CONTRAT 2009 2012

DEMANDE D'HABILITATION DE DIPLOME DE MASTER

Master Mention Mathématiques et Informatique
Université Paris 13

Master Mention Mathématiques et Applications
Université Paris 8

Descriptifs des unités d'enseignement

Spécialité

Mathématiques fondamentales et Protection de l'Information

Spécialité :	**Mathématiques fondamentales et Protection de l'information**

Intitulé de l'UE :	**Algèbre 1**	**S1**

Semestre : S1

Crédits : 6

Heures de cours : CM 39 TD 39

But du cours : Corps et théorie de Galois. Modules sur un anneau principal et applications.

Responsable : **LAGA**

Pré requis :

Contenu :

Polynômes symétriques, séries formelles

Corps : extensions de corps, polynôme minimal, corps cyclotomiques, corps finis

Correspondance de Galois

Modules de type fini sur un anneau principal, applications au théorème de structure des groupes abéliens de type fini et à la réduction de Jordan des matrices

Intitulé de l'UE :	**Analyse de Fourier et théorie du signal**	**S1**

Semestre : S1, obligatoire

UE commune avec la spécialité Algorithmique, Modélisation, Images

Heures de cours : CM 19,5 TD 19,5

But du cours : Analyse hilbertienne et de Fourier et applications en théorie du signal

Responsable : **LAGA**

Pré requis : Aucun

Contenu :

Compléments sur les espaces de Hilbert. Bases hilbertiennes, séries de Fourier. Théorème de Riesz, dualité.

Transformation de Fourier dans L^1, dans L^2 et sur l'espace de Schwartz. Convolution, régularisation.

Transformation de Fourier discrète, transformation de Fourier rapide.

Filtrage. Echantillonnage, théorème de Shannon.

Intitulé de l'UE :	**Modèles aléatoires 1**	**S1**

Semestre : S1

Crédits : 4

Heures de cours : CM 19,5 TD 19,5

But du cours :

Responsable : **LAGA**

Pré requis :

Contenu :

Rappels de probabilités, fonction génératrice des moments ; propriété de Markov. Probabilités de transition ; lois invariantes et lois limites.

Exemples de chaînes de Markov (marches aléatoires, modèles génétiques, files d'attente, chaînes de branchement, chaîne de naissance ou de mort.

États transients, états récurrents. Temps et probabilité d'absorption. Temps moyen de première visite et de récurrence.

Intitulé de l'UE : Analyse complexe S1

Semestre : S1

Crédits : 4

Heures de cours : CM 19,5 TD 19,5

But du cours : Application de la théorie de la variable complexe aux équations différentielles provenant de la mécanique et de la physique

Responsable : **LAGA**

Pré requis :

Contenu :

Rappels :

- fonctions holomorphes : équations de Cauchy-Riemann, théorème de Cauchy, fonctions multiformes, points de branchement, développement en séries de Taylor/de Laurent, formule des résidus, prolongement analytique (principe de symétrie de Schwarz).

- théorie des équations différentielles : sous des hypothèses de régularité, l'espace des solutions d'une équation différentielle linéaire homogène d'ordre n est de dimension n.

Propriétés des intégrales de Cauchy : limite à droite et à gauche de l'intégrale de Cauchy, valeur principale, formules de Plemelj, problème de Hilbert.

Transformations conformes, exemples.

Résolution de problèmes de physique et de mécanique de la rupture par la variable complexe : fonctions harmoniques, fonctions biharmoniques, résolution de quelques problèmes d'élasticité linéaire et application à la mécanique de la rupture, applications aux équations intégrales.

Intitulé de l'UE : Analyse fonctionnelle S1

Semestre : S1

UE commune avec la spécialité Algorithmique, Modélisation, Images

Crédits : 4

Heures de cours : CM 19,5 TD 19,5

But du cours : Théorèmes généraux et outils fondamentaux de l'analyse fonctionnelle.

Responsable : **LAGA**

Pré requis :

Contenu :

Espaces fonctionnels : exemples classiques, théorème de Baire, de Banach-Steinhaus, du graphe fermé et de l'application ouverte.

Théorème d'Ascoli. Dualité, Théorème de Hahn-Banach. Topologies faibles.

Eléments de théorie spectrale des opérateurs.

Spécialité :	**Mathématiques fondamentales et Protection de l'information**

Intitulé de l'UE :	**Géométrie différentielle**	**S1**

Semestre : S1

Crédits : 4

Heures de cours : CM 19,5 TD 19,5

But du cours : Théorèmes généraux et outils fondamentaux de la géométrie différentielle.

