Code Researchers Fear NSA's Control

By Philip J. Hilts
Washington Post Staff Writer

The National Science Foundation, in cooperation with the National Security Agency, plans to withhold certain funds for research in cryptography—the science of codes.

The move has raised fears in academic circles that eventually all financial support for such work will be taken over by the intelligence agency.

Such a development, many believe, would effectively place control of this field in the hands of the intelligence agency, with the result that much research important to society could end up locked in the so-called "dark chambers" of NSA.

Until recent years, cryptography was of interest almost exclusively to military and intelligence agencies.

But now, with the society clicking steadily toward electronic storage and communication of practically all kinds of information, the science has become critical for business and home computer systems as a means of guarding their privacy.

The situation has been complicated by the fact that the best work on cryptography in recent years—new codes that are in practical terms truly unbreakable—has been done by university researchers, not by intelligence agency cryptographers.

Ever since the unbreakable codes were openly published in 1977 by scientists such as Leonard Adleman and Ronald Rivest at MIT, the NSA has made it clear through a number of incidents that it would like to have more control over cryptographic researach.

It was a grant proposal by Adleman to NSF that precipitated the latest round of controversy.

NSF has recently reached an agreement with NSA to cooperate in the giving of cryptography grants—a common arrangement for NSF when it knows that other agencies are interested in a particular subject. Under such an agreement, NSF may pay for some of the work and pass other parts of it along to the second agency for support.

Two weeks ago, Adleman was told by NSF that part of his proposal would be funded and part would not, but that NSA was interested in picking up the unfunded part. This was quickly confirmed by NSA.

"I understand that the mission of the NSA might include bringing cryptography research under its control to a degree," Adleman said. "I can see the predatory animal as noble in its own way. At the same time, I don't like being the prey."

He feels it is important that his and other researchers' work be openly available to science and the public, unless the government can prove some overriding need of national security. He is afraid that the NSA, because of its mission, would be unlikely to decide the question fairly.

When NSA feels national security may be threatened, it can bar researchers who work for it from publishing their papers.

"The NSF has been strongly in favor of academic freedom in the past, and I am afraid that they may be not advocating that position strongly enough in this case allowing the NSA to have their way too much," Adleman said.

Adleman said he was surprised to find that a proposal he sent to NSF now was under consideration for funding by NSA, and he was unnerved because he and other university cryptography researchers "have been skirmishing with the NSA for three years now. That has had a chilling effect on us," he said.

He said that a letter was once received by a meeting of the researchers, telling them that their work or public discussion of it might violate the law. The letter was from a man in Bethesda who did not identify himself, but Adleman says he later found out that the man worked for NSA.

MIT also told Adleman to stop sending out reprints of his most popular cryptography paper until lawyers could determine if it might make him liable for prosecuton.

The NSA also in the past three years slapped a secrecy classification on the work of George DeVita at the University of Wisconsin when he applied for a patent on one bit of cryptographic work.

The NSF has had for some time a panel working on the issue of academic freedom versus national security and how such situations might be handled, but that panel has not been able to devise a policy to guide NSF on cooperation with NSA.

Kent Curtis, head of the computer sciences division of NSF, said that the action NSF took would be normal in any other case and sharing grants saves NSF much needed money. But the case is made special because of the possibility that the NSA might put security classifications on any work that scientists might do for them.

"This situation is a clash of valid national security interests and the need and interest of the public to know about and use cryptographic research," Curtis said.