Université Paris-Saclay

Université de Versailles Saint-Quentin-en-Yvelines

Master 1 Algébre Appliquée
Site UVSQ

Présentation et Syllabus [1]

1. Les informations contenues dans le présent document sont susceptibles d'évoluer légèrement.

Contacts

Enseignant responsable du Master 1 Algèbre Appliquée

Ana-Maria Castravet
Mél : ana-maria.castravet@uvsq.fr

Secrétariat du département de mathématiques

Mme Sandrine Pyrrhé
Bâtiment Fermat, 45 avenue des États-Unis,
78035 Versailles Cedex.
Mél : sandrine.pyrrhe@uvsq.fr

Scolarité

Bureau des Masters
Mme Jennifer Pucheu-Lashores
Bâtiment Fermat, 45 avenue des États-Unis,
78035 Versailles Cedex.
Mél : jennifer.pucheu-lashores@uvsq.fr

Le Master Algébre Appliquée

Le Master (M1 et M2) «Algébre Appliquée» proposé par l'Université de Versailles Saint-Quentin fait partie du Master «Mathématiques et Applications» de l'Université Paris-Saclay.

Le Master est destiné aux étudiant.es désirant acquérir une formation solide et moderne en calcul formel, algèbre et cryptographie pour la recherche fondamentale et le développement dans l'industrie. À l'issue de cette formation, les étudiant.es maîtriseront des techniques d'algèbre moderne sur les plans théorique et pratique. Ils.elles seront capables de modéliser algébriquement un problème concret, d'estimer la difficulté à résoudre ce problème, et enfin d'utiliser et adapter des algorithmes récents rapides pour procéder à sa résolution.

Le Master Algébre Appliquée ouvre à des débouchés académiques et privés : thèse dans un organisme public (universités, INRIA, etc.) ou en collaboration avec une entreprise privée, recherche en mathématiques fondamentales ou appliquées à la théorie du contrôle, à la cryptographie et à la sécurité informatique dans les milieux académique ou privé (Accenture, Dictao, Gemalto, Oberthur, Orange, etc.). Les étudiants pourront également s'orienter vers l'informatique théorique et les métiers d'ingénieurs dans le domaine des mathématiques appliquées à l'informatique (cryptologie, robotique).

Cours M1 Algébre Appliquée

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)

Programme des cours

du Master 1 Algébre Appliquée

Semestre 1

Algèbre générale

Code UE: MYMAA001
Tutelle: Département de Mathématiques, UVSQ
Volume horaire: CM: 24h TD: 24h
ECTS: 6
Semestre: 1
Intervenants: Vincent Sécherre
Lieu: UVSQ
Parcours: «Algèbre appliquée»

Pré-requis: Algèbre de licence (anneaux, idéaux, groupes)

Description

La théorie de Galois, développée par le mathématicien français Evariste Galois (1811-1832), établit le lien entre deux familles d'objets algébriques : les groupes et les corps. Dans ce cours nous allons étudier des différents types d'extensions de corps (finies, algébriques, séparables, normales, galoisiennes) et leurs groupes d'automorphismes afin d'arriver à démontrer le théorème fondamental de la théorie de Galois qui établit le lien mentionné ci-dessus.

Contenu

- extensions de corps : finies, algébriques, séparables, normales, galoisiennes
- morphismes d'extensions
- groupes de Galois
- théorème fondamental de la théorie de Galois

Bibliographie

- Calais J., Extensions de corps, théorie de Galois, Ellipses, 2006.
- Chambert-Loir A., Algèbre corporelle, disponible à l'adresse : `http://www.math.polytechnique.fr/ chambert/`
- Escofier J.-P., Théorie de Galois, Dunod, 2000.
- Gozard I., Théorie de Galois, Ellipses, 1997.
- Morandi P., Field and Galois theory, GTM 167, Springer, 1996.
- Tauvel P., Corps commutatifs et théorie de Galois, Calvage et Mounet, 2008.

Anglais

Code UE: MSANGS1
Tutelle: Institut d'Etudes Culturelles et Internationales
Volume horaire: CM: 0h TD: 27h
ECTS: 3
Semestre: 1
Intervenants: Lionel Thevenard
Lieu: UVSQ

Parcours : Algèbre Appliquée, Analyse, Modélisation, Simulation, Mathématiques et apprentissage statistique.

