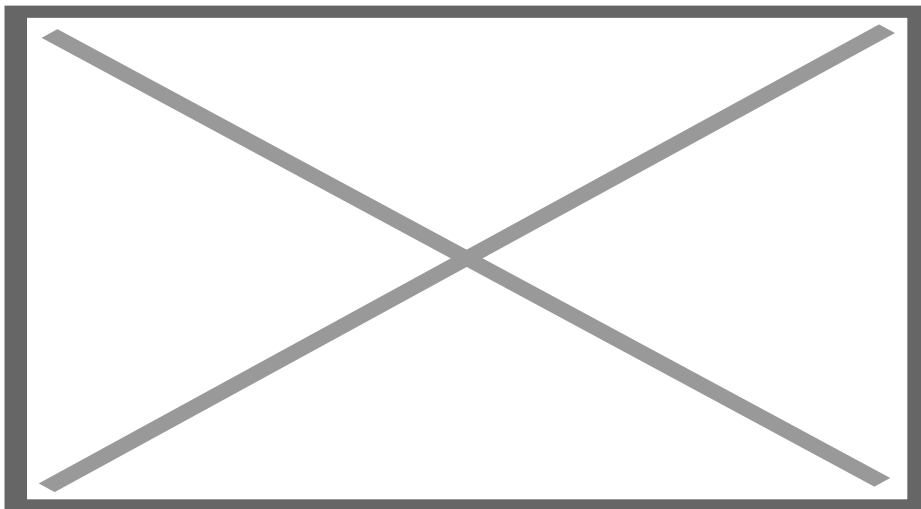
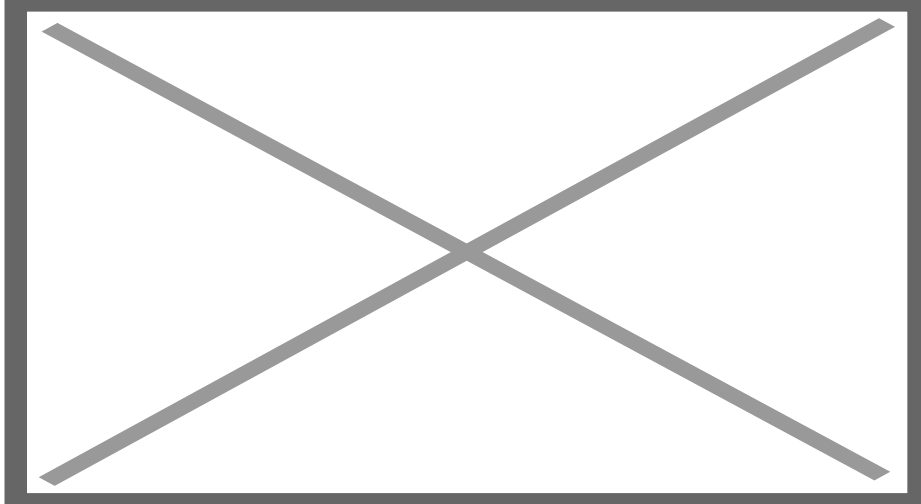
Français

