Exercices et problèmes de cryptographie

Damien Vergnaud

Exercice complémentaire n° 6.10 (bis)

Exercice 6.10 (bis) FACTORISATION PAR LA MÉTHODE DE FERMAT

Factoriser l'entier

$$n = 611902125534358514566889258476973437333826470340870589224315 9$$

par la méthode de Fermat.

Solution : L'application directe de la méthode de Fermat révèle immédiatement que $n = pq$ avec

$$\begin{aligned} p &= 247366555042179967406890911638 3 \\ q &= 247366555042179967406890911847 3 \end{aligned}$$

avec $|p-q| = 2090$ et p et q sont des nombres premiers (comme on peut le vérifier facilement en appliquant le test de primalité de Miller-Rabin par exemple). □