Pré-requis:

- Etre capable de comprendre à l'oral comme à l'écrit des supports d'anglais général et scientifique.
- Etre capable de faire des présentations orales et écrites sur des sujets d'actualité divers.
- Avoir d'importantes notions en grammaire anglaise.

Description

Dans un contexte à caractère professionnel, les cours en anglais Master visent à aider les étudiants à faire face aux exigences du monde du travail.

Contenu

- Job Interview
- Debating
- CV - Cover letter - Essay writing
- Listening Comprehension
- TOEIC training

Cryptographie

Code UE: MIN15123
Tutelle: Département d'Informatique et Département de Mathématiques, UVSQ
Volume horaire: CM: 15h TD: 30h
ECTS: 6
Semestre: 1
Intervenants: Louis Goubin
Lieu: UVSQ
Parcours: «Algèbre appliquée», Informatique

Pré-requis: Algèbre et algébre linéaire de licence : arithmétique modulaire, calculs dans les corps finis. Rudiments de théorie des probabilités et de statistiques. Connaissances de base en algorithmique.

Description

Le but est de présenter un panorama des principaux algorithmes utilisés en chiffrement, authentification et signature électronique, ainsi que leur utilisation pour sécuriser les communications numériques.
A l'issue de ce cours, les étudiants devront pouvoir :

- utiliser l'arithmétique modulaire et les opérations de base sur les corps finis liées aux techniques cryptographiques
- décrire les concepts et algorithmes cryptographiques de base, incluant le chiffrement/déchiffrement, les fonctions de hachage et la cryptographie à clé publique
- évaluer la sécurité de primitives cryptographiques
- concevoir et analyser des protocoles pour des objectifs de sécurité variés

Contenu

- Cryptographie à clé secrète, Cryptographie à clé publique
- Attaques brutales, attaques par rejeu
- Attaques à chiffré seul, attaques à clair choisi, attaques à clair et chiffré choisis
- Attaques interactives et non interactives
- Chiffrement par flot, chiffrement par blocs
- Transposition et substitution, schémas de Feistel
- DES, AES
- Fonctions à sens unique, fonctions de hachage
- Algorithmes d'échange de clés
- RSA, Algorithmes zero-knowledge
- Applications

Bibliographie

- N. Koblitz, *A Course in Number Theory and Cryptography*, GTM 114, Springer, 1994.

— A.J. Menezes, P.C. van Oorschot, S.A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1997.
— D. Stinson, *Cryptography : Theory and Practice*, Third Edition (Discrete Mathematics and Its Applications), CRC Press, 2005.
— S. Vaudenay, *A Classical Introduction to Cryptography : Applications for Communications Security*, Springer, 2005.

Introduction au calcul formel

Code UE: MYMAA002
Tutelle: Département de Mathématiques, UVSQ
Volume horaire: CM: 20h TD: 20h
ECTS: 6
Semestre: 1
Intervenants: Guillermo Moreno-Socias (CM), Pierre-Guy Plamondon (TP)
Lieu: UVSQ
Parcours: «Algèbre appliquée»,«Analyse, Modélisation et Simulation»

Pré-requis: algèbre et analyse de licence, bases d'algorithmique

Description

Ce cours est une initiation au Calcul formel (Computer Algebra en anglais). Celui-ci s'intéresse aux méthodes qui permettent de trouver des résultats de façon :

— Exacte (par opposition au Calcul numérique).
— Effective (par opposition aux théorèmes purement existentiels).
— Efficace (par opposition aux calculs dont la faisabilité est purement théorique).

L'outil de base est donc l'algorithme, dont on verra divers types. La question de l'efficacité donnera lieu à des analyses de complexité. Une partie non négligeable du cours se passera devant des ordinateurs, et sera consacrée à implémenter des algorithmes vus en cours en s'appuyant sur des logiciels de calcul formel tels que Sage.

Contenu

- Éléments de complexité
- Arithmétique des grands entiers : représentation, addition, multiplication, division euclidienne, algorithme d'Euclide. Étude d'algorithmes et de leur complexité. Algorithme de Karatsuba pour la multiplication.
- Arithmétique modulaire : calcul de l'inverse, théorème chinois.
- Polynômes : représentations, algorithmes d'addition, de multiplication, de division euclidienne et algorithme d'Euclides. Améliorations.
- Algèbre linéaire : complexité du calcul du produit matriciel, de l'inverse, du rang et du déterminant.
- Factorisation de polynômes sur un corps fini.
- Transformée de Fourier rapide et applications.