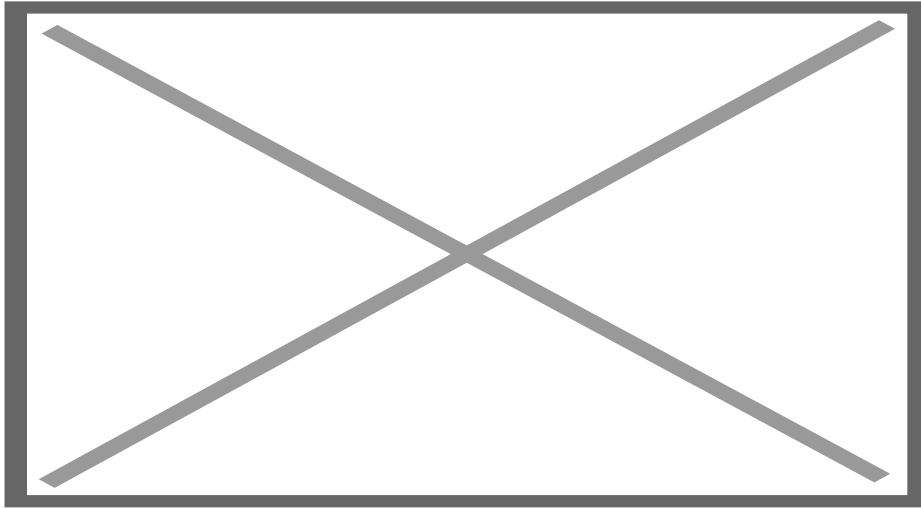
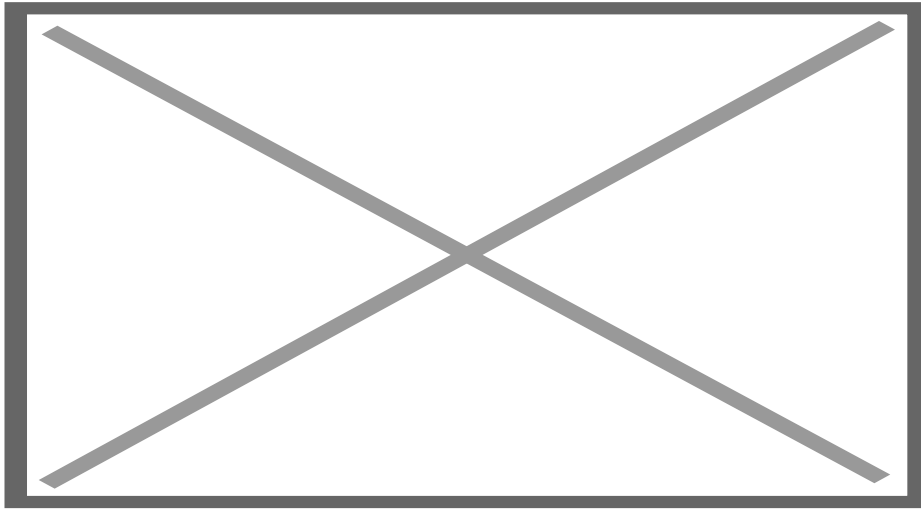
Le parcours Algèbre Appliquée et Cryptologie allie les mathématiques fondamentales, telles l'algèbre et la géométrie, aux applications à la cryptologie.

LeM2 se déroule en deux sessions de 7 semaines, suivies d'un stage de 6 mois.

[Télécharger la fiche détaillée](#)

[Je candidate](#)





■ ■

Informations

- [Présentation](#)
- [Admission](#)
- [Programme](#)

Présentation

Compétences

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

Objectifs pédagogiques de la formation

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. Pour plus d'informations, vous pouvez consulter le site web de cette formation M2 Algèbre appliquée.

Débouchés

Poursuite d'études

Chercheur/chercheuse en R&D ou expert·e en modélisation et analyse de données dans des entreprises ou laboratoires de pointe.

Doctorat

Thèse de doctorat

Agenda

Début de la formation (date indicative)

06/09/2026

Fin de la formation (date indicative)

30/09/2027

Admission

Voie d'accès

Mathématiques

Capacité d'accueil

Places

20

Public visé et prérequis

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

Plateforme Inception

Du 01/04/2026 au 30/06/2026

Pièces justificatives

Obligatoires

Lettre de motivation.

Tous les relevés de notes des années/semestres validés depuis le BAC à la date de la candidature.

Attestation de français (obligatoire pour les non francophones).

Curriculum Vitae.

Descriptif détaillé et volume horaire des enseignements suivis depuis le début du cursus universitaire.

Dossier VAPP (obligatoire pour toutes les personnes demandant une validation des acquis pour accéder à la formation) <https://www.universite-paris-saclay.fr/formation/formation-continue/validation-des-acquis-de-lexperience>.

Fiche de choix de M2 (obligatoire pour les candidats inscrits en M1 à l'Université Paris-Saclay) à télécharger sur <https://urlz.fr/i3Lo>.

Facultatives

Document justificatif des candidats exilés ayant un statut de réfugié, protection subsidiaire ou protection temporaire en France ou à l'étranger (facultatif mais recommandé, un seul document à fournir) :

- Carte de séjour mention réfugié du pays du premier asile
- OU récépissé mention réfugié du pays du premier asile
- OU document du Haut Commissariat des Nations unies pour les réfugiés reconnaissant le statut de réfugié
- OU récépissé mention réfugié délivré en France
- OU carte de séjour avec mention réfugié délivré en France
- OU document faisant état du statut de bénéficiaire de la protection subsidiaire en France ou à l'étranger.

