Exercices et problèmes de cryptographie

Damien Vergnaud

Exercice complémentaire n° 7.6 (bis)

Exercice 7.6 (bis) DIFFUSION DE DONNÉES CHIFFRÉES AVEC RSA

Un même message m a été chiffré avec le système de chiffrement RSA naïf à trois utilisateurs dont les clés publiques sont $(N_1, 3)$, $(N_2, 3)$ et $(N_3, 3)$. Le chiffrement a produit les trois chiffrés c_1, c_2 et c_3 (respectivement).

$$
\begin{aligned}
N_1 &= 29252782106552116939571206620961169386155639634151619813504 37\\
c_1 &= 27186029662828171119877463228328279757280283054954737274903 33\\
N_2 &= 41184063581262786561101549546047745542714610684345069421455 11\\
c_2 &= 22448585324626016445276909597688380684265747563715116152919 43\\
N_3 &= 30216717759105610903233410454177128075880007181934524632256 59\\
c_3 &= 13964994015539435706620943463181247478066911510124481533410 97
\end{aligned}
$$

Solution : Avec les notations de la solution de l'exercice 7.6, en appliquant le théorème chinois des restes, nous obtenons

$$\begin{aligned} c = m^3 \quad = \quad & 13758655830110027819424485939684210602536280697 23 \\ & 995960322491245735480370666999000000000 \end{aligned}$$

et il suffit d'extraire la racine cubique de c pour obtenir le texte clair

$$m = 111222333444555666777888999000$$

□