Bibliographie

— Tutoriel Sage, https ://doc.sagemath.org/html/fr/tutorial/index.html
— Michel Demazure, Cours d'algèbre : Primalité. Divisibilité. Codes. Nouvelle Bibliothèque Mathématique, 1. Cassini, Paris, 1997. xviii+302 pp.

— Donald E. Knuth, The art of computer programming, Volume 2 : Seminumerical Algorithms, Second edition, Addison-Wesley, Reading (MA), 1981, ix+689pp.
— V. Shoup, A Computational Introduction to Number Theory and Algebra, 2nd Edition, Cambridge University Press (2008).
— J. Von zur Gathen & J. Gerhard, Modern Computer Algebra, 3rd Edition, Cambridge University Press (2013).

Probabilités

Code UE: MYMAA003
Tutelle: Département de Mathématiques, UVSQ
Volume horaire: CM: 18h TD: 12h
ECTS: 3
Semestre: 1
Intervenants: Catherine Donati-Martin
Lieu: UVSQ

Parcours : Algèbre Appliquée, Analyse, Modélisation, Simulation, Mathématiques et apprentissage statistique.

Pré-requis: Calcul intégral et Théorie de la mesure ; Probabilités

Description

Le module est consacré principalement à l'étude des chaînes de Markov à espace d'états discret, avec des applications aux marches aléatoires et à des processus à valeurs dans un espace d'états discret. Dans le cadre de cette étude, nous approfondirons les notions d'espérance conditionnelle et de loi conditionnelle. Le cours se terminera par des théorèmes limites incluant des rappels sur les différents modes de convergence possibles dans le domaine des probabilités.

Contenu

- Espaces de probabilités, variables aléatoires, indépendance
- Conditionnement, Espérance conditionnelle.
- Chaînes de Markov discètes, marches aléatoires discrètes
- Convergences des variables aléatoires
- Théorèmes limites pour les chaînes de Markov discètes,

Bibliographie

- J.F. Le Gall. Cours Fimfa. Intégration, probabilités et processus aléatoires. https://www.math.u-psud.fr/ jflegall/IPPA2.pdf
- P. Barbe et M. Ledoux, *Probabilité*, Belin, 1998.
- B. Bercu et D. Chafai, *Modélisation stochastique et simulation. Cours et applications*, Dunod, 2007.
- R. Durrett, *Probability : Theory and Examples*, Duxbury, 2005.
- D. Foata et A. Fuchs : *Calcul des Probabilités : Cours, exercices et problémes corrigés*, Dunod, 2003.
- Olivier Garet, Aline Kurtzmann, *De l'intégration aux probabilités*, Ellipses, 2011.
- P. Baldi, L. Mazliak et P. Priouret *Martingales et Chaînes de Markov*. Hermann, collection Méthodes, 1998.

Théorie des nombres

Code UE: MYMAA004
Tutelle: Département de Mathématiques, UVSQ
Volume horaire: CM: 24h TD: 24h
ECTS: 6
Semestre: 1
Intervenants: Guillermo Moreno-Socias (TD)
Lieu: UVSQ
Parcours: «Algèbre appliquée»

Pré-requis: Algèbre de Licence (groupes, anneaux, corps, polynômes et congruences)

Description

L'objectif de ce cours est de mettre en évidence la façon dont des propriétés algébriques (notamment les structures de groupe et d'anneau) peuvent servir à prouver des résultats arithmétiques, avec des applications à la cryptographie. Au début du cours, on rappelle brièvement les notions de théorie des groupes et des anneaux qui seront nécessaires dans la suite. On étudie notamment l'anneau des entiers relatifs et les anneaux de polynômes en une indéterminée à coefficients dans un corps, en insistant sur leurs propriétés algébriques communes. On étudie ensuite les propriétés arithmétiques des anneaux de congruence $\mathbb{Z}/n\mathbb{Z}$ et des corps finis, y compris la loi de réciprocité quadratique de Gauss, et on en déduit plusieurs tests de primalité. On introduit ensuite diverses propriétés de structure (anneaux euclidiens, principaux, factoriels, intégralement clos, etc.) et leurs conséquences en arithmétique (notamment le théorème des deux carrés). On introduit enfin la notion d'entier quadratique et on démontre le théorème des unités, qui permet de résoudre l'équation de Pell $x^2+dy^2=1$.