Programme

Partie théorique (Informatique)

Matières	ECTS	Semestre	Cours	TD	TP	Cours- TD	Cours- TP	TD- TP	A distance	Projet	Tutorat
<u>Algorithmique et Langage C</u>	6	Semestre 1	21	21							

Algorithmique et Langage C

ECTS : 6

Semestre calendaire : Semestre 1

Détail du volume horaire

Cours magistraux : 21

Travaux dirigés : 21

Langue d'enseignement

Français

Enseignement à distance

non

Prérequis

Bases d'algèbre, d'algorithmique et de programmation

Programme / plan / contenus

- Multiplication de matrices 32×32 dans $GF(2)$.
- Eléments 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 $GF(2)$.

Objectifs d'apprentissage

Le but de ce cours est l'apprentissage de techniques algorithmiques visant à programmer efficacement, ainsi que du langage C, afin d'illustrer ces techniques. Un aperçu des outils d'analyse et de débogage gprof et gdb, ainsi que de la librairie de grands nombres GMP vient compléter ces objectifs. Chaque cours consiste en une étude approfondie d'un exemple, choisi en relation avec

Matières	ECTS	Semestre	Cours	TD	TP	Cours- TD	Cours- TP	TD- TP	A distance	Projet	Tutorat
<u>Algorithmes avancés de la cryptographie, Cryptanalyse</u>	6	Semestre 2	21	21							

Algorithmes avancés de la cryptographie, Cryptanalyse

ECTS : 6

Semestre calendaire : Semestre 2

Détail du volume horaire

Cours magistraux : 21

Travaux dirigés : 21

Langue d'enseignement

Français

Enseignement à distance

non

Prérequis

Bases en algèbre et en cryptographie.

Programme / plan / contenus

- 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.

Objectifs d'apprentissage

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.

Nature de l'évaluation

Evaluation Continue non Intégrale

Matières	ECTS	Semestre	Cours	TD	TP	Cours- TD	Cours- TP	TD- TP	A distance	Projet	Tutorat
<u>Complexité algébrique et cryptographie</u>	6	Semestre 1	21	21							

Complexité algébrique et cryptographie

ECTS : 6

Semestre calendaire : Semestre 1

Détail du volume horaire

Cours magistraux : 21

Travaux dirigés : 21

Langue d'enseignement

Français

Enseignement à distance

non

Prérequis

Bases d'algèbre et de cryptographie.

Programme / plan / contenus

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).

Objectifs d'apprentissage

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

Bibliographie

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 : Basic Applications (Cambridge University Press, 2004) Neal Koblitz, A Course in Number Theory and Cryptography (GTM 114, Springer, 1994) Neal Koblitz, Algebraic Aspects of Cryptography (Cambridge University Press, 1999) M. G. K. J.

Stage et séminaire

Matières	ECTS	Semestre	Cours	TD	TP	Cours-TD	Cours-TP	TD-TP	A distance	Projet	Tutorat
Stage	21	Semestre 2									

■

Stage

ECTS : 21

Semestre calendaire : Semestre 2

Langue d'enseignement

Français

Enseignement à distance

non

Nature de l'évaluation

Evaluation Continue non Intégrale

[Séminaire étudiant](#)

3

Semestre 2

■

Séminaire étudiant

ECTS : 3

Semestre calendaire : Semestre 2

Langue d'enseignement

Français

Enseignement à distance

non

Nature de l'évaluation

Evaluation Continue non Intégrale

Partie théorique (Mathématiques)

Matières	ECTS	Semestre	Cours	TD	TP	Cours-TD	Cours-TP	TD-TP	A distance	Projet	Tutorat
Courbes algébriques	6	Semestre 1	21	21							

Matières	ECTS	Semestre	Cours	TD	TP	Cours- TD	Cours- TP	TD- TP	A distance	Projet	Tutorat
■											

Courbes algébriques

ECTS : 6

Semestre calendaire : Semestre 1

Détail du volume horaire

Cours magistraux : 21

Travaux dirigés : 21

Langue d'enseignement

Français

Enseignement à distance

non

Prérequis

Algèbre commutative et Théorie de Galois.

