الـجـزائـريـة الـديـمـقـراطـيـة الـشـعـبـيـة الـجـمـهـوريـة
REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

Faculté : ***Mathématiques***

Département : ***Algèbre***

Laboratoire : ***Algèbre et Théorie des Nombres***

Offre de formation L.M.D.

LICENCE ACADEMIQUE

« Algèbre et cryptographie »

Année universitaire 2009-2010

A - Objectifs de la formation

La licence « Algèbre et Cryptographie » est une formation universitaire dont le but est d'acquérir les bases des mathématiques. Par le biais de ses unités d'enseignements variées, le parcours proposé permet soit une insertion professionnelle à l'issue de la licence, soit une poursuite d'études en Master.

Les orientations principales souhaitées pour cette licence sont les domaines des mathématiques ou de l'algorithmique qui interviennent, entre autre, dans la théorie des codes et la cryptographie. Ces choix se reflètent dans les programmes de la licence. En plus d'une importante composante informatique liée à la pratique des machines et des langages de programmation C et C++, ce parcours comporte une partie mathématique permettant une double compétence, à la fois très appréciée des entreprises et ouvrant largement les possibilités de poursuite d'études. Une partie importante de ces mathématiques est tournée vers les applications qui interviennent dans les nouvelles technologies, plus précisément la théorie des codes correcteurs et la cryptographie.

Précisons cependant que nous ne visons pas seulement les théorèmes mathématiques "utiles" par leurs applications actuelles, mais qu'il s'agit de donner aux étudiants une culture solide et durable afin qu'ils puissent observer les domaines mathématiques étudiés d'une hauteur suffisante à la poursuite de leurs études en Master de mathématiques et propre à leur assurer, à long terme, une capacité d'adaptation à l'évolution des théories mathématiques et des technologies de l'information.

B – Profils et compétences visées

Les diplômés maîtriseront les savoirs disciplinaires : algèbre, arithmétique, calcul différentiel et intégral, théorie de la mesure, géométrie, probabilités, analyse complexe, langages C et C++, architecture d'un processeur et structures des données des systèmes d'exploitation, algorithmique, complexité, codage, cryptographie et le LaTeX.
Ils auront également acquis la rigueur du raisonnement mathématique et des capacités d'analyse et de synthèse. Ils sauront mobiliser leur connaissance des théories mathématiques dans la résolution de problèmes purement mathématiques ou posés par d'autres sciences.

La licence « Algèbre et Cryptographie » prépare à une carrière scientifique dans les entreprises (banques, recherche et développement, production, études et conseils, cryptographie), dans l'administration (impôts, douanes...), les institutions étatiques spécialisées dans les télécommunications (Algérie Télécom) et la sécurité des télécommunications (services de sécurité) ainsi qu'aux métiers de l'enseignement et de la recherche.

Cette licence offre des poursuites d'études dans une large palette de masters de mathématiques pures ou appliquées : Cryptographie, Théorie des nombres, Géométrie Algébrique, Géométrie différentielle, Analyse.

C – Potentialités régionales et nationales d'employabilité

Pour la première fois en Algérie, avec la licence « Algèbre et Cryptographie », une formation universitaire en cryptographie sera proposée. Les étudiants ayant choisi ce parcours pourront apprendre différentes techniques de cryptage et de cryptanalyse basées sur des outils mathématiques assez avancés comme les corps finis (cryptosystème AES) et l'arithmétique (cryptosystème RSA).
Par le biais de ses unités d'enseignements variées, la licence « Algèbre et Cryptographie » permet soit une insertion professionnelle dans des institutions chargées du traitement et de la protection de l'information tels que le développement de transactions sécurisées sur Internet ou de protection de réseaux informatique des entreprises et administrations (banques, Algérie Télécom, services de sécurité…), soit une poursuite d'études en Master de cryptographie suivie d'une carrière académique de chercheur en cryptographie.

