LETTERS

Cryptography Research Funding

I believe it is necessary to correct some misconceptions about the acts of the National Security Agency (NSA) as described in the article "Cryptography: A new clash between academic freedom and national security" (News and Comment, 29 Aug., p. 995).

NSA, as the primary user of cryptography and research in cryptography in the government, is increasingly interested in investing in primary research in cryptography as well as related fields, such as mathematics. Up to now this effort has been by means of entering into contracts with companies and institutions, although we are hoping to expand our efforts to include grants for significant primary research. This effort is meant in no way to supersede or freeze out any other funding mechanisms for research in cryptography.

In particular, although NSA has provided assistance to the National Science Foundation (NSF) for the last few years in evaluating research proposals in cryptographic areas, NSA does not now have and does not intend to seek the authority to prohibit NSF funding in this area. We do hope, however, that NSA will become an increasingly important sponsor of research in this area in addition to other sources of financing currently available.

I anticipate that the results of most of the research funded by NSA will raise no direct questions of national security and could be published and otherwise publicly released. On occasion, because of the nature of cryptographic materials and of the work done by NSA, it may be necessary to classify resulting publications because of their impact on the national security. We are currently working out the procedures for such classification, which I hope would permit sufficient channels of review and appeal to assure the researchers working with NSA that the agency is not acting arbitrarily with regard to classification. Such mechanisms for review and classification are commonplace to anyone who has worked under contracts or grants for the Department of Defense. I have asked Leonard Adleman and Ronald Rivest for their views on how such mechanisms should work, and I would hope that satisfactory procedures can be developed.

B. R. INMAN

National Security Agency, Fort George G. Meade, Maryland 20755

Recent articles in *Science* about the potentially chilling effect of prior restraint on cryptographic and related research fields suggest impacts that could extend far beyond the comparatively narrow concerns of security, federal research funding, and academic tenure. One commentator is quoted (29 Aug., p. 995) as having said he believes a leading NSA figure in the dispute really does not "understand how the university and academic community works." There now may be sufficient cause to wonder if some NSA members understand how security works.

For the sake of argument one could well imagine that another nation's security service would be most pleased to champion the cause of prior restraint on cryptographic research in the United States on the grounds that it would

1) Hamper our scientists' capacity and willingness to undertake some aspects of basic research in such vital areas as mathematics, information science, and artificial intelligence.

2) Decrease the probability that U.S. scientists would appreciate the potential cryptographic significance of scientific work in other countries.

3) Diminish the incentive for research in the private sector by discouraging U.S. computer and communications manufacturers from developing cryptographic hardware and software to meet the growing private demand. This in turn would seriously compromise their ability to compete in international and domestic markets with foreign manufacturers who would be unrestricted by NSA policy. Conceivably, NSA might soon have to purchase its own cryptographic hardware from, say, Japanese manufacturers.

4) Perpetuate an anachronism of the 19th-century diplomacy of sealed royal letter boxes whose keys are worn around the necks of foreign ministers. Restricting cryptographic traffic and methodology to a security elite serves only to narrow sharply the focus of would-be interceptors and decipherers.

It is unfortunate that, in the extensive literature on cryptography, security, privacy, and related matters, surprisingly little appreciation is shown for the potentially positive applications of these functions. Only recently, through advances in electronic computation and communication, has it been feasible to explore the rewarding applications of truly anonymous information-gathering: protecting the rights of experimental subjects; facilitating anonymous peer review; enhancing scientific communication; and pre-

serving and enhancing confidentiality between professionals and their clients.

Such critical matters should not be subordinated to the narrow considerations of interagency jurisdictional disputes. NSF's peer review processes may not be perfect, but they are apt to be vastly superior to the staff resources that NSA may command in judging scientific research. If NSA wishes to underwrite scientific exploration of matters related to cryptography, it would do well to confine its role to complementary funding of basic research and the commission of such proprietary applications as it may require.

ROBERT BEZILLA
Benson & Benson, Inc.,
18 Nassau Street, Post Office Box 269,
Princeton, New Jersey 08540

Condor Conservation

The opening paragraphs of Constance Holden's account of the controversy surrounding the death of the young condor (News and Comment, 8 Aug., p. 670) contain a few errors of fact and interpretation.

Holden refers to the condor "plying a 50,000-square mile area in the mountains of central California." This is somewhat misleading. The condor's present range comprises a 50,000-square-mile area shaped in the form of a great arc or "U" extending around the southern end of the San Joaquin Valley. Starting far up the Coast Range in Santa Cruz County, the condor range extends southward down the Coast Range almost to Los Angeles, westward across the Transverse and Tehachapi ranges, then northward up the western slope of the Sierra Nevadas into Fresno County. Within that vast area of mountains, foothills, valleys, and dry rangelands about 50 percent is already in public ownership, and less than 1 percent is closed to human entry in order to protect known condor nest sites and roosting areas. The proposed Sespe-Frazier Wilderness closure would add some additional protection to another 1 percent. The fact that approximately half of the condor range is privately owned bears obvious implications for any condor conservation program.

