Jacques Stern : « La cryptologie fait partie de notre vie quotidienne »

- Informatique - Sécurité Informatique -

Date de mise en ligne : mardi 18 dÃ©cembre 2007

Spyworld Actu

Médaille d'or du CNRS en 2006, mathématicien mais aussi entrepreneur et président de l'Agence nationale pour la recherche, Jacques Stern est le grand spécialiste français de la cryptologie. Il s'est confié à Futura-Sciences.

Connu pour avoir cassé en 1997 un code réputé inviolable par IBM, Jacques Stern doit surtout sa célébrité à ses découvertes importantes en cryptologie, qui lui ont valu la Médaille d'argent du CNRS puis, en 2006, la Médaille d'or. Nous l'avons rencontré à Lyon, au colloque organisé par l'Ecole Normale Supérieure (ENS), « Création de savoirs, création de valeurs ». Le thème correspond bien au parcours de ce mathématicien, professeur à l'ENS, directeur du laboratoire d'informatique (unité mixte ENS/CNRS), devenu responsable du conseil d'administration d'Ingénico, fabricant de terminaux de paiement et de solutions de transactions sécurisées. Depuis le mois de septembre dernier, Jacques Stern est aussi le président de l'Agence nationale pour la recherche.

Futura-Sciences : Comment définiriez-vous la cryptologie ? Est-elle plutôt une branche des mathématiques ou une spécialité informatique ?

Jacques Stern : La cryptologie a d'abord été un art. Regardez les travaux du Florentin Leon Battista Alberti... Elle est ensuite devenue une technique. Aujourd'hui, c'est une science. Elle opère dans un certain environnement (actuellement l'informatique), met en oeuvre une ingénierie (nous utilisons des outils, qui peuvent aller jusqu'au fer à souder) et se base sur des concepts mathématiques. Son objet est la trilogie fondamentale : l'intégrité (les informations doivent restées intactes), l'authenticité (l'origine ou la personne doivent être reconnues) et la confidentialité (les informations ne doivent pas être divulguées).

FS : Quelles ont été les évolutions déterminantes ?

Jacques Stern : La dernière date de 1976-1978 avec l'apparition de la cryptologie asymétrique. On a alors considéré qu'il existait une dissymétrie entre, d'une part, le fait de cacher un message et, d'autre part, l'opération à réaliser pour récupérer ce message. On a ainsi inventé le principe de la clef publique : le message est crypté par une méthode connue de tous mais seul le destinataire peut le lire.

FS : Quelle est la plus belle méthode, selon vous ? Et la plus utilisée aujourd'hui ?

Jacques Stern : Elles sont toutes belles ! La plus efficace et la plus utilisée dans le domaine de la cryptologie asymétrique est celle de Rivest, Shamir et Adelman, dite RSA. Il existe bien d'autres méthodes. En cryptologie symétrique, les plus connues sont RC4 (celle utilisée sur Internet sur les sites sécurisés reconnaissables au « s » ajouté à « http»), mais aussi DES (Data Encryption Standard) et AES (Advanced Encryption Standard).

Concernant les méthodes asymétriques, on peut aussi parler de la géométrie des nombres, une voie dans laquelle, pour casser un code, on ne cherche pas des biais statistiques mais des structures mathématiques.

FS : Quelle est la place de la cryptologie aujourd'hui ?

Jacques Stern : Nous vivons dans un monde virtuel. De nombreuses informations concernant notre vie privée, voire notre santé, sont inscrites quelque part bien qu'elles ne doivent pas être publiques. La cryptologie fait désormais

partie de notre vie quotidienne. Elle est utilisée dans notre carte bancaire et dans notre téléphone portable, par exemple. En fait, on pourrait dire que l'intérêt de la cryptologie a commencé à exister avec l'invention de l'écriture, qui conduit à ne plus garder sur nous des informations qui viennent de nous-mêmes.

FS : Vous étiez mathématicien à l'origine. Comment êtes-vous passé à la cryptologie ?

Jacques Stern : Au moment de ma thèse, je m'étais spécialisé dans la logique. Je m'intéressais à ce que les mathématiques peuvent faire ou ne peuvent pas faire, dans la lignée des logiciens, comme Kurt Gödel. J'ai réalisé alors que je ne voulais pas passer ma vie à essayer de démontrer que des choses sont impossibles. Dans le domaine de la cryptologie, au contraire, on voit ce qui est impossible... Le sujet était donc complètement différent. J'ai dû me reformater.

FS : Quelle a été votre contribution ?

Jacques Stern : En cryptographie (le codage), j'ai proposé de nouvelles méthodes pour l'authentification. Elles ne font que cela (alors que le procédé RSA assure aussi la confidentialité et l'intégrité) mais elles le font bien plus rapidement et sont actuellement utilisées sur Internet. Je me suis aussi intéressé à la cryptanalyse, l'autre versant de la cryptologie. Si la cryptographie est le bouclier, la cryptanalyse est l'attaque. Du côté des codes que j'ai pu casser, j'ai un beau tableau de chasse... J'ai également travaillé sur la détermination du niveau de sécurité des méthodes proposées, ce qui a conduit au concept de « sécurité prouvée ». En informatique se pose toujours à un moment ou à un autre un problème de norme. J'ai pu démontrer que certaines normes de cryptage n'affectaient pas le niveau de sécurité. On peut donc choisir une certaine façon de procéder en fonction du niveau de sécurité recherché et de la rapidité souhaitée pour le décryptage.

FS : On parle d'une école française de cryptologie, dont vous seriez le père. Quelle est cette « école » ?

Jacques Stern : Les équipes françaises sont en pointe. Je le constate tous les jours. Mes élèves, dont les plus âgés atteignent maintenant les 30 à 40 ans, sont reconnus à l'international. En France, nous avons une forte tradition pour les mathématiques. J'ai pu réunir des gens de valeur. La mayonnaise a pris facilement.

Post-scriptum :

http://www.futura-sciences.com/fr/s...