Pacific Institute *for the* Mathematical Sciences

PIMS Public Lecture: Avi Wigderson

Thursday, 7 March, 2013

University of British Columbia, Vancouver
3:00 pm ESB Rm 2012
2:30 pm Reception in PIMS lounge

CRYPTOGRAPHY: SECRETS AND LIES, KNOWLEDGE AND TRUST

Avi Wigderson (Institute for Advanced Study, Princeton)

email address/username

****

LOGIN

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? Can two people who never met create a secret language in the presence of others, which no one but them can understand? Is it possible for a group of people to play a (card-less) game of Poker on the telephone, without anyone being able to cheat? Can you convince others that you can solve a tough math (or SudoKu) puzzle, without giving them the slightest hint of your solution?

These questions (and their remarkable answers) are in the realm of modern cryptography. In this talk I plan to survey some of the mathematical and computational ideas, definitions and assumptions which underlie privacy and security of the Internet and electronic commerce. We shall see how these lead to solutions of the questions above and many others. I will also explain the fragility of the current foundations of modern cryptography, and the need for stronger ones.

No special background will be assumed.

DR. AVI WIGDERSON is a widely recognized authority in theoretical computer science. His main research area is computational complexity theory. This field studies the power and limits of efficient computation and is motivated by such fundamental scientific problems as: Does P=NP? Can every efficient process be efficiently reversed? Can randomness enhance efficient computation? Can quantum mechanics enhance efficient computation? He has received, among other awards, both the Nevanlinna Prize and the Gödel Prize.

www.pims.math.ca