Responsable : **LAGA**

Pré requis :

Contenu :

· Propriétés affines et métriques des surfaces de R, formes fondamentales, calculs d'aire

· Sous-variétés de R^n : définitions, espaces tangents, exemples. Groupes classiques, application exponentielle

· Champs de vecteurs sur une partie ouverte de R^n : flots, tracés d'orbites, aspects dynamiques. Exemples des champs de gradient et des champs hamiltoniens

· Théorème du puits et description de la structure locale au voisinage d'une singularité non dégénérée.

· Exemples de champs de vecteurs tangents à une sous-variété.

Intitulé de l'UE :	**Topologie**	**S1**

Semestre : S1

Crédits : 4

Heures de cours : CM 19,5 TD 19,5

But du cours : Topologie ensembliste et introduction à la topologie algébrique

Responsable : **LAGA**

Pré requis :

Contenu :

· Compléments de topologie : espaces topologiques, connexité, compacité, topologie-quotient, espaces séparés et normaux, espaces paracompacts

· Groupes topologiques, surfaces

· Homotopie entre applications continues

· Groupe fondamental : exemples, revêtements, revêtement universel.

Spécialité :	**Mathématiques fondamentales et Protection de l'information**

Intitulé de l'UE :	**Complexité algorithmique**	**S1**

Semestre : S1

UE commune avec la spécialité Algorithmique, Modélisation, Images

Crédits : 4

Heures de cours : CM 19,5 TD 19,5

But du cours : Introduire les concepts de la complexité en temps et en espace.

Responsable : **Christophe Tollu**

Pré requis : Aucun

Contenu :

1. Rappel sur la notion de calculabilité.
2. Machine de Turing.
3. Classes PSPACE, P et NP.
4. Problèmes NP-difficiles ; exemples issus de l'arithmétique et de la cryptographie.
5. Classes probabilistes.

Intitulé de l'UE :	**Programmation pour la cryptographie**	**S1**

Semestre : S1

Crédits : 4

Heures de cours : CM 19,5 *TD 19,5*

But du cours : programmation en C des principaux algorithmes utilisés dans le domaine de la correction d'erreur et de la cryptographie .Il montrera sur des exemples variés comment les notions mathématiques sont représentées en machine.

Responsable : **Sihem Mesnager**

Pré requis : Connaissances de base en algorithmique et éléments de base du langage C ou une bonne pratique d'un autre langage de programmation.

Contenu Liste (non exhaustive) des algorithmes traités :

1. Algorithmes généraux d'algèbre :
   - Algorithme d'Euclide binaire et calcul d'inverse, sur les entiers et les polynômes binaires.
   - Algorithmes de calcul sur les corps finis, irréductibilité des polynômes.
   - Transformée de Fourier discrète.
2. Algorithmes utilisés en cryptographie asymétrique :
   - Calculs modulaires, Exponentiation.
   - Fractions de Gauss, suites de Fibonacci, suite de Lucas.
   - Tests de primalité, tests probabilistes de primalité, pseudo premier de Fibonacci, pseudo-premier de Fermat.
   - Algorithme de calcul du symbole de Legendre, symbole de Jacobi , résidus quadratiques.
3. Algorithme pour l'analyse des primitives du chiffrement symétrique : Fonctions Booléennes et vectorielles
   - Forme Algébrique Normale, degré algébrique
   - Transformée de Walsh et ordre de corrélation/résilience
   - Non-linéarité
   - Fonction auto-corrélation.

Spécialité :	**Mathématiques fondamentales et Protection de l'information**

Intitulé de l'UE :	**Traitement statistique du signal**	**S1**

Semestre : S1

UE commune avec la spécialité Algorithmique, Modélisation, Images

Crédits : 4

Heures de cours : CM 19,5 TD 19,5 TP 12

But du cours : Apprendre aux étudiants à utiliser les processus stochastiques stationnaires du second ordre (principalement à temps discret) comme outils de modélisation permettant de résoudre, de manière statistiquement optimale (au sens du minimum de variance) des problèmes de filtrage, d'estimation et de prédiction

Responsables : **Caroline Kulcsár et Henri-François Raynaud (L2TI)**

Pré requis : notions de base de la théorie des probabilités, et de l'algèbre linéaire et quadratique

Contenu :

Processus aléatoires à temps discret : moments, processus stationnaires, processus gaussiens scalaires et vectoriels. Notions d'espace de Hilbert stochastique. Ergodicité.

Représentation spectrale, fonction d'autocorrélation, densité spectrale de puissance, bruit blanc.

Modèles paramétriques AR et ARMA. Modèles markoviens, représentations d'état, problème de réalisation.

Filtrage et prédiction à variance minimale. Filtre de Kalman.

Estimation des paramètres d'un modèle AR/ARMA. Méthode de Yule-Walker.

Introduction aux processus à temps continu. Problème de discrétisation.

