



Jacques Stern



© CNRS Photothèque – Christophe
LEBEDINSKY

20 ans au service de la cryptologie

ou l'homme qui a rendu nos échanges plus sûrs.

« *J'ai toujours été attiré par la science à temps court. J'aime que mes idées passent rapidement au stade des applications...* ». On comprend vite, face à cet homme calme, à la voix douce, aux termes précis et surtout concrets, pourquoi le jeune enseignant et chercheur en mathématiques (sorti de l'École normale supérieure à 22 ans et professeur à l'université de Caen à 30) a changé son fusil d'épaule à l'orée des années 80 pour devenir, en même temps que l'informatique prenait son essor, le chantre de la cryptologie française. Un besoin de peser sur le réel.

Mais une évolution, pas une rupture. Ses premiers travaux de recherche sur la logique, spécialité des mathématiques la plus proche de l'informatique, préparaient le terrain. « *Je m'intéressais aux résultats d'impossibilité en théorie des ensembles* », explique Jacques Stern dans son bureau bien rangé de la rue d'Ulm, à Paris, près duquel, dans un couloir, on pouvait lire, il y a peu, sur une affiche : « *la crypto c'est rigolo* ». Les mathématiciens Kurt Gödel, Alan Turing et Paul Cohen sont alors ses inspirateurs. Le même Turing qui, au début des années 1940, « casse » les codes de l'armée allemande... « *En allant voir ce qui se passe aux limites de la pensée mathématique, je suis arrivé à la cryptologie. J'ai toujours été attiré par certains paradoxes que l'on rencontre en logique, mais aussi en cryptologie : comment transmettre une correspondance secrète sans s'être jamais rencontrés ?* »

Dès lors le choix est fait : nous sommes en 1986, la cryptologie est devenue un domaine académique aux Etats-Unis depuis qu'a été inventé le concept de « clé publique » en 1976. La France balbutie en la matière, mais « *je voulais devenir un acteur de cette science* ».



Une école de cryptologie française

Sous l'impulsion de celui qui est aujourd'hui professeur à l'ENS, directeur de son département d'informatique et directeur du laboratoire d'informatique de l'ENS (LIENS, unité mixte ENS/CNRS), c'est une véritable école de cryptologie française qui va se créer en 20 ans. Les travaux poursuivis par le chercheur et son équipe du LIENS toucheront aux grands domaines de la discipline : conception d'algorithmes, cryptanalyse (attaque des systèmes proposés par d'autres), preuves de sécurité, normalisation de systèmes cryptographiques, et enfin protocoles et applications notamment dans le domaine de l'Internet avec en particulier le vote électronique.

La reconnaissance est vite internationale et aux plus hauts niveaux, pour le scientifique et ses travaux qui vont produire plus de 150 publications ainsi qu'une grande quantité de thèses. Auteur du livre « La science du secret » (chez Odile Jacob), Jacques Stern a obtenu la Médaille d'argent du CNRS en 2005. Il est également à l'origine d'un rapport au gouvernement sur la nouvelle réglementation de la cryptographie.

Chevalier de la Légion d'honneur, Jacques Stern s'est vu décerner en 2003 le prix Lazare Carnot de l'Académie des sciences pour l'ensemble de son « œuvre ». Marié et père de deux enfants, l'homme n'est en rien exubérant. S'il n'est pas immodeste, on le sent fier d'avoir d'une certaine façon rendu nos échanges plus sûrs. Son grand calme dissimule mal la passion pour une discipline qui lui prend beaucoup. Mais lui laisse un peu de temps pour son autre inclination : l'opéra. « *Classique, j'insiste...* ».



Jacques Stern

Né le 21 août 1949 à Paris

Formation : un cursus académique

- études secondaires au lycée Michelet et au lycée Louis-le-Grand à Paris
- 1968 : reçu à l'Ecole Polytechnique et à l'Ecole Normale Supérieure (ENS)
- 1968-1972 : élève à l'ENS
- 1971 : agrégé de mathématiques
- 1975 : docteur ès sciences

Carrière : des mathématiques à la cryptologie, en passant par l'informatique

- 1972-1978 : assistant puis maître-assistant à l'université Paris 7
- 1979-1986 : professeur à l'université de Caen
- 1986-1992 : professeur à l'université Paris 7
- 1986-1998 : maître de conférences à l'Ecole polytechnique
- 1992-1993 : directeur de recherche au CNRS
- 1993 - : professeur à l'ENS
- 1996 - : directeur du laboratoire d'informatique de l'ENS (LIENS, ENS/CNRS)
- 1999 - : directeur du département d'informatique de l'ENS

Publications et ouvrages

- 150 publications scientifiques entre 1975 et 2006
- 30 directions de thèses
- un livre : « *La science du secret* ». Editions Odile Jacob.

Prix et distinctions

- chevalier de la Légion d'honneur
- lauréat du prix Lazare Carnot de l'Académie des sciences en 2003
- Fellow of the IACR (International Association of Cryptology Research)
- Médaille d'argent 2005 du CNRS
- Médaille d'or 2006 du CNRS

