Cryptography: Secrets and Lies, Knowledge and Trust

Avi Wigderson, Institute for Advanced Study

Abstract

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 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 led 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.