Intitulé de l'UE :	**Culture générale**	**S1**

UE commune avec la spécialité Algorithmique, Modélisation, Images

Semestre : S1, obligatoire

Crédits : 4

Anglais

Heures de cours : CM-TD 19,5

Responsables : **Gary Grill, Monique Nicolas, Edith Patrouilleau**

Contenu :

Entraînement systématique à la compréhension orale et à la prise de parole en continu (exposé, analyse personnelle argumentée).
Traitement de l'information à partir de messages oraux et écrits de plus en plus complexes et orientés vers le domaine "sciences et technologie" (émissions de radio, de télévision, extraits de films, articles de presse).
Recherche documentaire dans la presse scientifique et sur internet.
Une approche interculturelle est développée dans une perspective d'ouverture à l'international.

Histoire des sciences : Mathématiques et sciences : la question des fondements

Heures de cours : CM 19,5

Responsable : **Marie-José Durand-Richard**

Contenu :

Les mathématiques disposent d'un édifice théorique structuré par la géométrie depuis les Eléments d'Euclide. Il existe pourtant d'autres formes de pensée mathématique que celle-ci dans d'autres civilisations, et la nature des fondements

des mathématiques s'est trouvée sans cesse ré-intérrogée du fait d'autres pratiques que celles de la géométrie, notamment avec la naissance et la formalisation de l'algèbre, la distinction entre algèbre et analyse, la naissance des géométries non-euclidiennes, l'algébrisation de la logique, la naissance de la topologie. Ces développements sont consubstantiels de la mathématisation de nouveaux secteurs d'activité scientifique.

Principaux thèmes abordés

• Géométrie euclidienne et théorisation du continu

• Unification des problèmes arithmétiques et géométriques autour de la symbolisation de « l'inconnue » : la naissance de l'al-jabr

• Approche algébrique de la notion de dérivée et maîtrise de la notion de vitesse

• Algébrisation de la logique

• Diversification des géométries au 19ème siècle

• Mathématiques et relativité

• Mathématiques et Géodésie : de l'Analysis Situs à la topologie

• Théorie de l'information et probabilités

Spécialité :	**Mathématiques fondamentales et Protection de l'information**

Intitulé de l'UE :	**Travail d'études et de recherche (TER)**	**S2**

Semestre : 2

Crédits : 6

Heures de cours : TP 58,5

But du cours : Expérience d'un travail personnel de documentation et de synthèse.

Responsable : **LAGA**

Pré requis : Le sujet du TER doit être cohérent avec les choix d'option de l'étudiant.

Contenu :
L'étudiant doit réaliser un mémoire sous la direction d'un enseignant de l'équipe pédagogique sur un sujet qu'il choisit en accord avec cet enseignant.

Il est demandé un travail de documentation personnelle et de synthèse sur un thème qui ne fait pas partie de l'objet d'un cours. Il sera accompagné d'une implémentation sur ordinateur pour les sujets qui s'y prêtent.

Ce travail aboutira à la rédaction d'un rapport et à un exposé de soutenance.

Intitulé de l'UE :	**Algèbre 2**	**S2**

Semestre : S2

Crédits : 4

Heures de cours : CM 19,5 TD 19,5

But du cours : Introduction à l'algèbre commutative et à la théorie des nombres

Responsable : **LAGA**

Pré requis :

Contenu :

Introduction à l'algèbre commutative : conditions de finitude, extensions entières d'anneaux, norme, trace et discriminant.

Introduction à la théorie des nombres : anneaux de Dedekind, corps de nombres, le groupe des unités est de type fini.

Intitulé de l'UE :	**Courbes elliptiques et tores complexes**	**S2**

Semestre : S2

Crédits : 4

Heures de cours : CM 19,5 TD 19,5

But du cours : Introduction à la théorie des courbes elliptiques avec comme l'un des objectifs l'illustration de l'interaction entre différents domaines des mathématiques: analyse, algèbre, géométrie et applications.

Responsable : **LAGA**

Pré requis :

Contenu : Théorie complexe : fonctions elliptiques, équations de Weierstrass complexes, paramétrisation complexe d'une courbe elliptique par un tore complexe, points de torsion, isogénies.

Spécialité :	Mathématiques fondamentales et Protection de l'information

Théorie algébrique : introduction à la théorie des courbes algébriques, théorème de Riemann-Roch, équations de Weierstrass algébriques, invariant j, module de Tate.

Théorie sur les corps finis : nombre de points, théorème de Hasse, isogénie de Frobenius, algorithmes de comptage de points, applications à la cryptographie.

Intitulé de l'UE :	Cryptographie	S2

UE mutualisée avec la spécialité Algorithmique, Modélisation, Images

Semestre : S2, obligatoire pour le parcours Protection de l'information.

Crédits : 4

Heures de cours : CM 19,5 TD 19,5

But du cours : Approfondir la connaissance la cryptographie, en particulier des chiffrements par flots et par blocs, des protocoles sans transfert de connaissances et les cryptosystèmes à clé publique utilisant les codes

Responsable : **Claude Carlet**

Pré requis : Une connaissance de base des corps finis et de la cryptographie correspondant au cours d'introduction à la cryptographie de la licence de mathématiques et informatique de l'Université Paris 8. Un polycopié de ce cours ainsi qu'une liste d'exercices corrigés seront mis à disposition des étudiants.