Contenu

- Groupes et anneaux
- Entiers et polynômes en une indéterminée
- Congruences modulo un entier
- Corps finis
- Les entiers de Gauss et le théorème des deux carrés
- Anneaux euclidiens, principaux, factoriels
- Le théorème des unités et l'équation de Pell

Bibliographie

- M. Demazure, *Cours d'algèbre*, Cassini, 1997.
- M. Hindry, *Arithmétique*, Calvage et Mounet, 2008.
- K. Ireland et M. Rosen, *A classical introduction to modern number theory*, Graduate texts in mathematics **84**, Springer, 1990.
- D. Perrin, *Cours d'algèbre*, Ellipses, 1996.

Programme des cours

du Master 1 Algébre Appliquée

Semestre 2

Algèbre commutative

Code UE: MYMAA005
Tutelle: Département de Mathématiques, UVSQ
Volume horaire: CM: 24h TD: 24h
ECTS: 6
Semestre: 2
Intervenants: Ana-Maria Castravet
Lieu: UVSQ
Parcours: «Algèbre appliquée»

Pré-requis: Algèbre de Licence (groupes, anneaux, corps, polynômes et congruences), cours de théorie des nombres et cryptographie

Description

L'objectif de ce cours est de permettre aux étudiants d'aborder sereinement la géométrie algébrique et l'algèbre effective. Le cours est tourné vers l'étude des anneaux de polynômes. On cherche constamment à interpréter géométriquement les théorèmes d'algèbre abstraite : lemme de normalisation vs. projection sur un espace vectoriel, Nullstellensatz vs. recherche de l'idéal d'un fermé algébrique. Interprétation géométrique de la dimension de Krull.

Contenu

- Anneaux noethériens, théorème de la base de Hilbert.
- Topologie de Zariski de k^n.
- Correspondance entre idéaux et fermés algébriques.
- Anneaux de fractions, localisation.
- Extensions entières : going up et going down.
- Lemme de normalisation, degré de transcendance, dimension.
- Nullstellensatz.

Bibliographie

- Atiyah et Mac Donald, *An introduction to commutative algebra*, Addison-Wesley, 1969.
- Chambert-Loir *Algèbre commutative et introduction) la géométrie algébrique* http://www.math.u-psud.fr/ chambert/enseignement/2013-14/aceiga/Dea.pdf
- Cox, Little et O'Shea, *Ideal, varieties and algorithms*, Springer, 1991.
- Matsumura, Hideyuki *Commutative ring theory*. Cambridge University Press, 1986.
- C. Peskine *An algebraic introduction to complex projective geometry, I. Commutative algebra*, Cambridge University Press, 1996.
- D. Perrin, *Cours d'algèbre*, Ellipses, 1996.
- Samuel et Zariski, *Commutative algebra*, 2 volumes, Springer.

Analyse d'algorithmes, Programmation

Code UE: MYMAA006
Tutelle: Département de Mathématiques, UVSQ
Volume horaire: CM: 20h TD: 20h
ECTS: 5
Semestre: 2
Intervenants: bauer
Lieu: UVSQ
Parcours: «Algèbre appliquée», «Analyse, Modélisation et Simulation»

Pré-requis: non suggérés

Description

Introduction aux techniques de conceptions d'algorithmes et d'analyse de performances. TPs sur machine avec environnement Python/Sage.

Contenu

- Analyse d'algorithmes, modèles de complexité, complexité asymptotique, classes de complexité.
- Algorithmes de tri.
- Structures de données et algorithmes : piles, files, tables de hachage, arbres, graphes.
- Programmation dynamique, programmation linéaire entière.
- Problèmes NP complets, machines de Turing.

Bibliographie

- Thomas H. Cormen. Charles E. Leiserson. Ronald L. Rivest. Clifford Stein. Introduction to Algorithms. Third Edition. The MIT Press. Cambridge, Massachusetts.
- Christos H. Papadimitriou. Computational complexity. Addison-Wesley, 1994. 523 pages.

