

*réussite internationale*

“RSA 129” est un nombre de 129 chiffres grâce auquel Ronald RIVEST, Adi SHAMIR et Leonard ADLEMAN ont codé un message en 1977 ; ils avaient alors défié quiconque de le décrypter. L'été dernier, Arjen LENSTRA proposa à tous les volontaires disposant d'un accès au réseau électronique Internet de participer à la relève de ce défi. Il fallait factoriser RSA 129, c'est fait au 26 avril 1994. Plus de 600 personnes — d'Afrique du Sud, Allemagne, Australie, Belgique, Brésil, Canada, Chili, Danemark, Espagne, Finlande, France, Hollande, Irlande, Israël, Italie, Japon, Norvège, Nouvelle Zélande, Portugal, Royaume Uni, Suisse, USA, Vénézuéla — ont ainsi collaboré pour venir à bout de la factorisation de “RSA 129” = 114381625757888867669235779976146612010218296721242362562561842935706935245733897830597123563958705058989075147599290026879543541. Voici leur résultat :

$$\begin{aligned}
 &114381625757888867669235 \\
 &779976146612010218296721 \\
 &242362562561842935706935 \\
 &245733897830597123563958 \\
 &705058989075147599290026 \\
 &879543541 = 349052951084 \\
 &765094914784961990389813 \\
 &341776463849338784399082 \\
 &0577 \times 32769132993266709 \\
 &549961988190834461413177 \\
 &642967992942539798288533
 \end{aligned}$$

On est bien peu de choses !