CENTRE NATIONAL
DE LA RECHERCHE
SCIENTIFIQUE

La médaille d'or 2006 du CNRS décernée à Jacques Stern, professeur d'informatique, spécialiste français des codes secrets

COMMUNIQUÉ DE PRESSE – PARIS – 6 OCTOBRE 2006 www.cnrs.fr/presse

La Médaille d'or du CNRS, plus haute distinction pour des travaux de recherche scientifique en France, est décernée cette année à Jacques Stern, 57 ans, professeur à l'Ecole normale supérieure (ENS), directeur du laboratoire d'informatique de l'ENS (unité mixte ENS/CNRS) et chercheur mondialement connu pour ses travaux sur la cryptologie. A l'origine de 150 publications, véritable père fondateur d'une école de cryptologie classant la France aux avant-postes de l'Europe dans la discipline, Jacques Stern a débuté sa carrière comme mathématicien avant de s'intéresser à l'informatique puis à la cryptologie. Un résumé de ce qui est aussi l'évolution récente de cette discipline…

Internet, comptes bancaires, enchères en ligne, vote électronique, communications téléphoniques… Alors que la cryptologie est restée très longtemps un domaine réservé aux militaires et aux diplomates, ses applications aujourd'hui très vastes touchent largement le grand public.

Spécialiste français mondialement reconnu, Jacques Stern a ouvert la voie de la cryptologie en France et y a consacré 20 années de travaux de recherche. D'abord mathématicien (logique et théorie des ensembles), il s'est ensuite tourné vers la complexité algorithmique avant de se lancer dans ce domaine de recherche.

Ancien élève de l'Ecole normale supérieure et docteur ès-sciences, Jacques Stern est aujourd'hui professeur à l'ENS rue d'Ulm à Paris où il dirige le laboratoire d'informatique de l'ENS (LIENS - unité mixte ENS/CNRS) et le département d'informatique. Il est l'auteur de 150 publications scientifiques, d'un ouvrage intitulé « *La science du secret* » (Editions Odile Jacob) ainsi que d'un rapport au gouvernement qui a été suivi d'une nouvelle réglementation de la crytographie. Médaillé d'argent du CNRS en 2005, 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 ses travaux dans le domaine.

Cette reconnaissance de 20 ans de recherche par la Médaille d'or du CNRS est l'occasion d'honorer une science singulière, qui a longtemps - par nature - cultivé le sens du secret mais qui, avec la numérisation et la mondialisation des échanges, concerne aujourd'hui le plus grand nombre.

CENTRE NATIONAL
DE LA RECHERCHE
SCIENTIFIQUE

Une nouvelle discipline scientifique

Etymologiquement, cryptologie signifie « science du secret ». Les premiers « travaux » remontent à plusieurs siècles avant Jésus-Christ et au fil du temps, la cryptologie est devenue une discipline scientifique à part entière dont le but est d'assurer l'intégrité d'une information, son authenticité et sa confidentialité dans les données et les échanges. Pour ce faire, elle établit des « règles du jeu » et des procédés pour résister aux « adversaires » qui ne les respecteraient pas. Exemples : le codage des messages diplomatiques doit lutter contre les services de renseignements d'autres pays ; une banque doit s'assurer de l'identité du porteur d'une carte de crédit, etc.

Les grands principes sont simples. Pour échanger une information que deux protagonistes (organisations ou individus) veulent conserver confidentielle, et pour s'assurer de leur identité respective, chacun doit posséder à la fois une clé pour s'identifier et une formule afin de coder puis de décoder le message. A partir de là, tout se complique. Les concepts font appel aux mathématiques les plus sophistiquées. Les chercheurs contemporains puisent leur inspiration dans les travaux de mathématiciens tel Alan Turing qui, dans les années 1930, a exploré à la suite de Kurt Gödel, les limites de la pensée mathématique.

Techniquement, la cryptologie a rejoint l'informatique depuis la fin de la deuxième guerre mondiale, et les scientifiques utilisent massivement l'ordinateur comme outil pour générer ou « casser » les algorithmes de codage les plus puissants. Sur le plan économique, enfin, c'est un secteur en pleine expansion du fait de l'explosion des communications électroniques.

Si les termes les plus simples, comme « code secret » ou « code PIN » pour la carte bancaire et la « carte SIM » pour les téléphones mobiles, sont dans la bouche de tous, qui connaît « clé secrète », « clé publique », « RSA », etc…? Derrière ces mots se cache une discipline en pleine effervescence, devenue indispensable, souvent stratégique et d'une grande richesse scientifique.

Quatre grands chantiers de la cryptologie moderne

A travers la Médaille d'Or 2006 du CNRS, c'est d'abord l'œuvre d'un chercheur qui est saluée, mais aussi les travaux de son équipe qui sont en pointe en Europe, se distinguent au plan mondial et ont permis en une vingtaine d'années des avancées majeures dans plusieurs domaines, en particulier dans quatre grands chantiers actuels de la cryptologie.

La conception d'algorithmes donne naissance à de nouveaux schémas cryptographiques, dont on a sans cesse besoin pour répondre à de nouveaux besoins (authentification, signature au moyen d'une carte à puce). Jacques Stern et son équipe ont, par exemple, pu faire la preuve d'un algorithme d'authentification, dit « GPS », élaboré avec France Télécom et devenu une norme ISO en 2005.

CENTRE NATIONAL
DE LA RECHERCHE
SCIENTIFIQUE

La cryptanalyse permet de « casser » des codes secrets prétendus inviolables. L'équipe de l'ENS/CNRS a notamment prouvé la fragilité d'algorithmes pourtant réputés solides voire inviolables ; en 1998, elle a pu « casser » un algorithme d'IBM qui se voulait une solution alternative à RSA fondée sur des outils mathématiques de la géométrie des nombres.

La sécurité prouvée. Ce n'est pas parce qu'un algorithme a résisté aux attaques des cryptanalystes qu'il est sûr ! Il faut en apporter la preuve, et c'est par exemple ce qu'a fait l'équipe de cryptologie de l'ENS en participant au « sauvetage » d'une norme. En 1994, une équipe américaine a publié un algorithme qui est devenu une norme d'échanges sur l'Internet. En 2000, un vent de panique a soufflé chez les utilisateurs, devant une rumeur selon laquelle sa preuve était fausse. L'équipe ENS/CNRS, en collaboration avec des chercheurs japonais, a pu trouver une preuve correcte.

Les applications et les protocoles. Vote électronique, enchères en ligne sur Internet, téléphonie 3 G, les équipes françaises autour de Jacques Stern ont apposé leur signature sur de nouveaux schémas cryptographiques qui concernent une multitude d'acteurs. On parle d'ubiquité de la cryptologie.

Pour en savoir plus :

http://www.di.ens.fr/CryptoTeam.html.fr
http://www.di-ens.fr/~stern/