Contenu :

• Attaques sur les schémas de chiffrement par flots (à la volée) : attaques par corrélation et fonctions résilientes ; attaque par approximation linéaire et nonlinéarité des fonctions booléennes. Constructions de fonctions hautement résilientes et de forte non linéarité. Attaques algébriques et immunité algébrique des fonctions booléennes.

• Rappels et compléments sur les attaques sur les schémas de chiffrement par bloc. Mesures de la non linéarité des fonctions booléennes vectorielles; fonctions presque parfaitement non linéaires et fonctions presque courbes.

• Cryptographie à clé publique :

- protocoles d'authentification, transfert nul de connaissances.

- codes correcteurs et cryptographie.

Intitulé de l'UE :	Décisions statistiques	S2

UE commune avec la spécialité Algorithmique, Modélisation, Images

Crédits : 4

Heures de cours : CM 19,5 TD 19,5

But du cours : Maitrise de quelques outils avancés de l'analyse statistique

Responsable : **LAGA**

Pré requis :

Contenu :

Problème d'estimation : Estimateur ; Risque quadratique ; Statistique exhaustive ; Modèle Exponentiel. Construction d'estimateurs : Estimateur de substitution ; Estimateur bayésien ; maximum de vraisemblance. Information de Fisher et Inégalité de Cramer-Rao.

Vecteurs Gaussiens : Loi du X2 ; Théorème de Student ; Théorème de Cochran.

Intervalle et Région de confiance. Tests d'hypothèses : Lemme de Neyman-Pearson ; Test du rapport de vraisemblance ; Famille à rapport de vraisemblance monotone ; Tests UPP ; Théorème de Lehmann ; Test de comparaison.Tests du X2 ; test d'ajustement.

Spécialité :	**Mathématiques fondamentales et Protection de l'information**

Intitulé de l'UE :	**Optimisation continue**	**S2**

Semestre : S2

UE commune avec la spécialité Algorithmique, Modélisation, Images

Crédits : 4

Heures de cours : CM 19,5 TD 19,5

But du cours : Maîtriser les résultats et méthodes de l'optimisation en dimension finie

Responsable : **LAGA**

Pré requis :

Contenu :

Optimisation avec ou sans contraintes : convexité, lagrangien, dualité, points selles.

Algorithmes pour l'optimisation sans contrainte : gradient, gradient conjugué, gradient conjugué non linéaire, régions de confiance...

Algorithmes pour l'optimisation avec contraintes : Algorithmes de projection, Uzawa…

Intitulé de l'UE :	**EDP et distributions**	**S2**

Semestre : S2

UE commune avec la spécialité Algorithmique, Modélisation, Images

Crédits : 4

Heures de cours : CM 19,5 TD 19,5

But du cours :

Responsable : **LAGA**

Pré requis :

Contenu :

Introduction à la théorie des distributions. Convolution, régularisation, distributions sur un ouvert.

Distributions tempérées, transformation de Fourier et lien avec les espaces de Sobolev.

Application à la résolution des équations aux dérivées partielles linéaires : laplacien, équation de la chaleur, équation des ondes.

Intitulé de l'UE :	**Processus stochastiques**	**S2**

UE commune avec la spécialité Algorithmique, Modélisation, Images

Semestre : S2

Crédits : 4

Heures de cours : CM 19,5 TD 19,5

But du cours : Familiariser l'étudiant avec des techniques avancées de probabilités et processus et en travaillant sur des modèles venant de la finance et de l'assurance.

Responsable : **LAGA**

Pré requis : Modèles aléatoires 1

Spécialité :	Mathématiques fondamentales et Protection de l'information

Contenu :

Conditionnement (Espérance conditionnelle et lois conditionnelles).

Vecteur gaussiens.

Martingales à temps discret.

Introduction aux modèles financiers à temps discret.

Options européennes et américaines. Modèle de Cox-Ross-Rubinstein.

Processus de Poisson et applications à l'assurance.

Intitulé de l'UE :	Systèmes dynamiques	S2

UE commune avec la spécialité Algorithmique, Modélisation, Images

Semestre :

Crédits :

Heures de cours : CM 19,5 TD 19,5

But du cours : Théorèmes et outils fondamentaux de systèmes dynamiques.

Responsable : **LAGA**

Pré requis :

Contenu :

Systèmes dynamiques à temps discret ou à temps continu.

Premiers exemples : problème des n corps, pendule, billard, décalage de Bernoulli, homéomorphismes du cercle.

Flots sur les tores.

Relèvement des applications continues, translations et endomorphismes linéaires des tores.

