Factorisation d'entiers

Stéphane Horte & Gabriel Lewertowski

16 mars 2014

Table des matières

Résumé

Nous présentons trois algorithmes de factorisation d'entiers : les algorithmes ρ et $(p-1)$ proposés par J.M Pollard en 1974 dans [1] ainsi que l'algorithme *ECM* (Elliptic Curve Method) décrit par H. W. Lenstra, Jr dans [2]. Nous testons ensuite nos implémentations sur des grands nombres choisis aléatoirement, et nous comparons avec les résultats obtenus par GMP-ECM.

Références

[1] J. M. Pollard, *A Monte Carlo method for factorization*, BIT, 1975, pp.331-334

[2] H. W. Lenstra, Jr, *Factoring integers with elliptic curves*, Annals of Mathematics, 1987, pp.649-673