Programme / plan / contenus

- 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

Bibliographie

W. Fulton, Algebraic curves, Benjamin 1969. R.

Hartshorne, Algebraic Geometry, Springer 1977. R.J.

Walker, Algebraic curves, Princeton University Press

Nature de l'évaluation

Evaluation Continue non Intégrale

[Courbes
elliptiques](#)

6

Semestre 1

21

21

Matières	ECTS	Semestre	Cours	TD	TP	Cours- TD	Cours- TP	TD- TP	A distance	Projet	Tutorat
■											

Courbes elliptiques

ECTS : 6

Semestre calendaire : Semestre 1

Détail du volume horaire

Cours magistraux : 21

Travaux dirigés : 21

Langue d'enseignement

Français

Enseignement à distance

non

Prérequis

Algèbre commutative, théorie de Galois, courbes algébriques.

Programme / plan / contenus

- 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

Objectifs d'apprentissage

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

Bibliographie

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.

Nature de l'évaluation

Evaluation Continue non Intégrale

[Algèbre effective](#)

6

Semestre 1

21

21

Matières	ECTS	Semestre	Cours	TD	TP	Cours- TD	Cours- TP	TD- TP	A distance	Projet	Tutorat
■											

Algèbre effective

ECTS : 6

Semestre calendaire : Semestre 1

Détail du volume horaire

Cours magistraux : 21

Travaux dirigés : 21

Langue d'enseignement

Français

Enseignement à distance

non

Prérequis

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 / plan / contenus

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

Bibliographie

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.

Nature de l'évaluation

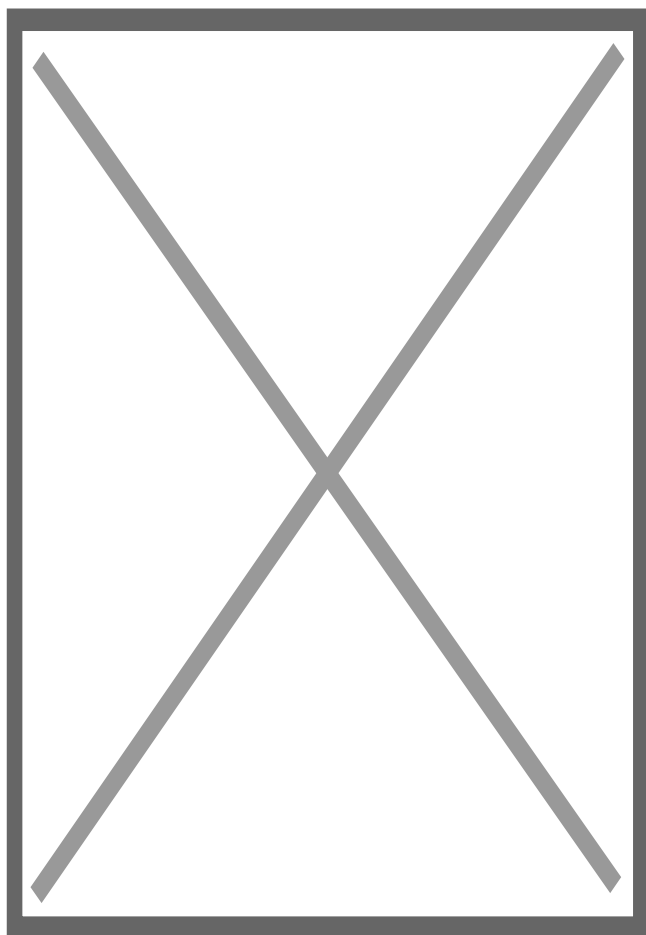
Evaluation Continue non Intégrale

Lieu(x) d'enseignement

VERSAILLES

Campus de la formation

Javascript est requis pour visualiser cette carte.



Versailles

Versailles

Bus 471, 5371, 6179, 6201, 6203, 6204, 6205, 6217

Versailles Rive Droite - Ligne L

RER C Versailles Château Rive gauche

[Voir](#)

Restaurant CROUS

Bibliothèque

Résidence étudiante

Contact(s)

- **Pierre-Guy PLAMONDON**

Liens

[Vidéo de présentation](#)

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