Cryptographie Avancée (40 h, 6 ECTS)

Enseignant : Prof. D. Tieudjo

Objectifs

Ce cours a pour buts d'étudier les nouveaux objets algébriques, géométriques et physiques, utilisés dans la cryptographie contemporaine. Les concepts de base et les ouvertures de recherche sont présentés. A l'issue de ce cours, un étudiant pourra choisir un domaine de recherche et s'y lancer.

Plan du cours pour 2011

Ce cours est divisé en 4 (quatre) parties. Chaque partie sera assurée par un enseignant différent.

1ère Partie : Cryptographie sur les courbes elliptiques
2ème Partie : Cryptographie basée sur la théorie combinatoire des groupes. La cryptographie sur les groupes des tresses occupe une bonne partie
3ème Partie : Les codes détecteurs/correcteurs d'erreurs, codage et applications à la cryptographie.
4ème partie : La cryptographie du futur. Ici on examinera la cryptographie quantique et d'autres techniques du futur.

Pré-requis

Cryptographie algébrique

Langue

Le cours est donné en français. Des documents en anglais sont disponibles.

Bibliographie

- P. Dehornoy, *Braid-based cryptography*, Contemp. Math, 360, (2004), 5-33.
- D. Garber, *Braid group cryptography*, arXiv:0711.3941v2, (2009)
- Y. Deneulin et *al.*, *Théorie des codes : Compression, Cryptage, Correction*, Support de cours (2005)
- M. Hedabou, *Amélioration et sécurisation des calculs arithmétiques pour la cryptographie basée sur les courbes elliptiques*, Thèse de Doctorat, Institut National des Sciences Appliquées de Toulouse (2006) (1ère partie surtout).