LETTERS

Cryptography, NSF, and NSA

In view of the extensive recent discussion (News and Comment, 31 Oct., p. 511) of the respective roles of the National Science Foundation (NSF) and the National Security Agency (NSA) in support of cryptologic research, I believe it may be useful to restate the Foundation's established policy in this area.

The essential points of our policy with respect to cryptologic research are these:

1) Since mid-1977, we have routinely referred proposals with relevance to cryptology to NSA for review. We will continue to do this. The practice serves to keep NSA informed of NSF's activities in this area and gives NSA an opportunity to make technical comments on proposals which can be useful in making funding decisions. It is not a "clearance" process; whatever comments NSA may make are advisory.

2) The NSF has long had a policy of encouraging other agencies to support basic research in areas relevant to their missions. We have specifically encouraged NSA to establish an unclassified basic research program and stand ready to assist that agency in this effort. We believe it is fundamentally healthy to have alternative sources of support in important areas of science and anticipate no difficulties in maintaining close coordination between NSF and NSA.

3) In cases in which alternative sources of support are available, we routinely encourage principal investigators to apply to such sources as well as to NSF. However, if an investigator prefers to apply only to NSF, we will consider the proposal in the usual manner, without prejudice, and reach a decision on funding using our usual criteria and peer review process.

4) The NSF does not expect that the results of the basic research which it supports will be classified, except in very rare instances. The NSF does not currently have classification authority, but it has responsibility, under routine executive orders issued by both the current and previous administrations, to refer any information which it believes might require classification to the agency with appropriate subject-matter interest and original classification authority. For cryptologic research, that agency is NSA. The important point here is that it makes no essential difference, in terms of the likelihood of classification, whether research is supported by NSF or NSA. This policy is of long standing, and applies to all areas of research.

5) The NSF has long-established reporting requirements which allow it to meet its responsibility for prudent use of public funds. These might not be adequate in all cases where research could have special relevance to national security, and in such cases we may consider special reporting requirements. We have not done this in the past, and we may not have to do it in the future. If we did have to establish such reporting requirements, however, we would regard this not as a change in policy but simply as a change in administrative procedure necessary to apply a long-standing policy to a changed situation.

In summary, NSF will continue to support cryptologic research, will continue to coordinate such research with NSA, and will continue to encourage NSA to develop its own basic research support program. The results of such research have not been classified in the past, and we do not expect them to be in the future, but we will ensure that our reporting requirements are adequate to allow us to meet our responsibilities with respect to possible classification. Most important, NSF has a fundamental policy of supporting the best research it can find in all areas of science and engineering, with the fewest possible restrictions on investigators.

DONALD N. LANGENBERG
Office of the Director, National Science Foundation, Washington, D.C. 20550

I find it very strange that the Public Cryptography Study Group was put together by the American Council on Education, which represents university administrators, rather than by the mathematical community. As a result the group seems to have missed the essential feature of modern-day communication of information among mathematicians. Most new results in mathematics are circulated by means of preprints at least 1 to 2 years before they are published. Furthermore, preprints are usually sent out simultaneously with the submission of a paper for publication. Thus prepublication review of math journals (voluntary or otherwise) by the NSA would do little to impede the circulation of new results in cryptography obtained by mathematicians not affiliated with the NSA.

If the NSA seriously wants to restrict such circulation, it would have to prevent individual researchers from mailing out preprints of new results which the NSA deems relevant to cryptography. How does the NSA propose to do this? What does the NSA consider as being

work relevant to cryptography? The work of Miller (*1*) on primality depends on the truth of the generalized Riemann conjecture, and it is not inconceivable that future factoring algorithms would also depend on basic results in number theory of the same ilk. Would that then mean that all future work on the Riemann conjecture would have to be cleared by the NSA before publication? What about general work on zeta functions that might relate to the Riemann conjecture?

Similarly the work of Rivest, Shamir, and Adleman (*2*) is based on number-theoretic results attributable to Euler and Gauss among others. Does that then mean that all future extensions of Gauss's and Euler's work must be cleared by the NSA before they can be discussed with colleagues?

The threat of possible classification of a research result as well as the knowledge that publication would be delayed due to the extra NSA review is sure to have chilling effects on the eagerness with which nontenured researchers would approach problems relating to cryptography. A major result, therefore, of an NSA review will undoubtedly be less research in this area. Is this one of the NSA's aims?

It seems to me that the scientific community should give much more thought to the question of the implications of prior restraint and should oppose it. If the NSA wants to exercise a policy of prior restraint, it should either be forced to obtain a legislative mandate for such a policy or made to test its current authority in the courts.

RICHARD MANDELBAUM
Department of Mathematics,
University of Rochester,
Rochester, New York 14627

References

1. G. L. Miller, thesis, University of California, Berkeley (1975).
2. R. Rivest, A. Shamir, L. Adleman, *Commun. ACM* (February 1978).

Participatory Management

Amitai Etzioni (Editorial, 22 Aug., p. 863) concludes that "We have overburdened our industrial machine, the modern American economy. . . . We have indulged in overconsumption . . . and underinvestment. This is reflected in most . . . components of the industrial system . . . . Once the broader picture is drawn, the corrective practically suggests itself: a decade or so of reindustrialization of America . . . ."

The manner in which decisions are made and implemented to modernize equipment or plant may have very considerable influence on payoff from the investment. Many organizations overlook this point in their managerial decision-making. As an illustration, a small steel company that I was consulting with a few years ago decided to install a new furnace at the cost of several million dollars. This furnace had the rated capacity to yield x melts a day with fewer workers, compared with the existing furnace from which the company was getting an average of $3/5x$ melts per day. The potentially much more efficient and productive furnace seemed necessary to lower costs and thus make it possible to compete with the Japanese steel imports that had seriously decreased this company's share of the market.

The manner of planning, making, and implementing that decision was (characteristically) unilateral—the company's top management and engineering department just arranged with the furnace manufacturer to build and install the new equipment, without involving the various stakeholder groups (union, workers, foremen, and so forth) in the plan. The result: Because of some design errors (not all relevant personnel were consulted in the planning), inadequate training with the new equipment, and the workers' fear of losing their jobs by potential technological displacement, yield from the new furnace was only about the same number of melts a day as that from the old furnace—until union-management relations improved and a more participatory style of management was introduced.

Etzioni's Rx includes (among his priorities) the shoring up of human capital. One demonstrably effective way to do that—and to improve productivity and product quality in the process—is through joint management-labor efforts at improving the quality of working life. The nature of such efforts, and of conditions needed to optimize the likelihood of sustained success, has been well described in readily available articles and books. Despite evidence offered of outcomes such as markedly improved morale, job satisfaction, productivity, product quality, and overall economic performance, the spread of this managerial modus operandi has been slow.

EDWARD M. GLASER
Human Interaction Research Institute,
10889 Wilshire Boulevard,
Los Angeles, California 90024

Erratum: The correct surname of the first editor of *The Universe at Large Redshifts*, reviewed in the issue of 14 November, p. 781, is Kalckar.