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

CO_2 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