

Letters

Factoring and Cryptography

I would like to correct the misimpression given by Barry J. Cipra's Research News article (21 Oct., p. 374) that the accomplishment of Lenstra, Manasse, and others in factoring a 100-digit number somehow threatens the security of codes (such as the RSA public-key cryptosystem) that are based on the difficulty of factoring large integers.

As a cryptographer, I welcome all of this intense research into the difficulty of factoring large integers. In general, one has the most confidence in codes whose security has been extensively tested. The work on factoring Cipra describes helps establish more precisely the exact level of effort needed to factor numbers of various lengths; this is precisely what cryptographers and potential users of public-key cryptosystems based on factoring want to know. Given such information, it is possible to choose numbers of appropriate size to withstand any specific level of effort.

Let me be precise. Adding an additional digit to a number means that approximately 20% more computing power will be required to factor it, for numbers in the range from 100 to 300 digits. More precisely, the required effort to factor n with the use of the best algorithms available grows as $\exp(\ln(n)\ln\ln(n))^{1/2}$. The effort required to factor the 100-digit number by Manasse *et al.* was approximately 25 MIP-years, where an MIP-year is the computational power of a 1-million-instruction-per-second machine running for 1 year. Using this as a calibration point, we can estimate the effort required for larger numbers:

Length in digits	Effort required to factor (MIP-years)
100	25
150	3.5×10^5
200	1.2×10^9
250	2×10^{12}
300	1.6×10^{15}

Since doubling or tripling the length of numbers used in a cryptosystem only increases the encryption-decryption time by a constant factor, a cryptographer can easily choose a number of sufficient length to withstand a given level of attack, even including expected advances in computing technology and a degree of parallelism obtained by coordinating a number of workstations. I strongly disagree with Cipra's

conclusion that "the only real danger is to secrets that must remain secret for more than a few years." The danger only arises if one is ignorant of the true difficulty of factoring and chooses numbers that are too short. The nice thing about the recent factoring accomplishment is that it provides another calibration point on the difficulty curve, allowing one to choose numbers providing a given degree of security with a greater degree of confidence.

RONALD L. RIVEST
*Laboratory for Computer Science,
Massachusetts Institute of Technology,
Cambridge, MA 02139*

CO₂ Reduction and Reforestation

It is appropriate that *Science* address the global warming issue and especially the biotic interactions, including the possibility of reducing the atmospheric burden of carbon dioxide by the management of forests. William Booth's article (News & Comment, 7 Oct., p. 19) treats the planting of trees; the challenge is the management of forests.

Deforestation is progressing at a higher rate than ever previously. It is probably releasing 1 to 3 billion tons of carbon annually into the atmosphere. At the moment, the net annual accumulation of carbon dioxide in the atmosphere amounts to about 3 billion tons. That is the amount that must be removed from current releases to bring the atmosphere toward stability in the short term. A cessation of deforestation would obviously make a major contribution in that direction.

The reestablishment of forests is more than simply planting trees. Forests contain a diversity of species and, in the normal circumstance, build organic matter into soils over time. The total amount of carbon in a forest exceeds substantially the total amount in trees, and the total per unit land area in primary forests and in most secondary forests on fertile soils exceeds the total in plantations. The establishment of forests on about 2 million square kilometers of land would result, over much of the earth's surface, in the storage of about 1 billion tons of carbon per year throughout the period in which carbon is accumulating in the forest. That might extend for 40 to 50 years or longer, depending on the forest.

Planting trees in places such as the Los Angeles Basin is a constructive step. There is good reason to assume that a massive program of planting trees in such places would ameliorate the local climate and reduce demands for fossil fuel cooling in summer. But there is a substantial difference between

planting trees and reestablishment of forests as a tool in management of the global crisis of climate.

G. M. WOODWELL
*Director, Woods Hole Research Center,
Woods Hole, MA 02543*

Charles Hall is reported as stating, "I don't know if we're going to be able to significantly alter atmospheric carbon by planting trees, but so what? You haven't hurt anybody by planting trees on marginal lands." At least within the tropics, the use of massive tree planting to slow the increase rate of net global atmospheric carbon will require a social and demographic adjustment vastly more expensive, socially difficult, and time-consuming than would be the technically trivial task of reclothing large areas with woody plants. This is because at least a billion people in the tropics currently live on, or depend on, the production from marginal lands. Planted trees are a crop with a substantially lower yield per area per year than the current or potential yields from those marginal lands. While planted trees are important ingredients for many tropical human adjustments to their ecological realities, the massive reclothing of "marginal lands" with tree plantings would result in a substantial reduction in the contemporary and potential carrying capacity of much of the tropics. It seems clear that the tropics have already greatly exceeded their carrying capacity for numbers of humans with a reasonable standard of living. However, the mitigation of greenhouse gas production by extra-tropical societies through a yet greater reduction of the carrying capacity of huge tropical areas does not seem to me to be a solution.

DANIEL H. JANZEN
*Department of Biology,
University of Pennsylvania,
Philadelphia, PA 19104*

Booth notes that reforestation carries additional benefits: slowing soil erosion, improving watersheds, providing timber, and so forth. Coastal kelp farms could also provide benefits such as food, fertilizer, and fuels to help defray installation and operating costs. Values of many of these products are likely to increase over the long term, and new technology can be expected to reduce costs. New anchoring systems currently in use, for example, would reduce costs and enhance reliability compared with the design analyzed by Bird and Benson (1). Experiments have shown that kelp can now be easily and inexpensively planted on sand bottom (2).

