Exercices et problèmes de cryptographie

Damien Vergnaud

Exercice complémentaire n° 7.9 (bis)

Exercice 7.9 (bis)
Utiliser la méthode de l'exercice 7.9 pour retrouver le message m vérifiant $c = m^{17} \bmod N$ et $c' = (m+1)^{17} \bmod N$ avec

$$
\begin{aligned}
N &= 337243323462507588094544391222420349925602372206389211874759 9 \\
c &= 138477232122877701626508466321568304366270557657639715091687 6 \\
c' &= 857074172986171447050927626793359025381475153431433090216157
\end{aligned}
$$

Solution : En calculant le PGCD des polynômes $X^{17} - c$ et $(X+1)^{17} - c'$ modulo N, nous obtenons le polynôme $X - m$ avec

$$m = 24275398002889718586805919532418824138858038040617070203820 82.$$

□