

Cryptography: Secrets and Lies, Knowledge and Trust

THIRD ARNOLD FAMILY LECTURE

Avi Wigderson, Institute for Advanced Study, Princeton

1

Did you ever wonder what protects your computer password when you log on, or your credit card number when you shop on-line, from hackers listening on the communication lines?

2

Is it possible for a group of people to play a (cardless) game of Poker on the telephone, without anyone being able to cheat?

3

Can you convince others that you can solve a tough math (or SudoKu) puzzle, without giving them the slightest hint of your solution?

4

Can two people who have never met create a secret language in the presence of others that no one but them can understand?

November 3, 2011 / 7:00 pm

Institute for Mathematics
and its Applications

UNIVERSITY OF MINNESOTA
Driven to DiscoverSM

November 3, 2011 / 7:00 pm

175 Willey Hall • 225 19th Ave. South
West Bank, University of Minnesota, Minneapolis

Cryptography: Secrets and Lies, Knowledge and Trust

THIRD ARNOLD FAMILY LECTURE

Avi Wigderson, Institute for Advanced Study, Princeton

In this talk, Wigderson will survey some of the mathematical and computational ideas, definitions, and assumptions which underlie privacy and security of the Internet and electronic commerce. He will explain some of the magical consequences of this theory. For example, how the solution of question (1) enables a positive answer to questions (2), (3), and (4). He will also explain the fragility of the current foundations of modern cryptography and the need for stronger ones.

For more information: 612-624-6066 • www.ima.umn.edu

COLLEGE OF
Science & Engineering

UNIVERSITY OF MINNESOTA

The Institute for Mathematics and its Applications connects scientists, engineers, and mathematicians in order to address scientific and technological challenges in a collaborative, engaging environment, developing transformative, new mathematics and exploring its applications, while training the next generation of researchers and educators.

The University of Minnesota is an equal opportunity educator and employer.

Institute for Mathematics and its Applications

University of Minnesota
400 Lind Hall
207 Church Street, SE
Minneapolis, MN 55455

Nonprofit Org.
U.S. Postage
PAID
Twin Cities, MN
Permit No. 90155