Calcul sécurisé

Code UE: MIN17218
Tutelle: Département d'Informatique et Département de Mathématiques, UVSQ
Volume horaire: CM: 12h TD: 24h
ECTS: 4
Semestre: 2
Intervenants: Louis Goubin
Lieu: UVSQ
Parcours: «Algèbre appliquée», Informatique

Pré-requis: Cours de cryptographie (M1 MINT, 1er semestre)

Description

Traditionnellement, en cryptographie, on cherche à garantir la confidentialité, l'intégrité et l'authenticité de «messages», qui sont des objets «statiques» (stockés, ou transmis tels quels sur des canaux de communication non sécurisés). En revanche on ne considère pas la sécurité des algorithmes et protocoles cryptographiques eux-mêmes (qui sont en général des programmes, qui s'exécutent, et sont donc des objets «dynamiques»). Par exemple on ne s'intéresse pas :

- à la confidentialité des programmes (le principe de Kerckhoffs suppose qu'ils sont connus de tout le monde),
- ni à leur intégrité (on suppose qu'Alice et Bob exécutent ces algorithmes / protocoles / programmes correctement, sans aucune modification / erreur / bug),
- ni à leur authenticité (on suppose que les algorithmes / protocoles / programmes exécutés par Alice et Bob ont été installés par une autorité de confiance).

Dans l'UE «Calcul sécurisé», on verra qu'en réalité il est très important de sécuriser également les calculs (au sens d'algorithmes / protocoles / programmes).

Contenu

- Le cours couvrira des aspects pratiques de ces problèmes de sécurité (débordement de tampon, rétro-analyse de code, attaques par canaux auxiliaires, injection de fautes, ...)
- Ce sera aussi l'occasion d'approfondir des questions plus théoriques (modélisation de la notion de calcul, machines de Turing, garbled circuits, programmes auto-modifiants, obfuscation de code, ...), en montrant comment ces notions peuvent être utilisées pour prévenir les vulnérabilités du logiciel.
- Le cours et les TDs seront illustrés par de nombreux exemples, notamment issus de la sécurité des cartes à puce, de la virologie informatique, et des applications émergentes dans le «calcul en nuage» (cloud computing).

Calcul scientifique et modélisation

Code UE: MYANM006
Tutelle: Département de Mathématiques, UVSQ
Volume horaire: CM: 20h TP: 20h
ECTS: 6
Semestre: 2
Intervenants: Tahar Boulmezaoud
Lieu: UVSQ
Parcours: «Algèbre appliquée», «Analyse, Modélisation et Simulation»

Pré-requis: analyse et algèbre linéaire et matriciel de licence

Description

Le but de cette UE est de préparer les étudiants aux bases de la programmation et du calcul scientifique. Elle comporte essentiellement trois parties.
La première partie du cours sera dédiée à la maitrise des éléments fondamentaux d'un langage de programmation de type C ou Python. L'apprentissage du langage sera accompagné d'une mise en oeuvre de quelques algorithmes numériques.
La deuxième partie sera consacrée aux méthodes numériques modernes et leur implémentation. Il s'agira essentiellement de la résolution de systèmes linéaires, des équations différentielles et des équations aux dérivées partielles. On y abordera aussi l'étude de problèmes issus de la modélisation mathématique de phénomènes rencontrés dans d'autres disciplines (physique, biologie, sciences de l'ingénieur, science de données, etc.).
La troisième partie consistera en la réalisation d'un projet.

Contenu

- Eléments et bases de la programmation en Langage C (ou en Python).
- Rappels sur les méthodes directes pour la résolution de systèmes linéaires
- Méthodes itératives classiques (Jacobi, Gauss-Seidel, relaxation).
- Méthodes itératives modernes. Méthodes des sous-espaces de Krylov.
- Calcul de valeurs propres.
- Schémas de résolution d'équations différentielles.
- Méthode des différences finis.
- Introduction à la méthode des éléments finis (problèmes aux limites 1D et 2D)

Bibliographie

— J. Stoer et R. Bulirsh, Introduction to numerical analysis, Springer (2nd edition).
— Introduction à l'analyse numérique matricielle et Optimisation : Ph. G. Ciarlet, Masson, 1988.
— Introduction au calcul scientifique. Aspects algorithmiques, P. Ciarlet, en ligne.
— Analyse numérique des équations aux dérivées partielles, R. Herbin, HAL, en ligne.
— A. Ern et J.-L. Guermond, éléments finis : théorie, applications, mise en oeuvre, Springer.

