Letters

Computer Security and IBM

As one of the principal developers of the Data Encryption Standard (DES) algorithm, I would like to set the record straight on some serious misstatements in Gina Bari Kolata's article "Computer encryption and the National Security Agency [NSA] connection" (News and Comment, 29 July, p. 438).

In the first place, it is difficult to present a restrained response to the allegation by critics that my colleagues or I were involved with NSA and the National Bureau of Standards (NBS) in designing "trapdoors" so that a selected few would know how to break the DES algorithm. The allegation is totally false. The essence of the algorithm, including the "S-boxes." "P (permutation) box," and key schedules, was solely the product of work by my colleagues and myself at IBM. Our involvement with NSA was limited to obtaining permission to export computer equipment incorporating the DES. In no way did NSA affect the design of the algorithm.

The critics' argument that suspicion would be relieved if we were to provide our design and analysis notes is specious because those who want to believe the allegation could then argue, "How do we know you have given us everything?" I suggest instead that the only catharsis for the doubters is to apply sustained intellectual effort to seek a mathematical procedure that can solve for the key. In my professional opinion, they will fail, as have all previous attempts (including my own) during the past several years.

My estimate of the expense of building an ultralarge and fast, "brute force" machine was offered in response to a public statement made by Martin Hellman at the NBS workshop in August 1976. There was no IBM study of a "brute force" machine. However, I believed that Hellman's estimate of the cost to the manufacturer of $20 million for such a machine was off by an order of magnitude, by which I meant the cost was beyond reason.

Kolata states that IBM officials have since repudiated my comments. This also is not true.

IBM and I believe that the present key size is adequate for commercial applications for the foreseeable future. However, if for his own satisfaction, a user desires additional strength, there are numerous efficient ways of lengthening the effective key while maintaining use of the DES algorithm.

We expect the DES to be effective for a very long time.

W. L. TUCHMAN
Advanced Power Development,
Data Security Products,
International Business
Machines Corporation,
Kingston, New York 12401

Imprisoned Argentine Scientist

The undersigned members of the Cornell University faculty herewith bring to the attention of our colleagues in the scientific community the plight of Elena Sevilla, a 29-year-old Argentine physicist, who has been imprisoned without any charges for more than 18 months. The arrest took place in a hospital ward 5 days after Ms. Sevilla gave birth by cesarean section. (The facts of this case have come to our knowledge through the prisoner's sister, Alicia Sevilla, a graduate student in mathematics at Cornell.)

Elena Sevilla received the degree of Licenciado from the Instituto Balseiro of Bariloche in 1973. Thereafter she taught at the Universidad del Sur in Bariloche and did research on atomic collisions at the Instituto Balseiro.

In September 1975 her husband was arrested in Puerto Madryn; on 27 November Elena herself was arrested in the hospital of her hometown, Mendoza. Her arrest had been ordered by the federal judge in charge of her husband's case, but no charges were laid against her.

In January 1976 Ms. Sevilla was moved to the city of Rawson, where she was acquitted for lack of evidence. Nevertheless, the military intervened and ordered the Federal Police to continue her detainment. At this point she gave up her child, who has been living with her parents since then.

Ms. Sevilla is now in Villa Devoto Jail in Buenos Aires, where she shares a cell with 20 other women and lives under a very strict regime that only allows at most 1 hour per day outside her cell and very rare visits by her immediate family.

Historically Argentine political prisoners have had the option of leaving the country in lieu of staying in jail. The junta abolished this right on assuming power but reinstituted a highly qualified form of this privilege on 27 October 1976. On 14 December 1976, Ms. Sevilla filed a petition to leave. Although she received official notice that a decision would be made within 90 days, her family received word on 1 April that her petition had been denied.

In closing, we point out that Elena Sevilla was never politically active and has never been charged with any crime. Her 18-month imprisonment appears to be a capricious act of a government that seems to have lost all consideration for the rights and welfare of its own citizens.

Our purpose in writing this letter is to solicit help from those of our colleagues who maintain connections with prominent Argentine scientists. If you have such acquaintances, we ask you to seek their help in freeing Ms. Sevilla from her harrowing imprisonment so that she may resume her family life and scientific career.

KRAIG ADLER, SIMON H. BAUER
HANS A. BETHE, THOMAS EISNER
ROGER H. FARRELL
MICHAEL E. FISHER
PETER J. GIERASCH, KENNETH GREISEN
DONALD F. HOLCOMB, PETER J. KAHN
HARRY KESTEN, JACK KIEFER
JAMES A. KRUMHANSL
STEPHEN LICHTENBAUM
G. R. LIVESAY, FRANKLIN A. LONG
THOMAS R. PODLESKI, CARL SAGAN
HAROLD A. SCHERAGA, FRANK SPITZER
MOSS E. SWEEDLER, YERVANT TERZIAN
JAMES E. WEST, BENJAMIN WIDOM
Cornell University,
Ithaca, New York 14853

Rail Transit and Energy Consumption

In a recent issue (Letters, 1 July, p. 7), C. Kenneth Orski comments on my earlier work (*1*). The brevity of my original remarks has produced some misunderstandings:

1) When I said that San Francisco's Bay Area Rapid Transit (BART) system

was typical of modern rail transit, I meant typical only with respect to energy considerations—its energy construction cost per system-mile is the same as that of three other modern systems (Atlanta, Baltimore, and Washington, D.C.); and its operating energy per vehicle-mile is the same as that of the only other fully operating modern system (Philadelphia).

2) I certainly don't believe in the blanket encouragement of highway construction.

