LE MONDE SCIENCE & MEDECINE
Pays : France
Périodicité : Hebdomadaire

Date : 12 OCT 16
Journaliste : David Larousserie

Mathématiques

Jeu de triche et de vérité

Des chercheurs franco-américains se sont amusés à truquer des nombres premiers pour éprouver la sécurité d'Internet. Démonstration.

ACTUALITÉ

Des nombres truqués pour mieux espionner

MATHEMATIQUES - Des chercheurs franco-américains s'inquiètent du manque de transparence sur les nombres entiers choisis pour sécuriser les transactions électroniques

Tricher n'est pas jouer. Mais jouer à tricher peut être stimulant, surtout si cela met en doute la sécurité d'Internet... C'est à ce petit jeu que vient de se livrer une équipe de l'université de Pennsylvanie, du CNRS et d'Inria au sein du Laboratoire lorrain de recherche en informatique et ses applications (Loria) de Nancy.

Ces chercheurs ont, en quelque sorte, fabriqué une porte qui a toutes les apparences de la solidité, mais qui en réalité est facile à crocheter. En outre, ils sont inquiets du fait que certaines de ces portes prétendument blindées des réseaux informatiques, et qui assurent la sécurité des messages, des signatures, des paiements, des connexions chiffrées... pourraient ne valoir guère mieux !

Une clé secrète

Internet est un réseau sur lequel des machines se « parlent » en permanence pour autoriser des connexions : canal chiffré entre deux ordinateurs, transmission de messages cryptés, signature électronique... La première étape est d'échanger une clé secrète, c'est-à-dire une série de chiffres qui servira ensuite à chiffrer et déchiffrer des messages ou authentifier des transactions. La solidité de ce maillon est donc cruciale. Et elle est en fait assurée par des fonctions mathématiques.

Certaines opérations sont en effet faciles à calculer mais difficile à inverser. Voire impossibles. Par exemple, multiplier deux nombres premiers entre eux est rapide, mais étant donné le résultat, retrouver ces deux entiers est d'autant plus ardu que des très grands nombres à plusieurs centaines de chiffres ont été utilisés. Et quand les puissances des ordinateurs progressent, il suffit d'augmenter la difficulté du calcul en accroissant la taille des nombres pour les préserver.

Le protocole Diffie-Hellman, du nom de ses inventeurs en 1976, premier maillon de la chaîne de confiance d'Internet, utilise une autre opération mathématique, plus compliquée à exposer, le logarithme discret. Le terme « discret » n'a rien à voir avec la confidentialité, mais indique que des entiers sont utilisés. Le terme « logarithme » suggère un lien avec des nombres élevés à une certaine puissance. Toujours est-il qu'étant donné un grand nombre premier p, il est possible de choisir un nombre entier secret x et de publier le résultat combinant mathématiquement p et x. En revanche, connaissant ce résultat et p, il est très long de trouver x ; le secret est protégé. C'est lui qui servira à chiffrer des messages.

En pratique, les nombres utilisés sont de 1024 bits, soit environ 300 chiffres. En juin, une équipe de l'université de Leipzig (Allemagne) et de l'Ecole polytechnique fédérale de Lausanne (Suisse) a établi un nouveau record, en réussissant à inverser l'opération à partir d'un p de 768 bits, montrant qu'il est dangereux d'utiliser des clés de cette taille.

Mais l'équipe américano-française est venue à bout d'un p plus grand, de 1024 bits, en recourant à dix fois moins de puissance de calcul que ses confrères. Deux mois de calculs, avec de 2000 à 3000 processeurs, ont été nécessaires, soit dix mille fois moins de temps que ce qu'on pensait. Comment est-ce possible ? En trichant. Les chercheurs ont fabriqué un nombre p ad hoc, de manière à faciliter leurs calculs, tout en faisant en sorte que ça ne se voit pas. Rien dans leur nombre ne laisse penser qu'il puisse être « truqué ».

Questions dérangeantes

L'exploit pourrait sembler anecdotique, s'il ne posait des questions dérangeantes. Quelle garantie que les entiers p utilisés soient moins robustes et aussi « truqués » que celui ainsi inventé ? Pour « causer » entre eux, les ordinateurs ne choisissent pas n'importe quel p, ils le piochent dans des listes de référence. Ces standards ne précisent pas comment ont été générés ces nombres. Et tout le monde utilise les mêmes...

« Pour ajouter à la parano, il faut dire que la recette pour construire notre entier a été proposée, en 1992, par Daniel Gordon, qui a ensuite été embauché par l'Agence nationale de sécurité américaine (NSA). De plus, l'un des protocoles qui liste des nombres premiers a été écrit par un sous-traitant de cette même agence », note Emmanuel

Thomé, chercheur à l'Inria de Nancy. Ce dernier évoque aussi les documents du lanceur d'alerte Edward Snowden qui ont notamment révélé que la NSA essayait d'*« influencer les politiques, les standards et les spécifications pour les technologies commerciales de clés publiques »*.

Autrement dit, d'autres auraient très bien pu avoir la même idée que les chercheurs, mais sans la publier, afin de bénéficier d'avantages pour l'espionnage. Car une fois la clé secrète connue, il est facile de déchiffrer les messages ou d'intercepter les informations circulant sur un canal chiffré, par exemple entre une entreprise et le domicile d'un de ses employés.

« Il faut éliminer tous les nombres premiers "inconnus", c'est-à-dire ceux dont on ne sait pas comment et pourquoi ils ont été choisis », estime Emmanuel Thomé. Et d'appeler avec ses coauteurs à piocher des entiers dans des ensembles plus sûrs, à doubler la taille de ces nombres, voire à changer d'opérations mathématiques « difficiles ». ■

DAVID LAROUSSERIE

COLIN ANDERSON/BLEND IMAGES LLC