Des scientifiques cassent une clé de sécurité de 768 bits

Un groupement de chercheurs de l' EPFL, l'Ecole polytechnique fédérale de Lausanne, mais aussi de l'**INRIA** (France), **NTT** (Japon), l **'Université de Bonn** (Allemagne) et **CWI** (Pays-Bas) viennent de casser une clé de sécurité particulièrement corsée.

Cette équipe internationale de scientifiques est parvenue à casser la **clé RSA de 768 bits** par la méthode de l'extraction des facteurs premiers de ses 232 chiffres. Bien que nécessitant une grande puissance de traitement, ce record a pu être atteint en **moins de deux ans et demi de travaux.**

L'école suisse EPFL estime qu'à terme « *on peut déjà s'attendre à ce que la clé RSA de 1024 bits perde son inviolabilité au cours de la prochaine décennie* ». Pourtant les **systèmes cryptographiques garantissent aujourd'hui la sécurité des échanges de données sur Internet** comme le standard ***https*** dans le cadre des paiements en ligne, par exemple.

Déjà, des calculs de ce même groupement de scientifiques avait permis de montrer la vulnérabilité des clés RSA de 512 bits en 1999, puis des 663 bits en 2005. De même, voilà une semaine, les chercheurs du groupe SySS avaient mis à jour l 'existence de failles sur les clés USB **Kingston, SanDisk et Verbatim.** Ils avaient ainsi découvert le moyen de passer outre le chiffrement de ces clés qui portaient l'assentiment du gouvernement américain et disposaient de la **certification FIPS 140-2** (Federal Information Processing Standard).

Si cette sécurité est basée sur le principe du **chiffrement AES en 256 bits**, les scientifiques remarquent que le chiffrement en lui-même ne pose pas problème. SySS s'est alors borné à analyser le logiciel de vérification de mots de passe et a ainsi estimé qu'ils pouvaient facilement déverrouiller les clés chiffrées…