Exercices et problèmes de cryptographie

Damien Vergnaud

Exercice complémentaire n° 6.13 (bis)

Exercice 6.13 (bis) FACTORISATION PAR LA MÉTHODE DE FERMAT

Factoriser l'entier

$$n = 106163123228701487539039766979786766546058330689245227481412 63$$

par la méthode $p - 1$ de Pollard.

Solution : L'application directe de la méthode $p-1$ de Pollard révèle immédiatement que $n = pq$ avec

$$\begin{aligned} p &= 149578066871199624632224690588 7 \\ q &= 709750603476628907661539855444 9 \end{aligned}$$

où p et q sont des nombres premiers (comme on peut le vérifier facilement en appliquant le test de primalité de Miller-Rabin par exemple) avec $q - 1 = 2^4 \cdot 47^2 \cdot 83^2 \cdot 179^2 \cdot 467^2 \cdot 983 \cdot 1619^3$. □