Mémoire de Master 1

L'étude du Cryptosystème NTRU

Le cryptosystème NTRU est défini à l'aide des opérations dans l'anneau des polynômes tronqués $\mathbb{Z}[X]/(X^n - 1)$ à coefficients entiers et ses réductions modulo un nombre premier. C'est l'un des rares qui a résisté aux différentes attques (à part RSA et ceux basés sur le problème du logrithme discret) et dont la mise en application est plus efficace.

Ce mémoire consiste en l'étude de NTRU, la mise en évidence que le problème mathématique difficile protégeant le système est le problème de recherche du plus petit vecteur dans un réseau et ses variantes, l'algorithme LLL qui trouve un tel vecteur etc...