Cryptography: A New Clash Between Academic Freedom and National Security

National Security Agency seeks to influence science agency policy

At the National Security Agency's (NSA) prodding, the National Science Foundation (NSF) last week told a computer scientist that it would withhold funds on certain parts of his cryptography research grant because they impinge on national security. This may be the beginning of a new sort of restraint on cryptography research.

About 3 years ago, academic scientists became interested in cryptography—both because the problems are of theoretical interest and because, for the first time, there is a need for codes in the private sector. With the advent of electronic fund transfers and electronic mail and with the widespread use of computers for storing and processing data, there has been a demand for good codes to keep sensitive computer messages and data secure.

Before, cryptography had been almost exclusively the domain of the military, in particular of the NSA. Ever since academic scientists took an interest in cryptography, they have had the feeling that the NSA was breathing down their necks. They have been told that their work may threaten national security and that it may be necessary to institute prior restraints on their research (*Science*, 27 June 1980). A number of academic scientists express grave concerns about these developments and have been waiting for the other shoe to drop. Now, it appears, it has.

The latest development occurred on Thursday, 14 August, when Leonard Adleman of the Massachusetts Institute of Technology (MIT) and the University of Southern California got a telephone call from Bruce Barnes of the NSF, who told him that parts of his grant proposal would not be funded. This is apparently the first time the NSF has refused funds to a researcher for reasons that have nothing to do with the merit of his proposal. When Adleman questioned Barnes further, he was told it was an "interagency matter."

The interagency matter turns out to involve the relationship between the NSF and the NSA. It has implications which, to a number of academic scientists, appear particularly ominous.

Acting NSF director Donald Langenberg refused to talk in any substance about his agency's relationship with the NSA, pointing out that he has only been acting director for 2 months and that he is still getting his bearings. But Vice Admiral Bobby Inman, the director of the NSA, talked freely with *Science* about his agency's contacts with the NSF.

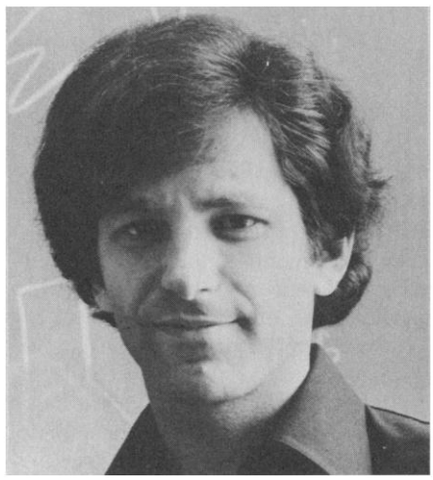
According to Inman, the reason the NSF chose not to fund parts of Adleman's grant proposal is that NSA wants to fund the research itself. The NSA, says Inman, first became interested in funding cryptography research when academic scientists started moving into the field. About 2½ years ago, Inman initiated conversations with the director of the NSF, then Richard Atkinson. "We got authority, good ideas, and help from Atkinson," he says. Since the heads of the two agencies began talking, the NSF has routinely sent all of its cryptography proposals to the NSA for review.

Finally, the NSA was ready to initiate its own funding. Two NSF proposals looked ideal for the NSA to support. "I wrote to Langenberg suggesting that these would be good ones on which to start," Inman says. One of the proposals was from Adleman. The other was from Ronald Rivest of MIT, who is Adleman's colleague.

Officials at the NSF refuse to talk of the matter, saying they are forbidden to discuss proposals until funds are formally granted or denied. Inman, however, reports that the NSF was undecided on how to react to the NSA's desire to fund Adleman and Rivest. Rivest was not so much of a problem because he had mistakenly submitted his proposal to renew his grant 1 year early. Barnes called Rivest and told him that he may hear from the NSA. So far, he has not. But Adleman was another matter. The NSF, apparently, did not want to cut off his funds entirely while it wavered on the NSA's request, so it informed Adleman it would fund only part of his proposal—the part that did not interest the NSA.

One day after hearing from the NSF, Adleman got a call from Inman, who explained that the NSA wanted to fund his proposal. Adleman was disturbed. "In the

Vice Admiral Inman



Leonard Adleman

Donald Langenberg

0036-8075/80/0829-0995$00.50/0

present climate, I would not accept funds from the NSA," he says. He worries about what terms the NSA might exact and points out that he applied to the NSF, not the NSA, and that he does not want any part of an implicit commitment to the NSA. He wonders what would happen if the NSA wanted to classify his work and he refused. Would his funds be cut off? If so, he believes he would have no due process. He is concerned about the NSF's agreement with the NSA. "It's a very frightening collusion between agencies," he says.

