2EL1740 - Algèbre et cryptologie

Responsables : **Remi GERAUD**

Département de rattachement : **DÉPARTEMENT MATHÉMATIQUES**

Langues d'enseignement : **FRANCAIS**

Type de cours : **Electif 2A**

Campus où le cours est proposé : **CAMPUS DE PARIS - SACLAY**

Nombre d'heures d'études élèves (HEE) : **60**

Nombre d'heures présentielles d'enseignement (HPE) : **30**

Année académique : **2024-2025**

Catégorie d'électif : **Sciences fondamentales**

Niveau avancé : **non**

Présentation, objectifs généraux du cours :

Ce cours est une introduction aux outils mathématiques modernes, et leur matérialisation en applications technologiques et scientifiques.

À la croisée des mathématiques fondamentales, de l'informatique et de la théorie de l'information, nous aborderons des questions telles que

- Comment envoyer un message depuis une sonde spatiale ?
- Comment garantir l'authenticité d'un document numérique ?
- Comment trouver de très grands nombres premiers ? Ou factoriser de grands nombres ?
- et beaucoup d'autres

Le thème directeur de notre exploration sera la théorie du logarithme discret et des réseaux euclidiens, qui sous-tend une immense partie des concepts cryptologiques des 20e et 21e siècles et croise de nombreuses questions fondamentales de mathématiques.

L'objectif de ce cours est de doter les étudiants :

- D'un bagage culturel sur le développement des mathématiques au 20e et 21e siècle, avec un langage qui leur permettra d'approfondir ces questions
- D'une maîtrise opérationnelle du calcul dans les structures algébriques, en particulier anneaux, corps finis et courbes elliptiques
- D'une compréhension des fondements mathématiques de la cryptologie moderne

Période(s) du cours (n° de séquence ou hors séquence) :

SG8

Prérequis :

Ce cours ne suppose pas de connaissances spécifiques au-delà de notions mathématiques générales normalement acquises en classes préparatoires.

Une familiarité avec la programmation informatique est fortement recommandée.

Attention, **ce cours demande un travail sérieux et conséquent**, pour assimiler et s'approprier les notions discutées.

Plan détaillé du cours (contenu) :

- En 2023 le cours détaillait notamment les points suivants :

- Applications des groupes cycliques [Diffie-Hellman'76, Schnorr'89, ElGamal'85]
- Constructions élémentaires sur les corps finis [Reed-Solomon'60, Shamir'79, Toom-Cook-66]
- Outils arithmétiques élémentaires [Miller-Rabin'80, Pollard'74, Dixon'81]
- Groupe de Picard des anneaux de Dedekind et des variétés projectives lisses
- Réduction de réseaux et applications [LLL''82, Lagarias-Odlyzo'85, Wiener'02, Coppersmith'96]
- Courbes elliptiques sur les corps finis et applications [Lenstra'85, Koblitz-Miller'86, NIST'05]
- Apprentissage avec erreurs et applications [Regev'05, Dilithium'22]

Déroulement, organisation du cours :

- Les cours sont présentés au tableau
- Des notes de cours, reprenant les éléments importants, sont fournies après les séances
- Des exemples commentés de calcul formel sont mis à disposition
- Les TDs prennent la forme d'une application détaillée des notions acquises et permet de les mettre en contexte et d'en discuter les spécificités ou les limites
- Un contrôle continu permet de s'approprier les notions importantes du cours et de les mettre en œuvre

Organisation de l'évaluation :

- Contrôle continu

Moyens :

- Cours magistral au tableau, certains exercices nécessitent l'utilisation de l'ordinateur. Le cas échéant on précisera les logiciels à installer.

Equipe enseignante : Rémi Géraud-Stewart (remi.geraud@ens.fr)

Acquis d'apprentissage visés dans le cours :

A la fin de ce cours, les élèves seront capables de :

- Identifier les structures algébriques manifestes dans les problèmes rencontrés
- Comprendre les enjeux et les outils de la cryptologie et de la théorie des codes, et (re)connaître leurs principales applications industrielles
- Maîtriser le langage dans lequel sont formulés et analysés les problèmes algébriques

Description des compétences acquises à l'issue du cours :

- 1. Recognise the presence of underlying algebraic structures in engineering problems

- C.1.2 : identify the structures that were discussed during lectures
- C.6.1 : invoke the relevant technological tools

2. Understand the issues addressed by cryptology and code theory, know and recognise their leading industrial applications

- C.6.7 : understand the technical aspects and difficulties related to communication and information transfer
- C.3.6 : evaluate technical solutions against specific needs and constraints
- C.6.1 and C.1.4 : introduce relevant tools and correct configurations

3. Master the mathematical language in which algebraic questions are formulated and analysed.

- C.2.3 : practice acquiring new skills to approach a given problem

Bibliographie :

- David Eisenbud, Commutative Algebra (with a View Toward Algebraic Geometry)
- Robin Hartshorne, Algebraic Geometry
- William Fulton, Algebraic curves: An Introduction to Algebraic Geometry
- Henning Stichtenoth, Algebraic Function Fields and Codes
- Michel Demazure, Cours d'algèbre
- Joseph H. Silverman, The Arithmetic of Elliptic Curves
- Joseph H. Silverman, Advanced Topics in the Arithmetic of Elliptic Curves
- Jean-Pierre Serre, Cours d'arithmétique
- Michael Tsfasman, Serge Vlăduţ, Dmitry Nogin, Algebraic Geometric Codes: Basic Notions