The condor has not been treated as an "endangered" species since 1949. This term did not come into general usage until the mid-1960's, with the passage of the Endangered Species Preservation Act of 1966. The condor received international recognition as a "threatened" species in 1949 when the International Technical Conference on the Protection of Nature included it on a list of 13 of the world's birds "in need of emergency action if they are to be saved from extinction" (*1*).

The date of the young condor's death was 30 June, not 8 June.

A Condor Recovery Plan was not "originally launched" by California in 1975. The original California Condor Recovery Plan was drafted by a team consisting of representatives of the U.S. Fish and Wildlife Service, the U.S. Forest Service, the U.S. Bureau of Land Management, the California Department of Fish and Game, and the National Audubon Society.

Topa Topa, the only California condor now in captivity, is not at the San Diego Zoo. This condor has been at the Los Angeles Zoo since 1967, which is a matter of some controversy. Many of the biologists who have reviewed the condor program have recommended that Topa Topa be transferred not to the San Diego Zoo but to the new condor breeding facility being constructed on an isolated, secure hilltop within the closed-to-the-public portion of the San Diego Wild Animal Park.

The rest of Constance Holden's article is a remarkably thorough and balanced treatment of this highly controversial issue.

RICHARD L. PLUNKETT
GLENN PAULSON
National Audubon Society,
950 Third Avenue,
New York 10022

References

1. C. B. Koford, *The California Condor* (Research Report No. 4, National Audubon Society, New York, 1953), p. 136.

Lunar Topography: Galileo's Drawings

I will not respond to Feyerabend's unsupported statements of opinion about the quality of Galileo's lunar observations (Letters, 1 Aug., p. 544) with a point-by-point refutation, since the facts, as given partially in my previous letter (2 May, p. 446) and more fully in my original paper (*1*), speak for themselves. Suffice it to add that Galileo's verbal descriptions of lunar surface topography are remarkably accurate and graphical, once the features being described have been determined; his drawings are at least as good as one might expect from a nonartistic person (which he admits) using an unmounted, 20-power, poor-quality, narrow-field, dim-imaged telescope in cold midwinter with a flickering candle for illumination. Although size reduction and further reproduction will undoubtedly cause loss of some of the finer points of correspondence at the terminators, I append without comment two of Galileo's less often seen but typical sketches together with photographs taken at similar phases for comparison.

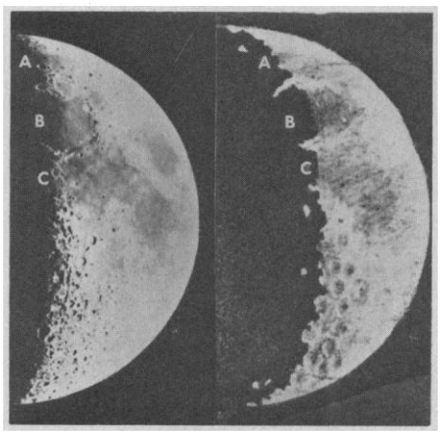

Fig. 1. Galileo's original sketch (right), deduced to have been made at about 5 p.m. Padua time on 2 December 1609, with photo (left) for comparison.

EWEN A. WHITAKER
Lunar and Planetary Laboratory,
University of Arizona, Tucson 85721

References

1. E. A. Whitaker, *J. Hist. Astron.* **9**, 155 (1978).

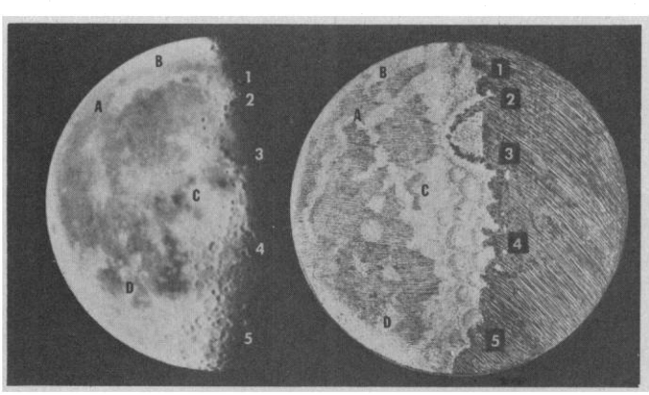

Fig. 2. Engraved version of Galileo's sketch (right), deduced to have been made about 5 a.m. on 17 December 1609, with photo (left) for comparison. Galileo naturally paid greater attention to the terminator because of the topography revealed there; this is reflected in the greater accuracy there compared with the remainder of the disk.