Cryptographic abundance: Essential and (almost) irrelevant

Andrew Odlyzko

AT&T Labs
Florham Park, NJ 07932, USA

amo@research.att.com
http://www.research.att.com/~amo

The important thing is to *maximize the value* of your intellectual property, not to protect it for the sake of protection.

Honor System Virus

This virus works on the honor system.

Please forward this message to everyone you know and then delete all the files on your hard disk.

Thank you for your cooperation.

main problems:

  (i) economic

 (ii) sociological

(iii) psychological

micropayments:

> *à la carte* or unit pricing will not
> be the dominant mode of
> commerce in information goods
>
> Fishburn-O.-Siders
> *First Monday,* July 1997
> ⟨http://firstmonday.org/⟩

results of PEAK experiment (⟨http://www.si.umich.edu/PEAK-2000/⟩):

> [Elsevier's] goal is to give people access to as much information as possible on a flat fee, unlimited use basis. [Elsevier's] experience has been that as soon as the usage is metered on a per-article basis, there is an inhibition on use or a concern about exceeding some budget allocation.
>
> Karen Hunter of Elsevier

Ultimatum game:

1. $10 to be divided by Alice and Barbara

2. Alice proposes a split (for example, $7 for Alice, $3 for Barbara)

3. (a) Barbara accepts: each gets specified amount

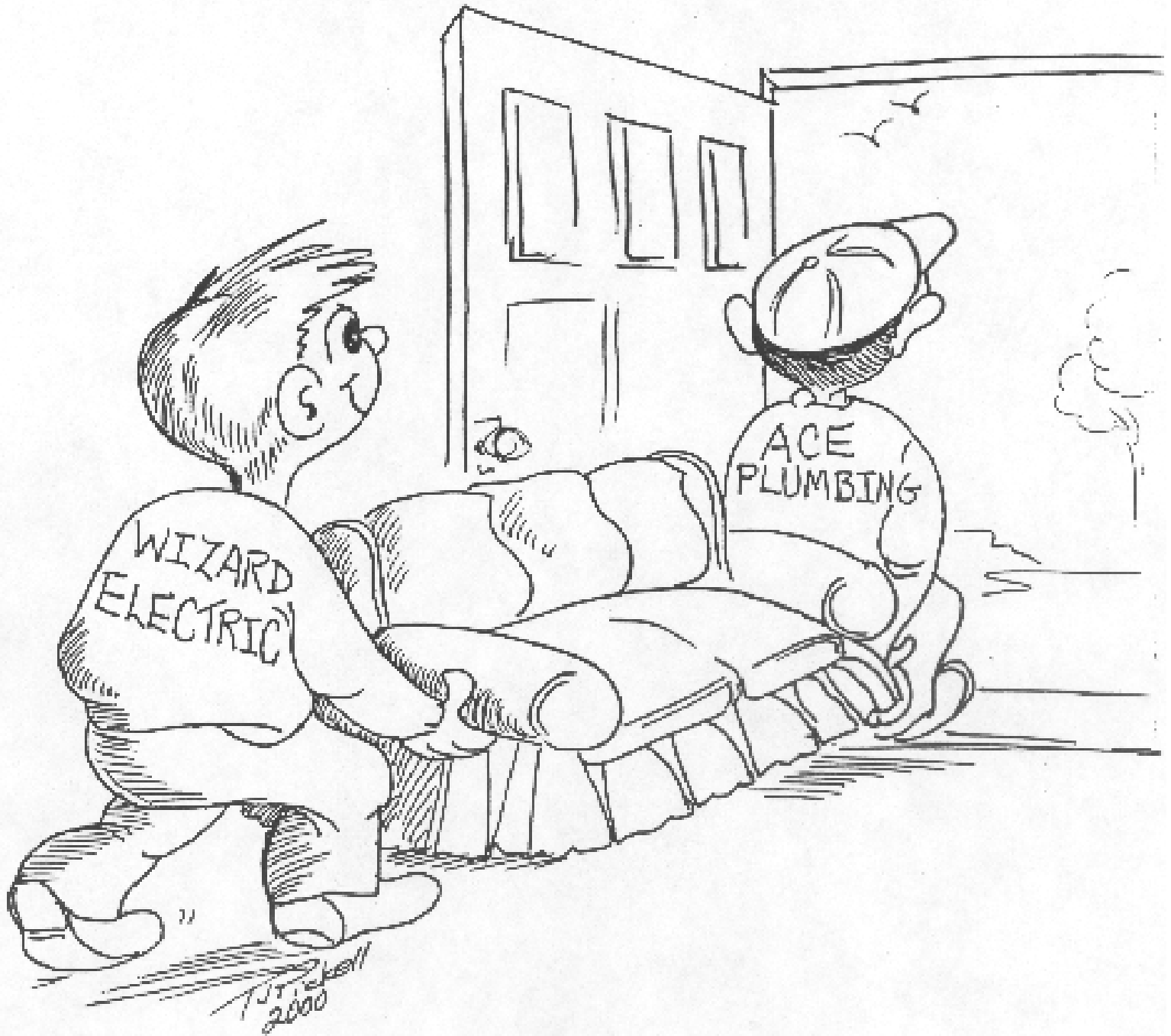   (b) Barbara rejects: neither gets anything

ALICE

BARBARA

Major problem with secure systems:

secretaries could not forge their bosses' signatures

Please let the plumber in to fix the leaky faucet.

impossibility theorems (Arrow, ...):

"marriage penalty" unavoidable if one insists on

(i) progressive income tax

(ii) equal treatment of households with equal incomes

crypto's function:

erect speed bumps on the
Information Superhighway

(starting with rot-13)