Kelp is an excellent feedstock for production of methane and hydrocarbons of low

molecular weight (1). The ultimate cure for the greenhouse should involve recycling of atmospheric carbon, not simply creating additional storage in various reservoirs. A marine farm has good potential for recycling carbon and reducing atmospheric pollution through production of clean-burning fuels. We urge that consideration be given to "Johnny Kelpspore and the Greenhouse."

HOWARD A. WILCOX
882 Golden Park Street,
San Diego, CA 92106

WHEELER J. NORTH
W. M. Keck Engineering Laboratories,
California Institute of Technology,
Pasadena, CA 91125

REFERENCES

1. K. T. Bird and P. H. Benson, *Seaweed Cultivation for Renewable Resources* (Elsevier, Amsterdam, 1987).
2. R. Streichenberger and W. J. North, unpublished data.

The Global ReLeaf effort described by Gregory Byrne (News & Comment, 21 Oct., p. 371) may be a worthwhile effort aimed at reducing atmospheric carbon dioxide. The proposed 100 million trees would certainly absorb carbon dioxide, but the impact on the carbon dioxide production-destruction equation is likely to be far great-

er than that suggested in the article. American Forestry Association executive vice president R. Neil Sampson is quoted as saying, "Those [trees] planted in urban areas would . . . help shade residences, leading to a savings in air-conditioning costs of \$4 billion a year." That cost represents about 6% of all U.S. residential electricity consumption and the avoided combustion of 16 billion tons of coal. Avoiding the combustion of the coal saves the release into the atmosphere of about 60 billion tons of carbon dioxide, three times what is absorbed by all the trees.

If the estimates of the American Forestry Association are correct, high priority should be placed on the planting of trees in locations where they shade air-conditioned structures, as those trees may have about four times the impact in decreasing atmospheric carbon dioxide as trees planted in other locations.

JAMES SWARTZ
Department of Chemistry,
Grinnell College,
Grinnell, IA 50112-0806

I read with interest Byrne's article "Let 100 million trees bloom." The article points out that 100 million additional trees would remove about 18 million tons of carbon dioxide from the atmosphere each year and

then goes on to state, "an estimated 6 billion tons of carbon dioxide from fossil fuels enter the atmosphere each year." The 100 million trees would therefore remove about 0.3% of the additional carbon dioxide.

A few simple calculations show that *all* of the additional carbon dioxide introduced by fossil fuels could be removed by a 2% increase in the quantity of phytoplankton in the world's oceans. We have effected marvelous improvements in the production of land-based plants. Could we not produce a 2% increase in the ocean's phytoplankton?

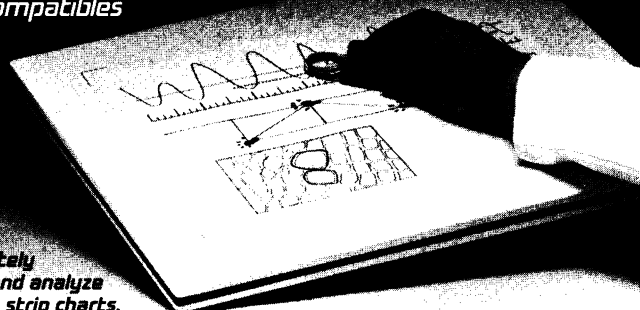
HORST HOYER
165 Watchung Avenue,
Montclair, NJ 07043

Erratum: In the report "Single-chain antigen-binding proteins" by Robert E. Bird *et al.* (21 Oct., p. 423), references 17 and 18 were inadvertently interchanged. Reference 17 should have been to J. S. Huston *et al.*, *Proc. Natl. Acad. Sci. U.S.A.* **85**, 5879 (1988), and reference 18 should have been to D. Scandella, P. Arthur, M. Mattingly, and L. Neuhold, *J. Cell Biochem.* **9B**, 203 (1985).

Erratum: The proportion of dogs among animals used in research was incorrectly reported in Constance Holden's article "Billion dollar price tag for new animal rules" (News & Comment, 4 Nov., p. 662). Dogs make up about 1% of research animals, according to the Office of Technology Assessment. Primates make up about 0.05%.

SigmaScan™ measures areas, lengths coordinates, angles, slopes, and more —

IBM PC and Compatibles



Quickly and accurately
digitize, measure and analyze
photomicrographs, strip charts,
X-rays, maps, and more — using
your own PC.

- Areas, lengths, angles, and slopes
- X,Y digitizing
- User-defined units
- Standard ASCII data output
(use in Lotus, dBase, etc.)
- Keyboard macros
- User-defined data transforms

Save hundreds of hours annually over
manual measurement techniques.
Automate complex analyses. Comes
complete with software, choice of
digitizing tablet, money-back guarantee
and full year hardware warranty.

Sigma-Scan™ software is also
available separately.

SCIENTIFIC

Announcement and call for Abstracts for
Conference on

Multidrug Resistance; Molecular Biology and Clinical Relevance

April 10-11, 1989
Bethesda Marriott Hotel
Bethesda, Maryland

Monday, April 10, 1989

Morning Session:
*Genetics and Biology of the
Multidrug Transporter (P-Glycoprotein)*
Afternoon Session:

Molecular Diagnosis of Multidrug-Resistance

Tuesday, April 11, 1989

Morning Session:
Reversing Multidrug-Resistance
Afternoon Session:
*Cellular Responses to DNA Injury and
other Forms of Drug Resistance*

Conference Organizers:
Bruce Chabner, M.D.
Michael Gottesman, M.D.

To receive conference registration and abstract
submission information, please call or write to:
Abbe Smith or Debra Casey
Technical Resources, Inc.
3202 Tower Oaks Blvd.
Rockville, MD 20852
301 • 770 • 3153

Deadline for abstract submission is **February 1**
Deadline for conference registration is **March 1**

Circle No. 214 on Readers' Service Card