Introduction aux courbes elliptiques

Code UE: MYMAA007
Tutelle: Département de Mathématiques UVSQ
Volume horaire: CM: 24h TD: 24h
ECTS: 6
Semestre: 2
Intervenants: Vincent Sécherre (CM)
Lieu: UVSQ
Parcours: «Algèbre appliquée»

Pré-requis: Algèbre de Licence et cours d'algèbre générale de M1 semestre 1

Description

C'est un cours d'introduction à la théorie algébrique des courbes elliptiques, considérées comme des cubiques du plan projectif. On définit d'abord le plan projectif, et on effectue la classification des coniques projectives planes (sur un corps algébriquement clos). On étudie ensuite les cubiques projectives planes : on prouve qu'elles possèdent toujours un point d'inflexion, et qu'elles sont entièrement caractérisées par leur invariant modulaire. On définit ensuite les courbes elliptiques, puis la loi de groupe, les fonctions rationnelles et les diviseurs sur une courbe elliptique. On termine le cours par le théorème d'Abel-Jacobi, déterminant à quelles conditions un diviseur sur une courbe elliptique est le diviseur d'une fonction rationnelle.

Contenu

- Droite et plan projectifs
- Coniques et cubiques projectives planes
- Points d'inflexions
- Invariant modulaire
- Courbes elliptiques
- Fonctions rationnelles et diviseurs sur une courbe elliptique
- Théorème d'Abel-Jacobi

Bibliographie

- J. Silvermann, The arithmetic of elliptic curves, GTM 106, Springer, 1986.
- J. Silverman & J. Tate, Rational points on elliptic curves, Springer, 1992.
- Tout autre livre introductif sur les courbes elliptiques.

Théorie de l'information

Code UE: MYMAA008
Tutelle: Département de Mathématiques, UVSQ
Volume horaire: CM: 12h TD: 12h
ECTS: 3
Semestre: 2
Intervenants: Yann Rotella
Lieu: UVSQ
Parcours: «Algèbre appliquée»

Pré-requis: Algèbre linéaire. Quelques éléments d'algèbre. Théorie élémentaire des probabilités.

Description

Le but d'un système de communication est le transport d'information d'une source à un destinataire via un canal de communication. Ce canal possède en général des imperfections ce qui peut engendrer des erreurs de transmission. Aussi, le canal peut être sujet à des écoutes ce qui peut poser des problèmes de confidentialité. Finalement, l'utilisation d'un canal a un coût, il est donc important d'optimiser son usage.

Pour répondre à ces différentes exigences, on effectue un prétraitement de l'information ; il s'agit de la chaîne de codage. Celle-ci se divise en trois étapes : compression, chiffrement et ajout de redondance. Ces techniques font appel à la théorie des probabilités et à l'algèbre discrète. Ce cours présente les bases de la première et la troisième étape de la chaîne de codage, la seconde étant abondamment étudiée dans des cours de cryptographie.

Contenu

- Notions de base en théorie de l'information (entropie, information mutuelle).
- Algorithmes de compression sans perte (étape 1 de la chaîne de codage).
- Théorie des codes correcteurs d'erreurs (étape 3 de la chaîne de codage).
  - Canal sans mémoire à temps discret. Notion de capacité. Théorème de codage pour un canal bruyant. Principe de décodage par maximum de vraisemblance. Borne sur la probabilité d'erreur de décodage.
  - Théorie des codes correcteurs en blocs. Distance minimale et problématique des bornes sur la taille d'un code. Notion de code parfait.
  - Codes linéaires. Matrice génératrice et matrice de parité. Décodage par syndrome. Codes duaux. Polynôme énumérateur des poids. Identité de Mac-Williams.
  - Etude de certaines familles de codes linéaires (en bloc) et algorithmes de décodage.
  - Codes convolutionnels et algorithme de Viterbi.

Bibliographie

— The Theory of Error-Correcting Codes. F. J. MacWilliams, N. J. A. Sloane North Holland Publishing Co. 1977.

— Théorie des codes (Compression, cryptage, correction). J.-G. Dumas, J.-L. Roch, E. Tannier et S. Varrette, Dunod 2007.

— Elements of Information Theory. Cover, Thomas M., and Joy A. Thomas. John Wiley & Sons, Inc., 2006.

