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