Exercices et problèmes de cryptographie

Damien Vergnaud

Exercice complémentaire n° 6.9 (bis)

Exercice 6.9 (bis) FACTORISATION PAR DIVISIONS SUCCESSIVES

Factoriser l'entier

$$n = 272356067011053460225277256572896131652284755763273986441396458998 1$$

par divisions successives.

Solution : L'application directe des divisions successives montre que $n = pq$ avec

$$\begin{aligned} p &= 185152423251018849453241306373286524488919828280322740943570 7 \\ q &= 1470983 \end{aligned}$$

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). □