D – Passerelles vers les autres spécialités

- Licences en mathématiques (académiques et professionnelles)
- Licence en Informatique
- Licence en Technologie
- Masters en mathématiques

E – Moyens humains disponibles : Capacité d'encadrement : 30

Nom, prénoms	Grade	Matière enseignée
BENZAGHOU Benali	**Prof**	**Anneaux et extensions de corps**
BETINA Kamel	**Prof**	**Introduction à LaTeX, Cryptographie**
KESSI Arezki	**Prof**	**Mesure et intégration**
HACHAÏCHI Med Salah	**MC (A)**	**Analyse complexe**
HERNANE M.O	**MC (A)**	**Arithmétique**
REZAOUI Med Salem	**MC (A)**	**Intégrales et séries numériques**
BEHLOUL Djilali	**MC (A)**	**Algorithmique arithmétique**
LAOUDI Aini	**MC (A)**	**Algèbre et géométrie**
BENCHERIF Farid	**MC (A)**	**Algèbre linéaire**
ABBACI Brahim	**MC (B)**	**Fonctions de plusieurs variables**
AIT AMRANE Yacine	**MC (B)**	**Topologie**
MESSACI Rabah	**MA (A)**	**Probabilités**
IDRIS BEY Amar	**MA (A)**	**Géométrie**
BELLAGH abdelaziz	**MA (A)**	**Corps et polynômes**
Mme CHERCHEM Leila	**MA (A)**	**Groupes et anneaux**
GARICI Tarek	**MA (A)**	**Programmation en langage C, Calcul formel**
BOUCHENNA Rachid	**MA (A)**	**Séries de fonctions**
CHERCHEM Ahmed	**MA (A)**	**Algèbre et codage**

Organisation semestrielle des enseignements

Semestre 1	Cours	TD	TP	Crédits
UE Fondamentale				
Algèbre 1	1 h 30	1 h 30	00	4
Analyse 2	3 h	3 h	00	6
Algorithmique 1	3 h	1 h 30	1 h 30	6
UE Méthodologie				
Bureautique	00	00	1 h 30	2.5
TEC 1	00	1 h 30	00	2.5
UE Découverte				
Mécanique du point	1 h 30	1 h 30	00	4
Histoire des sciences	1 h 30	00	00	2.5
Cours optionnel	1 h 30	00	00	2.5

Semestre 2	C	TD	TP	Crédits
UE Fondamentale 1				
Algèbre 2	1 h 30	1 h 30	00	4
Analyse 2	1 h 30	1 h 30	00	4
Statistique descriptive	1 h 30	1 h 30	00	4
UE Fondamentale 2				
Programmation fonctionnelle	1 h 30	00	1 h 30	3
Structure machine	1 h 30	1 h 30	00	3
Algorithmique 2	1 h 30	1 h 30	1 h 30	6
UE Découverte				
Electricité	1 h 30	1 h 30	00	3
UE Culture générale				
TEC 2	1 h 30	00	1 h 30	1.5
Technologie WEB	00	00	1 h 30	1.5

SEMESTRE 3	C	TD	TP	Crédits
UE Fondamentale 1				
Algèbre linéaire	1 h 30	3 h	00	6
Groupes et anneaux	1 h 30	3 h	00	6
UE Fondamentale 2				
Intégrales et séries numériques	1 h 30	3 h	00	6
Géométrie	1 h 30	3 h	00	6
UE Méthodologie				
Architecture et systèmes	1 h 30	1 h 30	00	4
Programmation en langage C	00	00	1 h 30	2

SEMESTRE 4	C	TD	TP	Crédits

UE Fondamentale 1				
Corps et polynômes	1 h 30	3 h	00	6
Algèbre et géométrie	1 h 30	3 h	00	6
UE Fondamentale 2				
Séries de fonctions	1 h 30	3 h	00	6
Topologie	1 h 30	3 h	00	6
UE Méthodologie				
Algorithmique arithmétique	1 h 30	1 h 30	00	4
Introduction à LaTeX	00	00	1 h 30	2

SEMESTRE 5	C	TD	TP	Crédits
UE Fondamentale 1				
Arithmétique	1 h 30	3 h	00	6
Algèbre et codage	1 h 30	1 h 30	1 h 30	6
UE Fondamentale 2				
Fonctions de plusieurs variables	1 h 30	3 h	00	6
Mesure et intégration	3 h	3 h	00	6
UE Méthodologie				
Langage C++	1 h 30	00	1 h 30	4
Anglais scientifique	1 h 30	00	00	2

SEMESTRE 6	C	TD	TP	Crédits
UEF1(O/P)				
Anneaux et extensions de corps	1 h 30	3 h	00	6
Cryptographie	1 h 30	1 h 30	1 h 30	6
UEF2(O/P)				
Analyse complexe	1 h 30	3 h	00	6
Probabilités	1 h 30	3 h	00	6
UEM1(O/P)				
Calcul formel	1 h 30		1 h 30	3
UED1(O/P)				
Mini projet	00	00	00	3

Contenu des cours

Algèbre linéaire : Rang d'une matrice. Déterminants. Applications linéaires. Représentation matricielle, changement de bases.
Réduction des matrices et des endomorphismes : valeurs et vecteurs propres, polynôme caractéristique, polynôme minimal, diagonalisation, trigonalisation. Application.

