INSTITUT DE FRANCE
Académie des sciences

COMMUNIQUÉ DE PRESSE 5 juillet 2012

La Grande Médaille de l'Académie des sciences décernée en 2012 à l'informaticien Adi SHAMIR

Elle lui sera remise **mardi 16 octobre 2012** sous la Coupole de l'Institut de France

La Grande Médaille de l'Académie des sciences est la plus haute distinction de l'Académie. Elle est décernée chaque année depuis 1997 à un savant, français ou étranger, ayant contribué au développement de la science de façon décisive, tant par l'originalité de ses recherches personnelles que par leur rayonnement international et l'influence stimulante qu'il aura eue en créant une véritable école de recherche.

Le lauréat 2012 est l'informaticien israélien Adi SHAMIR, figure emblématique de la cryptologie moderne, Professeur à la Faculté de Mathématiques et de Science informatique au Weizmann Institute of Science (Rehovot, Israël). Par ses travaux de premier plan en mathématique, informatique et ingénierie, le Pr. Adi SHAMIR a porté l'art de la sécurité des transactions et des échanges informatiques au rang de science. Sa contribution couvre un large spectre allant du fondamental à l'appliqué, redéfinissant au passage les bases théoriques de deux disciplines confluentes et concurrentes : la cryptographie, qui consiste à coder les messages, et la cryptanalyse, qui consiste à en déjouer les mécanismes secrets. Ses travaux ont donc un impact majeur sur la science informatique, sur l'industrie et sur la société.

Né le 6 juillet 1952, **Adi SHAMIR** a commencé brillamment sa carrière de chercheur à l'école de cryptographie réputée de l'Institut Weizmann. Il est l'un des 3 auteurs avec Ronald Rivest et Leonard Adleman de l'algorithme RSA, de cryptographie asymétrique (« à clé publique »), inventé en 1977. Cette percée a valu en 2002 au célèbre trio le Prix Turing, assimilé au Nobel de l'informatique. L'algorithme RSA actuellement implanté sur la quasi-totalité des ordinateurs, est toujours le plus utilisé dans le commerce électronique, et plus généralement pour échanger des données confidentielles sur Internet. A l'avant-garde de sa discipline depuis plus de trente ans, le Pr Adi Shamir a contribué à tous les domaines de la cryptographie et de la cryptanalyse : cryptographie distribuée (*Secret Sharing Scheme*), génération de séquences pseudo-aléatoires, protocoles *Zero-Knowledge* (dont le protocole Fiat-Shamir élaboré avec son étudiant Amos Fiat) etc. Il a proposé des méthodes de cryptanalyse d'une efficacité nouvelle et redoutable sur nombre de systèmes (téléphonie mobile GSM, 3G etc.) ; elles ont pour nom *Cache Attacks*, *Bug Attacks*, *Twinkle*… En bon passeur, Adi Shamir a lui-même formé de brillants chercheurs - dont Eli Biham, Uriel Feige, Amos Fiat - et signé plus de 180 publications. Lauréat 2008 du prix Israël, il est membre de plusieurs Académies des sciences dont celle des Etats-Unis et l'Academia europaea. Il est *Docteur Honoris Causa* de l'École Normale Supérieure, à Paris.

Liste des lauréats précédents de la Grande Médaille de l'Académie des sciences sous ce lien .
Accessible également depuis http://www.academie-sciences.fr/activite/prix/grande_medaille.htm

Contact presse :

Académie des sciences
Délégation à l'Information Scientifique et à la Communication
Bernard Meunier, Délégué, Membre de l'Académie des sciences
Marie-Laure Moinet, chargée des relations avec la presse
Tél. : 01 44 41 45 51 / 44 60
presse@academie-sciences.fr
http://www.academie-sciences.fr/

Contacts scientifiques :

Adi SHAMIR
adi.shamir@weizmann.ac.il
http://www.wisdom.weizmann.ac.il/

Gérard BERRY
Membre de l'Académie des sciences
INRIA Sophia Antipolis
Tél. : 06 79 52 62 65
gerard.berry@sophia.inria.fr