Propriétés topologiques et ergodiques des systèmes dynamiques. Mesures invariantes, théorèmes ergodiques. Illustrations sur les exemples.

Propriétés topologiques des flots, ensembles limites, sections de Poincaré globale et locale. Théorie de Poincaré-Bendixon.

Intitulé de l'UE :	Codes correcteurs	S2

Semestre : S2

Crédits : 4

Heures de cours : CM 19,5 TD 19,5

But du cours : Approndir la connaissance des codes correcteurs d'erreurs, en particulier des codes cycliques et de certains codes nonlinéaires.

Responsable : **Claude Carlet**

Pré requis : Une connaissance de base des corps finis et des codes cryptographie correspondant au cours d'introduction aux codes correcteurs de la licence de mathématiques et informatique de l'Université Paris 8. . Un polycopié de ce cours ainsi qu'une liste d'exercices corrigés seront mis à disposition des étudiants.

Contenu :

• Compléments sur les extensions galoisiennes et sur la factorisation des polynômes à coefficients dans les corps. Application à la construction des codes cycliques.

• Codes cycliques (rappels), borne BCH. Les codes de Reed-Solomon et la correction d'erreur dans le disque compact.

• Les algorithmes de décodage des codes cycliques.

• La borne de Gilbert-Varshamov et les codes géométriques.

• La dualité formelle des codes de Kerdock et de Preparata. Les codes Z4-linéaires et leurs généralisations.

Intitulé de l'UE :	Projets numériques	S2

UE mutualisée de la formation d'ingénieurs spécialité MACS

Semestre : 2

Crédits : 4

Heures de cours : CM 12 TP 24

But du cours : Faire acquérir aux étudiants une réelle compétence pratique dans les domaines étudiés.

Responsable : **Ahmed Kebaier et Nadia Oudjane**

Pré requis :

Contenu :

Appliquer les méthodologies acquises à des problèmes concrets sous forme de mini-projets d'application sur ordinateur, avec Matlab ou un autre logiciel.

Intitulé de l'UE :	Culture générale	S2

UE commune avec la spécialité Algorithmique, Modélisation, Images

Semestre : S2, obligatoire

Crédits : 4

Anglais

Heures de cours : CM et TD 19,5

Responsable : **Gary Grill, Monique Nicolas, Edith Patrouilleau**

Contenu :

Les supports oraux et écrits sont orientés autour de deux axes :
- le champ d'étude large de l'étudiant (documentation scientifique, conférences)
- le domaine professionnel (introduction au monde de l'entreprise)

La compréhension et l'expression orales sont privilégiées par des mises en situation visant à tester la capacité à interagir (l'anglais au téléphone, résolution de problèmes, participation à un projet). A partir de scénario "réalistes" les étudiants seront fortement incités à la prise de parole et à la production d'écrits (comptes-rendus, courriers divers présentation de travaux).

Histoire des sciences : Histoires de logiques

Heures de cours : CM 19,5

Responsable : **Marie-José Durand-Richard**

Contenu : *Formalisation, mécanisation et calculabilité*

Les travaux de G. Boole (1815-64) ont conduit à séparer radicalement la logique de l'analyse du langage et à l'identifier à un calcul écrit d'abord algébriquement. Ses successeurs (notamment Jevons, Frege, Russell) chercheront à en expliciter les conditions de validité. Les différentes étapes de cette restructuration déboucheront sur des distinctions — entre validité et vérité, entre syntaxe et sémantique — particulièrement pertinentes pour expliciter les automatismes logiques, ainsi que pour en concevoir et en réaliser la mécanisation.

Mais elles contribueront aussi à mieux appréhender les limites de cette conception du langage attachée à sa

formalisation.

Principaux thèmes abordés

• Le réseau des algébristes anglais et le rapprochement entre mathématiques et logique

• Le courant logiciste de Gottlob Frege (1848-1942) à Bertrand Russell (1872-1970)

• Potentialités et limitations des formalismes de Kurt Gödel (1906-1978) et Abraham Tarski à Alan Turing (1912-1954)

• Du projet d'intelligence artificielle à l'explosion des logiques

Spécialité :	**Mathématiques fondamentales et Protection de l'information**

Intitulé de l'UE :	**Mathématiques fondamentales**	**S3**

Trois unités optionnelles proposées chaque année

Semestre : S3

Crédits : 9

Heures de cours : CM 39

But du cours : Maîtrise d'outils sophistiqués des mathématiques

Responsable : **LAGA**

Pré requis :

Contenu :
Ces enseignements dont le contenu sera élaboré chaque année nécessiteront un travail personnel important. Il s'agira de cours devant permettre à l'étudiant d'acquérir des outils sophistiqués des mathématiques portant sur les thèmes suivants :