Groupes et anneaux : Groupes : sous-groupes, théorème de Lagrange, intersection de sous-groupes, générateurs, sous-groupe cycliques, sous-groupes de type fini. Sous-groupes normaux, groupes quotients, exemples de groupes (groupe symétrique, groupes abéliens de type fini). Homomorphisme de groupes. Automorphismes intérieurs. Centre d'un groupe. Groupe opérant dans un ensemble. Stabilisateur. Classes de conjugaison. Equation des classes. Théorèmes de Sylow. Anneau, homomorphisme d'anneaux, idéal d'un anneau, anneau quotient. Etude de l'anneau Z : division euclidienne, idéaux de Z, pgcd et ppcm, calcul du PGCD et de coefficients de Bézout dans Z. Le théorème fondamental de l'arithmétique. L'anneau Z/nZ.

Intégrales et séries numériques : Intégrales impropres, intégrales dépendant d'un paramètre, fonctions définies par une intégrale, exemple : étude de la fonction Gamma. Séries numériques. Transformation d'Abel.

Géométrie : Géométries vectorielle et affine en dimension 3. Barycentres, repères affines. Projections et symétries. Perpendiculaire commune à 2 droites. Distance d'un point à un plan ou à une droite. Courbes paramétrées, courbes en coordonnées polaires. Abscisse curviligne, longueur d'un arc. Surfaces paramétrées : exemples.

Architecture et systèmes : Connaissances de base en architecture et architecture fonctionnelle d'un processeur (central et/ou vidéo) : pipelining, architectures super-scalaire, vectorielle. Mémoire et stratégies de cache.
Algorithmique et structures de données des systèmes d'exploitation : système de fichiers, gestion des processus, partage de ressource et synchronisation.

Programmation en langage C : Cet enseignement est une introduction au langage le plus répandu actuellement, le langage C. Seront abordés les types, les expressions, les structures de contrôle, les fonctions et leurs modes de passages de paramètres. Les exemples, applications et TP seront orientés vers l'algèbre et l'arithmétique.

Corps et polynômes : Corps, caractéristique d'un corps, corps finis, Frobenius, existence de corps finis, éléments primitifs.
Etude de l'anneau K[x] des polynômes à une indéterminée à coefficients dans un corps commutatif : algorithme d'Euclide, théorème de Bezout, théorème de Gauss, idéaux de K[x], pgcd, ppcm, polynômes irréductibles. Cas particuliers : K=C, K=R, K=Q (on énoncera le théorème fondamental de l'algèbre).
Cas où le corps K est fini : polynôme minimal d'un élément x, corps de rupture. Calcul dans K[t]/(f) où f est un polynôme irréductible, calcul dans Fq, où q est une puissance d'un nombre premier. Application à la cryptographie : le système AES.

Algèbre et géométrie : Espaces euclidiens, dualité, formes quadratiques, orthogonalité. Bases orthogonales. Endomorphismes orthogonaux, matrices orthogonales. Réduction des matrices symétriques. Isométries.

Séries de fonctions : Suites et séries de fonctions. Convergence uniforme. Dérivation d'une série de fonctions. Espaces vectoriels hermitiens. Séries de Fourier. Séries entières, application aux équations différentielles.

Topologie : Espaces topologiques, exemples : espaces métriques, espaces vectoriels normés. Voisinages, adhérence, intérieur, topologie induite, topologie produit. Applications continues, homéomorphismes. Topologie quotient. Compacité. Connexité. Espaces métriques complets. Norme d'une application linéaire continue. Espace de Banach.

Algorithmique arithmétique : Notions générales. Algorithmes. Complexité. Listes à la caml. Liste tableaux. Tris simples, tri rapide, tri par tas. Arbres, arbres binaires de recherche. Programmation dynamique.
Théorie de la complexité : Machines de Turing déterministes. Indécidabilité - Ensembles décidables et récursivement énumérables. Machines de Turing non déterministes. Les exemples, applications et TD seront orientés vers l'arithmétique et la cryptographie.