Corps professoral

Balthazar Bauer
Adresse : Laboratoire de Mathématiques de Versailles
Université de Versailles Saint-Quentin-en-Yvelines
45, Avenue des Etats-Unis
78035 Versailles Cedex.
Tél. : +33 (0)1 39 25 36 23
Mél : balthazar.bauer2@uvsq.fr
Web : https://lmv.math.cnrs.fr/laboratoire/annuaire/membres-du-laboratoire/
Cours en master 1 :
- Analyse d'algorithmes, programmation

Tahar Z. Boulmezaoud
Adresse : Laboratoire de Mathématiques de Versailles
Université de Versailles Saint-Quentin-en-Yvelines
45, Avenue des Etats-Unis
78035 Versailles Cedex.
Tél. : +33 (0)1 39 25 36 23
Mél : tahar.boulmezaoud@uvsq.fr
Web : https://boulmezaoud.perso.math.cnrs.fr/
Cours en master 1 :
- Calcul scientifique et modélisation

Ana-Maria Castravet
Adresse : Laboratoire de Mathématiques de Versailles
Université de Versailles Saint-Quentin-en-Yvelines
45, Avenue des Etats-Unis
78035 Versailles Cedex.
Tél. : +33 (0)1 39 25 46 41
Mél : ana-maria.castravet@uvsq.fr
Web : https://sites.google.com/view/castravet/home
Cours en master 1 :
- Théorie des nombres et cryptographie
- Algèbre commutative

Catherine Donati-Martin
Adresse : Laboratoire de Mathématiques de Versailles
Université de Versailles Saint-Quentin-en-Yvelines
45, Avenue des Etats-Unis
78035 Versailles Cedex.
Tél. : +33 (0)1 39 25 30 61
Mél : @uvsq.fr
Web : http://lmv.math.cnrs.fr/annuaire/donati-martin-catherine/
Cours en master 1 :
- Probabilités

Louis Goubin
Adresse : UVSQ - Laboratoire PRISM
Batiment Descartes
45 Avenue des Etats Unis
78035 Versailles Cedex.
Tél. : ++ 33 (0)1 39 25 43 29
Mél : louis.goubin@uvsq.fr
Web : http://www.goubin.fr/
Cours en master 1 :
- Crypthographie
- Calcul sécurisé

Guillermo Moreno-Socias
Adresse : Laboratoire de Mathématiques de Versailles
Université de Versailles Saint-Quentin-en-Yvelines
45, Avenue des Etats-Unis
78035 Versailles Cedex.
Tél. : +33 (0)1 39 25 46 37
Mél : Guillermo.Moreno-Socias@uvsq.fr
Web : http://lmv.math.cnrs.fr/annuaire/guillermo-moreno-socias/
Cours en master 1 :
- Introduction au calcul formel et projet, Théorie de nombres

---

Pierre-Guy Plamondon
Adresse : Laboratoire de Mathématiques de Versailles
Université de Versailles Saint-Quentin-en-Yvelines
45, Avenue des Etats-Unis
78035 Versailles Cedex.
Tél. : +33 (0)1 39 25 36 17
Mél : pierre-guy.plamondon@uvsq.fr
Web : https://www.imo.universite-paris-saclay.fr/ plamondon/
Cours en master 1 :
- Introduction au calcul formel et projet

Emmanuel Rio
Adresse : Laboratoire de Mathématiques de Versailles
Université de Versailles Saint-Quentin-en-Yvelines
45, Avenue des Etats-Unis
78035 Versailles Cedex.
Tél. : +33 (0)1 39 25 36 26
Mél : emmanuel.rio@uvsq.fr
Web : https://lmv.math.cnrs.fr/en/laboratory/directory/emmanuel-rio/
Cours en master 1 :
- Probabilités

Yann Rotella
Adresse : Laboratoire de Mathématiques de Versailles
Université de Versailles Saint-Quentin-en-Yvelines
45, Avenue des Etats-Unis
78035 Versailles Cedex.
Tél. : +33 (0)1 39 25 40 35
Mél : yann.rotella@uvsq.fr
Web : https://rotella.fr/
Cours en master 1 :
- Analyse d'algorithmes, programmation
- Théorie de l'information

Vincent Sécherre
Adresse : Laboratoire de Mathématiques de Versailles
Université de Versailles Saint-Quentin-en-Yvelines
45, Avenue des Etats-Unis
78035 Versailles Cedex.
Tél. : +33 (0)1 39 25 36 20
Mél : vincent.secherre@uvsq.fr
Web :
https://lmv.math.cnrs.fr/laboratoire/annuaire/membres-du-laboratoire/vincent-secherre/
Cours en master 1 :
- Introduction aux courbes elliptiques