- Arithmétique et géométrie algébrique
- Modélisation et calcul scientifique
- Physique mathématique et équations aux dérivées partielles
- Probabilités et statistiques
- Systèmes dynamiques
- Topologie algébrique

Intitulé de l'UE :	**Mathématiques approfondies**	**S3**

Trois unités optionnelles proposées chaque année

Semestre : S3

Crédits : 8

Heures de cours : CM 26

But du cours : Maîtrise d'outils sophistiqués des mathématiques

Responsable : **LAGA**

Pré requis :

Contenu :
Ces enseignements dont le contenu sera élaboré chaque année nécessiteront un travail personnel important. Il s'agira de cours devant permettre à l'étudiant d'acquérir des outils sophistiqués des mathématiques portant sur les thèmes suivants :

- Arithmétique et géométrie algébrique
- Modélisation et calcul scientifique
- Physique mathématique et équations aux dérivées partielles
- Probabilités et statistiques
- Systèmes dynamiques
- Topologie algébrique

Spécialité :	**Mathématiques fondamentales et Protection de l'information**

Intitulé de l'UE :	**Cryptographie approfondie**	**S3**

UE commune avec la spécialité Algorithmique, Modélisation, Images

Semestre : S3

Crédits : 5

Heures de cours : CM 19,5 TD 19,5

But du cours : L'objectif du cours est d'une part d'approfondir les notions modernes de sécurité pour les algorithmes cryptographiques symétriques et asymétriques. D'autre part de donner aux étudiants une réelle expertise sur certains algorithmes cryptographiques et leur utilisation pour des applications réelles de l'industrie.

Responsable : **Philippe Guillot**

Pré requis : Cours de master 1 en cryptographie

Contenu :

- Générateur pseudo-aléatoire : lfsr, complexité linéaire, théorème de Blahut, combinaison de registres, borne de Key, définition trace des lfsr, registre filtré, principe des phases équidistantes, algorithme de Massey-Berlekamp.

- Courbes elliptiques : cryptographie dans un groupe, groupe des points d'une courbes elliptique, systèmes de coordonnées, méthodes de multiplication, forme non adjacente, suites de Lucas, anneau de coordonnées et fonctions rationnelles, ordre et pôles, diviseurs, couplage de Weil, isogénies, isogénie de Frobenius, théorème de Hasse, comptage des points, algorithme de Schoof, cryptographie bilinéaire et application au chiffrement avec l'identité.

- Théorie de l'information, entropie de Shannon, cryptographie parfaite, entropie de Renyi, distillation de secret et application à la cryptographie quantique.

Intitulé de l'UE :	**Preuves de sécurité**	**S3**

Semestre : S3

Crédits : 5

Heures de cours : CM 19,5 TD 19,5

But du cours : Les cryptosystèmes à nos jours s'accompagnent souvent des preuves de sécurité (en raison des attaques contre les schémas dans le passé). Les étudiants sont invités à étudier les formalisations des notions de sécurité et les techniques de preuves de sécurité pour la cryptographie symétrique et asymétrique.

Responsable : **Hieu Phan**

Pré requis : Introduction à la cryptographie ; Complexité algorithmique

Contenu :

1. Introduction à la cryptographie prouvable :
   - Preuve par réduction : réduire un problème interactif de sécurité à un problème statique d'algorithmique
   - Notions de sécurité : sécurité sémantique, non-malléabilité...
   - Modèles d'attaque : attaque à clairs choisis, à chiffrés choisis (non-)adaptatifs...

   - Relations entre les notions de sécurité et les modèles d'attaque

2. Preuves de sécurité en cryptographie symétrique :
   - Prédicat sûr ("hard-core predicate" en anglais) d'une fonction à sens unique : construction Goldreich-Levin
   - Générateur pseudo-aléatoire à partir des prédicats sûrs.
   - Fonction pseudo-aléatoire à partir des générateurs pseudo-aléatoires : construction Goldreich-Goldwasser-Micali
   - Permutation pseudo-aléatoire à partir des fonctions pseudo-aléatoires : construction Luby-Rackoff
   - Construction des chiffrements symétriques, codes d'authentification de message à partir des fonctions, permutations pseudo-aléatoires.
3. Preuves de sécurité en cryptographie asymétrique :
   - Chiffrement et signature dans le modèles d'oracle aléatoire : construction OAEP

- Chiffrement fondé sur des preuves non-intéractive à divulgation nulle de connaissance : construction de Naor-Yung
- Chiffrement Cramer-Shoup
- Signature RSA-PSS

Intitulé de l'UE :	Arithmétique algorithmique	S3

Semestre : S3

Crédits : 8

Heures de cours : CM 39 TD 19,5

But du cours : L'algèbre et l'arithmétique ont connu récemment des applications spectaculaires . Comment décomposer un nombre en facteurs premiers ? Comment reconnaitre qu'un nombre est premier ? C questions, revivifiées par l'existence des moyens modernes de calcul, se retrouvent aujourd'hui au cœur des procédés de cryptographie les plus récents.

