Deux ans et demi de calcul pour casser un cryptage informatique

Un laboratoire informatique de Nancy a réussi à montrer que les clés de cryptage, utilisées dans le commerce internet ou les cartes bancaires, ne seront plus fiables après 2010.

Sans le savoir, vous utilisez peut-être une clé RSA-768 bits. Que vous achetiez sur internet ou vous serviez de votre carte bancaire, ce système est l'un de ceux qui sert à crypter les échanges de données entre ordinateurs. C'est ce type de verrou qu'un laboratoire de Nancy, l'Institut national de recherche en informatique et en automatique (Inria) Nancy-Grand Est, avec quatre partenaires internationaux, a réussi à casser.

Le système repose sur un nombre à 232 chiffres. Le casser signifie trouver les nombres premiers qui permettent de l'obtenir, exactement comme lorsque vous obtenez 15 en multipliant 3 par 5. Sauf qu'ici, les deux nombres comptent chacun 116 chiffres ! Le calcul a pris deux ans et demi au total et a nécessité une puissance de calcul équivalant à 425 PC les plus récents, à plein temps.

Ce travail permet de relativiser l'efficacité de la clé RSA 768 bits. Et l'Inria confirme ainsi les recommandations de l'agence nationale de la sécurité des systèmes d'information : il est préconisé de passer à des clés à 2 048 bits (une unité de mesure informatique) dès cette année. Le nombre à trouver pour rééditer le forçage du système compterait alors... 617 chiffres !

Le risque existe

Mais pourquoi changer dès maintenant s'il faut une telle puissance de calcul pour vaincre le cryptage ? « *La puissance des ordinateurs augmente, il faudra cent fois moins de machines d'ici une dizaine d'années,* explique Paul Zimmermann, directeur de recherches à l'Inria. *Les clés mises en service le sont pour plusieurs années.* »

L'Inria n'a pu savoir si les banques utilisaient encore ce type de clé. Mais le chercheur explique que « *même si la puissance de calcul nécessaire paraît importante, une organisation gouvernementale ou malveillante pourrait la mettre en œuvre* ». A titre de comparaison, le même travail avec l'un des ordinateurs les plus puissants actuellement n'aurait nécessité que dix à quinze jours. Bref, des sites internet comme e-bay pourraient être piratés ou de fausses cartes bancaires créées. Paul Zimmermann avoue ne pas avoir d'information particulière, mais il pense probable que ces mêmes clés sont également utilisées par la Défense nationale.

« *Notre rôle, comme organisme de recherche publique, est de montrer la vulnérabilité de ce genre de système,* observe Paul Zimmermann. *Les algorithmes que nous avons développés nous serviront à résoudre d'autres problèmes similaires.* » Le chercheur officie au sein d'une équipe intitulée Courbes, Algèbres, Calculs, Arithmétique des Ordinateurs, CACAO en abrégé. Sa performance devrait donc, à l'avenir, aider usagers ou banquiers à ne pas finir « chocolats »...

Julien BÉNÉTEAU.

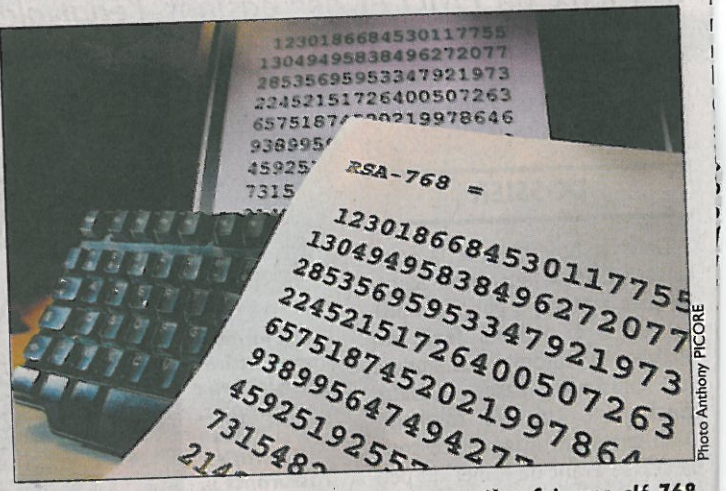

Photo Anthony PICORÉ

L" Inria a réussi à factoriser pour la première fois une clé 768 bits d'une longueur de 232 chiffres.