Faculté des Sciences & Techniques
Département de Mathématiques

Année 2017-2018

Master 1- Cryptis
Projet d'Initiation à la Recherche

Applications de la représentation matricielle des corps finis

En considérant la représentation matricielle des éléments d'un corps fini, Kern et Mignotte donnent dans ([3]) un algorithme rapide de résolution de l'équation $x^d = a$ dans un corps fini ainsi qu'une application à la décomposition d'un idéal dans un corps de nombres.

Travail à faire

Il s'agit d'abord de faire le point sur les méthodes de résolution de l'équation $x^d = a$ sur un corps fini. Ensuite, lire et détailler l'article de Kern et Mignotte ([3]). Une dernière partie consistera à étudier les différents algorithmes et les mettre en œuvre.

Références

[1] H. Cohen, *A Course in Computational Algebraic Number Theory*, Springer, Berlin, 1996.

[2] M. Mignotte, *Un algorithme sur la décomposition des polynômes dans un corps fini,* C. R. Acad. Sci. Paris Ser. A (1975), p. 137–139

[3] E. Kern, M. Mignotte, *Applications of the representation of finite fields by matrices,* Theoritical Computer Science 244 (2000), p. 263–265.

Contact : anec@unilim.fr