L'objectif de ce cours est l'étude des procédés algorithmiques utilisés en cryptographie.

Responsable : **Philippe Guillot**

Pré requis : Connaissances classiques en arithmétique (primalité, etc) , en théorie élémentaires des anneaux commutatifs (divisibilité, etc) et corps finis. Connaissance élémentaire en algorithmique.

Contenu :

- Complexité algorithmique

- Multiplication rapide : méthodes d'interpolation (Karatsuba,Thoom-Cook), transformée de Fourier discrète, algorithme rapide.

- Division euclidienne rapide, réduction de Montgomery, itérations de Newton, racines carrées entières.

- Fractions continues, réduites, approximations diophantiennes.

- Primalité, témoin de Fermat, réciprocité quadratique, témoin de Miller.

- Racines carrées modulo p, théorème chinois, lemme de hensel, racines carrées modulo n

- Résolution de systèmes linéaires, pivot de Gauss, systèmes creux, calcul polynôme minimal d'un endomorphisme, algorithme de Wiedmann.

- Factorisation des polynômes : sur Fp, dans Q, borne de Mignotte-Landau.

- Factorisation des entiers exponentielle : algorithme de Fermat, rho de Pollard, méthode p-1.

- Logarithme discret générique : rho et lambda de Pollard, Pas-de-bébé-pas-de-géants.

- Crible quadratique, polynômes multiples, densité des nombres premiers, complexité sous-exponentielle du crible quadratique.

- Factorisation en temps polynomial sur calculateur abstrait (machine quantique ou analogique).

Spécialité :	**Mathématiques fondamentales et Protection de l'information**

Intitulé de l'UE :	**Sécurité et réseaux**	**S3**

Semestre : S3

Crédits : 5

Heures de cours : CM 19,5 TD 19,5

But du cours : Donner une vue d'ensemble de la sécurité des applications et de la sécurité des réseaux. On s'attachera à montrer l'importance et les limites de la cryptographie dans la sécurité en s'appuyant sur des exemples concrets empruntés aux monde des télécommunications.

Responsable : **David ARDITTI** (FranceTelecom R&D)

Intervenants : spécialistes du domaine choisis dans le laboratoire de sécurité de FranceTelecom R&D

Pré requis : De solides connaissances en cryptographie.

Contenu :

Introduction et concepts fondamentaux
- La confiance et les réseaux.
- Les briques de confiance.
- Notion d'identité.
- Protocoles d'authentification, de signature, de chiffrement.
- Comment lier identité et clé : diversification – certification.
- Schémas basés sur l'identité.
- Carte à puce et cryptographie.

Applications reposant sur de la cryptographie symétrique
- Ticket pré-payé.
- Télécarte 1G et 2G.
- La carte bancaire B0' – EMV.
- La sécurité des réseaux radio
- Le GSM et ses défauts.
- L'UMTS.
- Le WIFI et le WIMAX

Applications reposant sur de la cryptographie asymétrique
- Retour sur la certification.
- Les infrastructures à clé publiques.

- Applications des ICP :
- SSL, IPSEC
- Application de SSL au paiement sur internet
- Messagerie sécurisée (Un TP à faire chez soi par e-mail sera proposé aux élèves)
- Téléprocédures, courrier recommandé…

Spécialité :	**Mathématiques fondamentales et Protection de l'information**

Intitulé de l'UE :	**Programmation mathématique approfondie**	**S3**

UE mutualisée de la spécialité Algorithmique, Modélisation, Images

Semestre : S3

Crédits : 5

Heures de cours : CM 19,5 TD 19,5

But du cours : Étudier et fournir les outils de la programmation mathématique nécessaires à la modélisation, à la formalisation et à la résolution algorithmique de problèmes d'optimisation combinatoire difficiles.

Responsable : **Lucas Létocart**

Intervenants : Sylvie Borne, Lucas Létocart, Anass Nagih

Pré requis : Programmation linéaire continue et entière

Contenu :

1. Méthodes de décomposition et génération de colonnes

2. Approches polyédrales

3. Programmation non linéaire, relaxation semi-définie et convexification

4. Applications pour des problèmes de planification en transport, de routage et de fiabilité dans les réseaux, ...

Intitulé de l'UE :	**Structures de Calcul II (calcul exact et approché)**	**S3**

UE mutualisée de la spécialité Algorithmique, Modélisation, Images

Semestre : S3

Crédits : 5

Heures de cours : CM 19,5 TD 19,5

But du cours : Ce cours fournit les différentes méthodes modernes de codage et de calcul de structures complexes en machine (par exemple les différentes façons de représenter – de façon exacte – l'infini en machine, quand c'est possible). Il pose aussi la question des deux sortes d'approximation ; par troncature (inductive) et par une ou des équivalences (projectives). Ce dernier cadre fournit également un lien avec la cryptographie. La partie centrale est constituée par la théorie moderne des automates (à multiplicités) qui englobe la théorie classique (booléenne) et des modèles comme les automates stochastiques et les transducteurs. Au passage ce cours fournit un solide bagage en algorithmique.

