40 ans d'aventure scientifique et humaine

Le LAAS célèbre cette année 40 ans d'existence. Créé en 1968 comme unité propre de recherche du CNRS, le « Laboratoire d'automatique et de ses applications spatiales » s'est très vite développé, avec un parti pris d'anticipation, dans d'autres disciplines qui allaient profondément modifier la vie scientifique, et révolutionner jusqu'à notre vie quotidienne : l'informatique, les micro et maintenant nanotechnolgies, la robotique et l'intelligence artificielle. Sans changer d'acronyme tout en tenant compte des évolutions de ses thématiques de recherche, il deviendra en 1973 le « Laboratoire d'automatique et d'analyse des systèmes » puis en 1994 ce qu'il est aujourd'hui, le « Laboratoire d'analyse et d'architecture des systèmes ». Qu'en est-il aujourd'hui dans ces domaines qui connaissent une évolution si rapide ? Quels sont les apports croisés d'une discipline à l'autre ? Comment, fort des avancées d'hier et d'aujourd'hui, se dessine demain ? Des scientifiques talentueux et renommés dans leur domaine, que le LAAS est honoré d'inviter, apportent leur éclairage dans un cycle de conférences tout au long de l'année 2008.

Laboratoire d'Analyse et d'Architecture des Systèmes du CNRS

7, avenue du Colonel Roche - 31077 Toulouse Cedex 4 - France
Tél. +33 (0)5 61 33 62 00 - www.laas.fr

Cycle de conférences du LAAS-CNRS 40e anniversaire

La cryptologie : des messages secrets aux transactions électroniques

par
Jacques STERN
Professeur à l'Ecole normale supérieure
Président de l'Agence nationale de la recherche
Président de la société Ingenico
Médaille d'or du CNRS

Vendredi 20 juin à 10 h 30
LAAS-CNRS, salle de conférences

résumé

Dans cet exposé, on évoquera brièvement les étapes de l'histoire de la cryptologie ou science des messages secrets. On expliquera notamment comment une spécialité, jadis confinée aux univers de la défense et de la diplomatie, est devenue, en une trentaine d'années, une science servie par une communauté de recherche active et on présentera certains des défis auxquels elle a été confrontée.
On s'attachera enfin à expliquer son rôle actuel dans la sécurisation des communications sur l'Internet et des transactions financières, en donnant des exemples de ce qu'on peut appeler l'ubiquité de la cryptologie moderne. Elle n'est plus seulement la science du secret mais la science de la confiance.

l'orateur

Ancien élève de l'École normale supérieure (ENS, 1968), docteur es sciences (Université Paris 7, 1975), Jacques Stern a été professeur à l'Université de Caen, puis à l'Université Paris 7 et, à partir de 1993, professeur à l'ENS et directeur du Département d'informatique qu'il a créé en 1999.

Jacques Stern est spécialiste de cryptologie. Il est l'auteur de plus d'une centaine de publications dans des revues scientifiques, portant sur tous les aspects de ce domaine de recherche, et d'un ouvrage intitulé « La science du secret » (éditions O. Jacob). Ses principaux travaux ont porté sur la cryptanalyse et les preuves de sécurité des algorithmes à clé publique, ainsi que sur la conception d'algorithmes cryptographiques adaptés aux cartes à microprocesseur.

Jacques Stern a participé à de multiples comités éditoriaux ou scientifiques et présidé celui de la conférence CCS (Communications and Computer Security) de l'ACM en 1996 et celui d'Eurocrypt en 1999. Il a également été conférencier invité dans de nombreux congrès, notamment Asiacrypt 1996 et Eurocrypt 2003. Il a été, en 2003, lauréat du prix Lazare Carnot de l'Académie des sciences, a reçu en 2005 la médaille d'argent du CNRS, en 2006 la médaille d'or du CNRS et en 2007 le RSA Award for excellence in mathematics. Il est chevalier de la Légion d'honneur.

Jacques Stern a été membre du Conseil scientifique de défense et du Conseil stratégique des technologies de l'information. Il siège au sein du Conseil scientifique de France Télécom et de l'Observatoire sur la sécurité des cartes de paiement.

Depuis 2005, Jacques Stern est administrateur d'INGENICO, entreprise de pointe dans le domaine des terminaux de paiement sécurisés. Il est président du Conseil d'administration d'INGENICO depuis juin 2007. Il est également, depuis août 2007, président du Conseil d'administration de l'Agence nationale de la recherche (ANR).