La cryptologie moderne et Jacques Stern

Médaille d'or du CNRS

Laurent DEMONET

Jacques Stern a reçu en 2006 la Médaille d'or du CNRS pour ses travaux fondateurs en cryptologie moderne. Cette distinction, la plus haute pour des travaux de recherche en France, est décernée chaque année depuis 1954 à un chercheur ayant contribué au rayonnement de la recherche française dans le monde. A 57 ans, Jacques Stern est directeur du Département d'informatique de l'ENS, chercheur d'exception aux nombreux disciples dans l'école française de cryptologie.

La cryptologie, science de paradoxes

L'art de crypter des messages est pratiquement aussi ancien que l'art militaire. Malgré cela, ce n'est que très récemment que la cryptologie est née en tant que discipline scientifique à part entière, rigoureuse, par opposition à la cryptographie empirique traditionnelle. La cryptologie rassemble essentiellement deux branches :

- la cryptographie qui consiste à inventer de nouvelles méthodes de cryptage, souvent appelées protocoles cryptographiques ;
- la cryptanalyse qui consiste à casser des protocoles cryptographiques, c'est-à-dire à trouver le moyen de décrypter des données sans posséder le code qui a permis de les crypter.

Ces deux branches sont intimement liées dans la cryptologie moderne, puisque trouver un protocole cryptographique efficace revient à diminuer au maximum la possibilité pour un adversaire de le casser. Au-delà de cette observation, il est extrêmement difficile de formaliser scientifiquement cette notion : comment garantir qu'un protocole résistera aux attaques des cryptanalystes sans connaître a priori les méthodes qu'ils utiliseront ? On sait aujourd'hui que cette question n'a pas de réponse absolue.

La question de la sécurité des protocoles cryptographiques est plus que jamais fondamentale, pour deux raisons : leur usage s'est banalisé, passant d'un usage militaire à un usage civil intensif (en particulier dans le cadre des transactions financières) d'une part, et les moyens potentiels de cryptanalyse ont explosé (naissance puis progrès de l'informatique). Par conséquent, la nécessité de prouver la sécurité de protocoles cryptographiques est devenue vitale, et c'est dans ce cadre qu'interviennent les mathématiques les plus poussées et, en un sens, les plus abstraites, utilisées dans les applications les plus concrètes. C'est dans ce domaine que Stern a obtenu de remarquables avancées.

Comment prouver un protocole cryptographique ?

Tout d'abord, il n'est pas possible d'inventer une méthode cryptographique absolument sûre, dans la mesure où il restera toujours une probabilité, éventuellement extrêmement faible, de réussir à décrypter un message quel que

soit le protocole utilisé. Le but est donc de limiter le plus possible cette probabilité relativement aux autres contraintes (en particulier aux contraintes de puissance : il faut par exemple que le cryptage du numéro d'une carte bancaire lors d'un achat sur Internet puisse être effectué par un ordinateur personnel en un temps extrêmement court, alors que l'on peut imaginer s'autoriser plus de temps et plus de puissance pour des applications militaires). Par ailleurs, il faut considérer qu'aucun des canaux de transmission n'est sûr (si c'était le cas, on n'aurait pas besoin de crypter) ; l'hypothèse que l'on fait donc habituellement en cryptologie est que le secret du cryptage est une donnée relativement petite, appelée clé. Dans le cadre de la preuve d'un protocole, on considère toujours le pire, c'est-à-dire le cas où le cryptanalyste possède toute l'information possible sur le protocole, sauf la clé. Le reste de la démarche consiste à démontrer que casser le protocole cryptographique revient à résoudre un problème qui est très difficile.

Cryptographie asymétrique : un progrès fondamental

La cryptographie habituelle est dite symétrique. C'est-à-dire que les deux personnes qui veulent communiquer partagent un secret (la clé) qui permet à la fois de crypter et de décrypter les messages. Par exemple, la méthode qui consiste à permuter les lettres de l'alphabet est un protocole symétrique : l'envoyeur et le destinataire du message


Jacques Stern

doivent tous deux savoir la manière dont sont permutées les lettres, manière qui constitue la clé.

La cryptographie asymétrique, parfois appelée aussi cryptographie à clé publique fait intervenir deux clés, une clé privée et une clé publique, qui sont liées ; la sécurité du protocole sera alors d'autant plus grande que la difficulté de déterminer la clé privée à partir de la clé publique est grande. La clé publique est alors publiée, et n'importe qui peut envoyer des messages cryptés au seul individu qui connaît la clé privée (puisqu'il ne l'a donnée à personne). On peut même utiliser ce principe pour crypter et signer des messages en même temps (signer un message consiste à prouver l'identité de l'envoyeur). Ainsi supposons qu'Alice veuille envoyer un message à Bob. Elle commence par crypter ce message avec la clé publique de Bob, puis elle crypte le message crypté avec sa clé privée. Ensuite, Bob commence par décrypter le message avec la clé publique d'Alice puis avec sa propre clé privée. Comme il faut la clé privée de Bob pour décrypter le

message, Alice est sûre que seul Bob pourra le lire. Par ailleurs, quand Bob aura décrypté le message et découvert quelque chose d'intelligible, il saura que c'est bien Alice qui l'a écrit puisque personne d'autre ne connaît la clé privée d'Alice.

