MA2825 Algèbre et cryptologie

Responsable : Remi GERAUD

Langue d'enseignement : FRANCAIS – **Heures** : 36 – **ECTS** : 3,0 - **Quota** :

Prérequis : Algèbre et informatique de base (L3)

Période : S8 électif 12 entre février et juin

Objectifs

Ce cours théorique vise à présenter des concepts et outils fondamentaux d'algèbre commutative via le prisme de la cryptologie moderne. En particulier, sont introduits certains éléments de théorie des nombres (corps finis, loi de réciprocité quadratique, courbes elliptiques).

La cryptographie est un ensemble de techniques qui permettent d'assurer la sécurité des systèmes d'information. Cette discipline, à la frontière des mathématiques, de l'informatique et de l'électronique, permet notamment de conserver aux données leur caractère confidentiel, de contrôler leur accès ou d'identifier des documents.

Parallèlement aux concepts mathématiques fondamentaux, ce cours introduira les outils algorithmiques et informatiques nécessaires aux applications. Il se propose de présenter les notions de base d'algèbre et d'étudier en détail certaines structures algébriques utiles pour la cryptologie à clé publique (anneaux finis et de polynômes, corps finis, ...). Il abordera également des notions de théorie algorithmique des nombres, avec pour objectifs certaines applications récentes à la cryptologie.

Compétences acquises en fin de cours

Outre les éléments de base de la cryptologie moderne, ce cours apportera aux étudiants une culture solide en algèbre et théorie des nombres. Il constitue un fondement important pour les étudiants souhaitant poursuivre un Master 2 dans ce domaine. Au-delà, ce cours offre une vue plus large des mathématiques modernes, qui sera utile aux étudiants souhaitant poursuivre leurs études dans d'autres directions.

Contenu

- Groupes, anneaux, corps, corps finis. Idéaux et spectres.
- Résidus et réciprocité quadratique, symboles, caractères.
- Algorithmes sur les corps finis, tests de primalité, factorisation.
- Courbes elliptiques sur les corps finis.
- Applications : codes correcteurs d'erreurs, schémas de signature numérique, protocoles d'identification à divulgation nulle de connaissance, chiffrement à clé publique, échange de clés.

Organisation du cours

Cours 22h, TD 9.5h.

Bibliographie / supports

Notes de cours, exercices, corrections, annales, et bibliographie fournie.

Évaluation

Contrôle Intermédiaire Obligatoire 1h30 sans document + Contrôle Final Obligatoire écrit 3h sans document.