Introduction à LaTeX : LaTeX est un système de traitement de texte très puissant servant mettre en forme et mettre en page, utile dans de nombreux domaines (littérature, textes scientifiques, etc.). Il est particulièrement adapté à l'écriture des symboles mathématiques et est utilisé dans la plupart des revues scientifiques. Le logiciel LaTeX appartient au monde du logiciel libre.

Arithmétique : Division euclidienne, calcul du PGCD et de coefficients de Bézout dans Z. Le théorème fondamental de l'arithmétique. Congruences : le théorème des restes " chinois ", résolution de systèmes, calcul modulaire. Le petit théorème de Fermat, la fonction d'Euler. Groupe multiplicatif du corps premier, multiplication dans les entiers modulo n.
La loi de réciprocité quadratique, symboles de Legendre et de Jacobi. Nombres premiers : les nombres de Fermat et de Mersenne, aperçus sur les tests de primalité, absolus ou probabilistes. Les nombres de Fermat et de Mersenne (test de Lucas). La fonction de densité (théorème de Chebychev). Application en cryptographie : le système RSA.
On présentera aussi les algorithmes de calcul et on utilisera des logiciels comme Maple.

Algèbre et codage : Codes détecteurs d'erreurs et codes correcteurs d'erreurs: généralités. Codes linéaires. Matrices génératrices et de parité. Décodage général des codes linéaires. Codes cycliques. Décodage général des codes cycliques. Principales classes de codes linéaires (Hamming, Reed-Muller, BCH, Reed-Solomon ...) et non-linéaires (Kerdock, Preparata). Décodages spécifiques de ces codes. Code de Goppa.
Mise en œuvre en Maple du codage et du décodage sur des exemples.

Fonctions de plusieurs variables : Fonctions de plusieurs variables : continuité, différentiabilité, gradient, formule de Taylor. Inversion locale. Fonctions implicites. Extrema, extrema liés.
Intégrales doubles et triples, intégrales curvilignes, intégrales de surfaces. Formules de Stokes, d'Ostrogradsky et de Green-Riemann (sans démonstration).
Equations différentielles y'=f(x,y). Théorème d'existence et d'unicité de Cauchy.

Mesure et intégration : Introduction à la théorie de la mesure et de l'intégration. Intégrale de Lebesgue. Convergences monotone et dominée. Intégrales dépendant d'un paramètre. Théorème de Fubini.

Programmation en langage C++ : Cet enseignement vise à présenter les principes et les concepts de la programmation. L'objectif du cours est de former les étudiants à la programmation orientée objets à l'aide du langage C++. Les exemples, applications et TP seront orientés vers l'algèbre et l'arithmétique.

Anneaux et extensions de corps : Anneaux noethériens, théorème de Hilbert. Propriétés arithmétiques des anneaux. Anneaux euclidiens, anneaux factoriels, anneaux principaux. Théorème de Gauss. Exemples. Extensions de corps : extensions finies, extensions algébriques. Construction à la règle et au compas. Corps de rupture, corps de décomposition, exemples. Extensions des corps finis. Irréductibilité des polynômes de K[x], où K est un corps. Cyclotomie.

Cryptographie : Chiffrement, cryptographie à clé secrète: schémas par blocs (présentation du DES et de l'AES). Cryptographie à clé publique : RSA, Diffie-Hellman, El Gamal. Définition d'une courbe elliptique sur un corps, loi de groupe, cryptosystèmes sur les courbes elliptiques sur un corps fini. Authentification, signature, fonctions de hachage. Les TD porteront en partie sur la cryptanalyse.

Analyse complexe : Fonctions analytiques. Principe des zéros isolés. Principe du maximum. Fonctions holomorphes. Théorème et formule de Cauchy. Théorème et calcul des résidus. Suites de fonctions analytiques. Théorème de Rouché. Théorème d'inversion locale, théorème d'inversion globale. Séries de fonctions holomorphes, produits infinis de fonctions holomorphes, séries de fonctions méromorphes, exemples.

Probabilités : Probabilités élémentaires : événements, indépendance, variables aléatoires, espérance, variance. Vecteurs aléatoires. Conditionnement élémentaire. Lois. Lois usuelles. Indépendance, corrélation de 2 variables aléatoires.
Loi des grands nombres, et énoncé du théorème limite central.

Calcul formel : Illustrations des enseignements d'algèbre, d'arithmétique et de cryptographie à l'aide d'un logiciel de calcul formel comme Maple ou Magma.

Stage pratique : Il s'agit de rédiger un mémoire scientifique sous la direction d'un membre de l'équipe pédagogique de la licence « Algèbre et cryptographie ».