Les avantages de la cryptographie asymétrique sont multiples : en particulier, elle permet de ne jamais avoir à transmettre la clé secrète, ce qui lui évite d'être interceptée par un individu malveillant ; par ailleurs, cela permet à chaque individu (ou à l'ordinateur de chaque individu) de n'avoir à retenir qu'une seule clé (sa clé privée), les clés publiques étant disponibles dans une sorte d'annuaire. Le défaut est alors qu'il faut qu'il existe un organisme jouant le rôle de cet annuaire ayant la confiance de tous (puisqu'il serait facile à cet organisme de remplacer par la sienne la clé publique de Bob). Ces organismes sont ceux qui produisent les certificats que les navigateurs Internet demandent d'accepter, en particulier lors de transactions.

Un exemple de protocole asymétrique est le protocole RSA (utilisé par exemple lors d'achats par cartes bancaires). La clé privée est un couple de deux grands nombres premiers et la clé publique est le produit de ces deux nombres. On considère actuellement que le fait de retrouver les deux facteurs du produit est un problème extrêmement difficile (on ne sait actuellement pas factoriser les entiers de plus de quelques centaines de chiffres).

Depuis toujours, Jacques Stern, pro-

fondément marqué par les travaux de Gödel et Turing, est attiré *par les sciences au tempo rapide, où les recherches trouvent rapidement des prolongements concrets*. L'entrée de la cryptologie dans le domaine académique, l'invention du concept à clé publique allaient ouvrir à ses recherches la voie d'une reconversion logique et en or !

Il lui fallut alors apprendre à programmer, travailler en théorie des nombres, transiter par la complexité algorithmique et potasser l'histoire de cette nouvelle science. Ses efforts paient ! A 37 ans, ses travaux en lien avec la cryptologie lui valent sa première invitation à un colloque international. Dix ans plus tard, il est à la tête du Laboratoire d'informatique, commun ENS-CNRS tout en ne négligeant pas l'enseignement car pour lui il s'agit *d'une activité où l'on voit les générations se former, et qui force un chercheur à clarifier ses idées*.

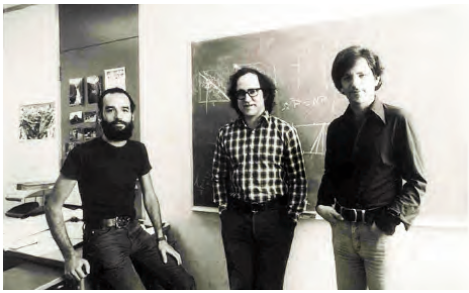
Le remarquable ouvrage qu'il publia en 1998 chez Odile Jacob *La science du secret* est à la fois le prolongement de cet enseignement, la nécessité d'ancrer ses

travaux dans une dynamique historique et la volonté de nouer des relations entre sciences et société.

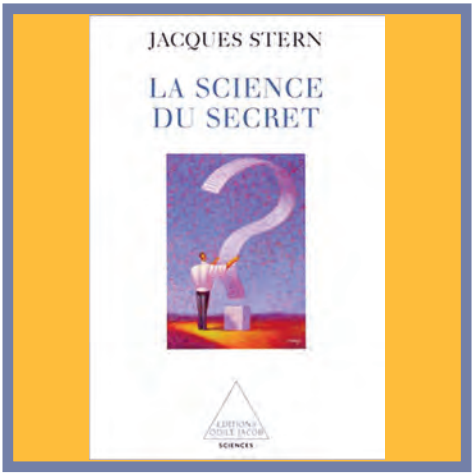
Il est membre du Conseil Scientifique de la Défense, du Conseil Stratégique de l'Information et il travaille à l'Observatoire de la Sécurité des Cartes de Paiement.

Jacques Stern est bien placé pour savoir que *Internet reste la zone de tous les dangers* mais il reste persuadé que la *cryptologie va sûrement évoluer vers de nouveaux concepts qui prendront en compte les mauvaises habitudes de l'utilisateur naïf qui, par exemple, ne met pas à jour régulièrement son système d'exploitation.*

Alors ce n'est plus un secret pour personne, Jacques Stern, premier informaticien au palmarès de la Médaille d'or du CNRS, avec ses nombreux étudiants, reste un expert des plus redoutés des inventeurs de code !



L'algorithme asymétrique de cryptographie à clé publique, **RSA**, très utilisé dans le commerce électronique et en particulier pour la circulation des données sur Internet, a été décrit en 1977 par trois jeunes américains Ron **R**ivest, Adi **S**hamir et Len **A**dleman.



Biographie de Jacques Stern

1949 : naissance de Jacques Stern
1968 : entrée à l'École Normale Supérieure
1971 : 1er à l'agrégation de mathématiques
1975 : doctorat de mathématiques
1979 : obtention du grade de professeur d'université (Caen)
1993 : professeur à l'ÉNS
1996 : directeur du laboratoire d'informatique de l'ÉNS
1998 : rapport sur la cryptologie remis au gouvernement qui aboutira l'année suivante à la nouvelle réglementation sur la cryptographie
1999 : devient directeur du département d'informatique de l'ÉNS
chevalier de la Légion d'honneur
2003 : prix Lazare Carnot de l'Académie des sciences
2005 : Médaille d'argent du CNRS
2006 : Médaille d'or du CNRS

Pour en savoir (un peu) plus :

Les livres suivants sont accessibles au grand public :

- *Jacques Stern*, La science du secret, Editions Odile Jacob, 1998

- *Jacques Stern,* Chapitre 6 de Paradigmes et enjeux de l'informatique (avec P. Nguyen), Editions Lavoisier, 2005 (ouvrage sous la direction de N. Bidoit, L. Fariñas del Cerro, S. Fdida, B. Vallée)