Adleman is a theoretical computer scientist. His research, says Rivest, "has to do with a fundamental understanding of what it means for a computation to be hard or easy." Rivest is gravely concerned that the NSA wants to fund such research. "I'm shocked," he remarks. "What worries me is that the line [between what is and what is not cryptography] is being pushed in a way that affects our ability to do basic computer science research."

What would happen if the NSA were to fund Adleman's work and to decide it should be classified for national security reasons? "We would not automatically classify the work. We would want to discuss with him the possibility of classifying it," Inman says, but he concedes that in such a case NSA would try to persuade Adleman that classification was necessary.

George Davida of the University of Wisconsin in Milwaukee had his own run-in with the NSA when the agency tried to slap a secrecy order on his invention of a cryptologic device. Since then, he has been extremely concerned about the agency's encroachment in academic research. "I really don't think Inman understands how the university and academic community works," he says. "Adleman is not tenured at MIT. If he begins to have trouble getting funded or publishing his research it could literally ruin his career."

Inman, however, thinks the agency is being entirely reasonable and that the NSA's funding of cryptographic research will work. "We just need two or three people who aren't scared to death of us. I really am dealing with sociological problems on both sides," he says.

In contrast to Inman, who seems quite clear about what his agency wants, the NSF appears unable to make up its mind. "We're still trying to work out a policy [on cryptography research]," says Langenberg. But if the NSF continues to delay, its policy may end up being worked out for it, and academic scientists may find that, without any public discussions, there are prior restraints on their research.—GINA BARI KOLATA

Navy Lab Concludes the Vela Saw a Bomb

Unlike the White House, the federal laboratories prefer the sinister explanation of the 22 September flash

Despite its best efforts to lead the choir, the President's science office has been unable to get the government's technical community to agree on whether or not someone secretly exploded a nuclear bomb on 22 September 1979 in the Southern Hemisphere. Discordant voices continue to rise above the White House mood music, whose theme is that probably nothing happened, and if something did, it cannot be proved (see *Science*, 1 August, p. 572).

The latest dissent comes from Alan Berman, director of research for the Naval Research Laboratory (NRL) and coordinator of a 300-page study sent to the White House on 30 June. Berman says that his report, the only comprehensive and original analysis commissioned by the government, concludes that there was a "nuclear event" on 22 September. The location—somewhere near Prince Edward Island, South Africa, or Antarctica.

When a signal was first received from a Vela surveillance satellite in 1979, it was accepted as evidence that a nuclear blast had occurred. South Africa was suspected of being the perpetrator because the flash was sighted near its borders. Then two journalists who were writing a book on Israel's nuclear program claimed to have learned that Israel and South Africa were cooperating to build a small nuclear device. Israel became a second suspect. Some saw the Soviets' hand in the plot. All these countries denied involvement.

The Vela's message proved impossible to corroborate. Lacking any clear physical proof that a blast had occurred, the White House assembled a panel of independent scientists to review all the data that had been collected. The group, chaired by Jack Ruina of the Massachusetts Institute of Technology, concluded in April that there was not enough evidence to support the original reading of Vela's signal. It was judged to have been caused by a natural event.

Berman's split with the Administration is notable because he is one of the few dissenters to speak publicly. Others may have been dazzled by the stellar cast of the White House panel, which was loaded with Nobel laureates, or silenced by a healthy respect for security regulations. One national laboratory executive who disagrees with the White House said, "I am keenly aware as a result of such things as the litigation that resulted from the *Progressive* case [in which U.S. prosecutors alleged that scientists leaked secret data to a free-lance writer] that our security laws are pretty effective for people who work in the industry as I do. . . . There may be folks who can talk a lot about such things that support the White House hypothesis. I can't talk that much about the things that support our hypothesis because I've got a different set of ground rules."

Scientists and intelligence analysts who have worked on the puzzle for the last year have divided into two camps, as one at the Los Alamos Laboratory in New Mexico put it: the believers and nonbelievers. The former think that the light sensors on the Vela surveillance satellite actually did "see" a bomb blast, and the latter take sides with the panel of distinguished experts convened by the White House, who think that some other natural event caused the satellite to make a false report. The believers in the Vela's signal tend to think that the White House is impelled by a political motive to ignore uncomfortable facts. "The crux of the matter," one said, "is that the White House is afraid that if this [Vela report] is true, its nuclear nonproliferation policy would be shot to hell. So they said, let's convene a panel

0036-8075/80/0829-0996$00.50/0