Orski also makes two suggestions for changing the analysis. I am happy to take his advice. First, he suggests that I deflate all costs to 1963 dollars before computing their energy content. If the Federal Highway Administration construction cost index is used, BART would have cost $962 million in 1963, and the 67.1 lane-miles of highway that BART replaces would have cost $26.4 million.

Second, Orski suggests that I take into account the extra cost of highway bridge building. We know that BART has removed enough traffic from the San Francisco Bay Bridge to reduce highway needs by about three-fifths of a lane (*2*, p. xv). The cost for the eight-lane Southern Crossing bridge proposed for San Francisco would have been $144 million in 1972. Buying one lane's worth of that, instead of the three-fifths of a lane which is needed, would have cost $11.1 million in 1963.

Adding the cost of the bridge to the highway estimate above and converting both this figure and the BART cost into 1963 energy equivalents shows that BART cost 7.1×10^{13} Btu's more than the highways it replaced.

If the only alternative to BART were a 14-mile-per-gallon automobile, then BART's saving of operating energy would be 680 Btu's per passenger-mile, which implies that it would take 237 years for BART to repay even its construction energy. (The payback time against a 27.5-mile-per-gallon automobile is infinite.)

Hence my original conclusion that BART is an energy waster. This does not imply that it should not have been built, though, as there are other potential benefits from such systems—which Orski and I agree must be evaluated on a case-by-case basis.

CHARLES A. LAVE
Department of Economics,
University of California, Irvine 92717

References

1. C. Lave, *Science* **195**, 595 (1977).
2. R. Ellis and A. Sharret, *Transportation and Travel Impacts of BART: Interim Service Findings* (Report No. FR 6-3-75, Peat, Marwick, Mitchell, San Francisco, 1976), pp. 71 and 165.

Radioactive Waste Disposal: An Environmental Standard

The National Academy of Sciences–National Research Council's Committee on Radioactive Waste Management has recently established a panel to study how the implementation of an environmental standard governing the disposal of high-level radioactive waste in geological formations can be verified. Although the standard has yet to be determined, for purposes of this study it is assumed to lie within the range of 0 to 25 millirems per person per year and to be applicable for at least 1000 years.

Because of the long time scale involved and the possibility that typical monitoring techniques may adversely affect the integrity of the waste disposal site, verifying the implementation of an environmental standard, as described above, is a unique and difficult task. Consequently, to assist the panel in carrying out its study, I am requesting that *Science* readers communicate any information, ideas, or philosophical approaches regarding this problem to Dr. Richard Milstein, Staff Officer, Committee on Radioactive Waste Management (JH 804), National Academy of Sciences, 2101 Constitution Avenue, NW, Washington, D.C. 20418.

ROBERT PENDLETON
Panel on the Implementation Requirements of Environmental Standards, Commission on Natural Resources, National Research Council, 2101 Constitution Avenue, NW, Washington, D.C. 20418

The Diesel's Advantages

It was satisfying to see in *Science* a sensible and accurate assessment of the automobile pollution situation (Editorial, 5 Aug., p. 517).

The diesel car, while it has problems, such as aldehyde and particulate emissions, roughness, noise, and cold-starting, has unequaled advantages and promise as an optimum solution to the difficult compromise between energy and pollution.

Other types of engine can be made to meet the Clean Air Act's ultimate emission specifications of 0.4 gram of hydrocarbons (HC's), 3.4 grams of carbon monoxide (CO), and 0.4 gram of nitrogen oxides (NO_x) per mile, but only by the use of catalysts in combination with a precarious balance of adjustment not likely to survive very long if present automobile maintenance practices remain the same. People will destroy catalysts by using leaded fuel because it is 3 to 4 cents cheaper, they will deactivate exhaust-gas recirculation systems to improve performance and economy, and they will neglect ignition and spark plug maintenance until misfiring takes place. Programs to coerce the car owner into maintaining the emission controls in his car will be expensive, only partly effective, and politically unpopular.

The diesel car requires no add-on units or precise adjustments to maintain its low level of emissions (0.3 gram of HC's, 2 grams of CO, and 1.5 grams of NO_x per mile, even for a good-sized car) or to maintain its fuel economy. For this reason, a new diesel car's margin of economy (25 percent) over a new gasoline car can be assumed to be larger when the lives of the two types of car are considered. Finally, diesel fuel has some formidable advantages over gasoline: (i) it requires no toxic additives, such as lead; (ii) it is not explosive and makes no evaporation pollution; and (iii) it yields more energy at a lower cost in energy and money for refining. But the limits on NO_x emissions presently specified by the Clean Air Act make use of the diesel in the United States impossible, and little attention has been paid to diesel development in this country.

If all passenger cars were putting out not more than 1.5 grams of NO_x per mile, emissions would be small in comparison with what they are now, and most probably small in comparison with what they would be if all cars had been built to meet the 0.4-gram limit when new (given current maintenance practices). Not only would it be a very large economic penalty to enforce a high level of maintenance on all car owners, but it would require facilities that do not exist at present.

FREDERICK J. HOOVEN
Thayer School of Engineering,
Dartmouth College,
Hanover, New Hampshire 03755

New Texico?

We in New Mexico have for decades been observing the gradual intrusions of Texans into our space, but not until Deborah Shapley (News and Comment, 8 July, p. 138) made Arizona contiguous with Texas did we realize the extent and suddenness with which this massive transposition has occurred.

W. LEE GARNER
Sandia Laboratories,
Albuquerque, New Mexico 87115