Responsable : **Gérard H. E. Duchamp**

Pré requis : Graphes, matrices

Contenu :

1. Codage des développements infinis en machine (boucles, rationalité, périodicité et pseudo-périodicité), applications aux générateurs de nombres aléatoires.

2. Automates et rationalité des fonctions sur les mots : séries génératrices à plusieurs variables noncommutatives, lien avec la théorie des langages, la réduction des BDD (Binary Decision Diagrams) et des fonctions booléennes.

3. Application de la variation de coefficients : recherche de plus court chemin dans un graphe avec listes d'adresses, modélisation de stratégies humaines, systèmes complexes.

4. Approximations : par troncature, modulo une ou des équivalences

5. Réduction et réécriture de termes.

Spécialité :	Mathématiques fondamentales et Protection de l'information

Intitulé de l'UE :	Représentation des images et ondelettes	S3

UE de la spécialité Algorithmique, Modélisation, Images

Semestre : S3

Crédits : 5

Heures de cours : CM 19,5 TD 19,5

But du cours : Donner les principales méthodes de représentation des images avec applications à la compression, au filtrage et à l'analyse d'images.

Responsable : **François Malgouyres**

Pré requis : Algèbre linéaire. Souhaité : analyse de Fourier

Contenu :

Rappels : Base et transformée de Fourier discrète : inversion de la transformée de Fourier, Fourier et convolution, Fourier et échantillonage, application au debruitage, au zoom et au filtrage d'images.

Base de cosinus locaux (JPEG),

Bases d'ondelettes : banques de filtres, ondelettes orthogonales et bi-orthogonales, applications au debruitage et a la compression d'images.

Bases de paquets d'ondelettes : construction, localisation fréquentielle des paquets d'ondelettes, application à la déconvolution d'images.

Introduction à la représentation dans un système redondant : indetermination des coordonnées, introduction des représentations parcimonieuses.

Les algorithmes gloutons : Matching Pursuit, Orthogonal Matching Pursuit, application en compression et analyse d'images. Les algorithmes d'optimisation (Basis Pursuit): le seuillage iteratif, application en analyse d'images.

Intitulé de l'UE :	Culture générale	S3

Semestre : S3, obligatoire

Crédits : 4

Anglais

Heures de cours : CM et TD 19,5

Responsable : **Gary Grill, Monique Nicolas, Edith Patrouilleau**

Contenu :

Les supports oraux et écrits sont orientés autour de trois axes :

- Les compétences de communication liées à l'emploi : savoir-faire et compétences répondant à la recherche de stage (CV, lettre de motivation, simulations d'entretiens d'embauche)

- Les compétences de communication liées à la vie universitaire et la recherche : production d'écrits et de présentations orales (résumés de conférences, rédactions d'articles courts, "abstracts", présentations orales de travaux)

- Une approche interculturelle sensibilise l'étudiant à une perspective d'échanges et d'insertion professionnelle dans des équipes multilingues.

Histoire des sciences : Histoire de la cryptologie

Heures de cours : CM 19,5

Responsable : **Marie-José Durand-Richard**

Contenu

Cette histoire tendra à éviter l'approche rétro-historique pour lui préférer une approche contextuelle. Elle permettra de poser la question de la théorisation de l'activité mathématique, des pratiques matérielles à l'écriture mathématique, et des transferts de signification lors de la transmission des connaissances entre différents lieux.

Principaux thèmes abordés

• Interactions entre linguistique, algèbre et cryptologie dans la phase de symbolisation de l'algèbre

• La cryptanalyse par l'analyse des fréquences dans le contexte arabe :

• Complexification du codage : chiffrement polyalphabétique

• Impact de la cryptanalyse sur la symbolisation de l'algèbre

• L'arrière-plan des Disquisitiones Arithmeticæ (1801) de Carl Gauss (1777-1855), du déchiffrement du code de Vigenère par Charles Babbage (1791-1871) aux tests de primalité d' Edouard Lucas (1842-91).

• Mécanisation du calcul et des systèmes de transmission : naissance d'une conception systémique du problème cryptologique de Kerckhoffs à W. Friedmann (1891-1969)

• De l'analyse des fréquences à l'indice de coincidence

• Cryptologie et structures algébriques de Lester S. Hill (1890-1961)

• De la cryptologie à l'information : Claude Shannon (1916-2001).

• L'informatique et les mutations de la cryptologie

• De la Guerre Froide à l'envahissement de la société civile par la cryptologie

• De la clé secrète à la clé publique : du DES au RSA.