Boosting cryptography's role in security

The U.S. State Department has regulations restricting the export of cryptographic software. Applying these rules, however, can lead to contradictory actions.

In 1994, officials ruled that a cryptography textbook that contained complete computer programs for several strong cryptographic schemes was freely exportable. Yet, when the same programs were put on a computer diskette, the department argued that the diskette qualified as a "defense article" and required a special license for export.

These rulings were obtained by Philip R. Karn Jr., a network engineer who works for Qualcomm in San Diego, to test the regulations governing the export of cryptographic technology. Karn's appeal of the decisions remains mired in the courts. Last week, a panel of the National Research Council released a report, "Cryptography's Role in Securing the Information Society," to highlight the importance of cryptography for the future of information technology and to point out shortcomings in current government policy on export controls.

Representing a wide range of interests, the 16-member panel recognized a tremendous and widespread need for technology to encrypt electronic information, making it easier to protect financial data, telecommunications networks, and other assets from crime and terrorism. Such technology could also provide greater privacy for individuals and boost the competitiveness of U.S. companies in international markets, the panel argued.

"Current [government] policy discourages the use of cryptography," says panel chair Kenneth W. Dam of the University of Chicago Law School.

The panel members strongly endorsed the idea that no law should restrict the manufacture, sale, or use of any form of encryption within the United States. It recommended progressively relaxing, though not eliminating, export controls on encryption technology.

Products incorporating a highly regarded cryptographic scheme known as the Data Encryption Standard should be easier to export, the panel suggested. One effect of such a change would be to encourage U.S. companies to include this high level of cryptographic security in their products. Congress is already considering legislation to relax export controls.

Even if the U.S. government heeds the suggestion, however, it may still be too little, too late, says Jim Bidzos of RSA Data Security in Redwood City, Calif. One Japanese company is already producing and selling throughout the world computer chips that offer considerably stronger cryptographic security than the Data Encryption Standard, he remarks. U.S. companies are currently shut out of this market.

The panel also concluded that the government plan to introduce so-called escrowed encryption is "relatively untried and entails its own potential risks." In this scheme, a third party (in addition to the message recipient) holds the digital keys required to unlock encrypted information (SN: 8/28/93, p. 394; 2/12/94, p. 100). Such an approach is attractive to law enforcement and national security agencies because with a court order they could obtain the relevant key from the third party and decipher the otherwise incomprehensible data.

"The NRC report is a very valuable contribution to this debate," says Bruce McConnell of the Office of Management and Budget and cochair of the interagency working group on cryptography policy. The report recognizes that a balance must be struck between computer security and concerns about national security and law enforcement. "Where we differ is in exactly how you achieve that balance," he notes.

"In the past, government officials have tended to treat many aspects of cryptography policy as top secret," Dam says. Most of the panel members had access to this classified information, and they concluded that such knowledge isn't essential for an informed public debate on cryptographic issues. —*I. Peterson*

Gene therapy strategy repairs RNA, not DNA

In a significant test of a novel strategy for gene therapy, investigators have inserted genes for unusual enzymes called ribozymes into mammalian cells and repaired the faulty protein-making instructions sent out by a mutant gene.

The ribozymes, which derive from single-celled pond organisms, had previously performed genetic repair jobs in test tubes and inside bacteria. Researchers were uncertain, however, whether these corrective enzymes could function within the radically different chemical milieu of mammalian cells.

"It's fantastic that it's working," says Nava Sarver of the National Institute of Allergy and Infectious Diseases in Bethesda, Md., which funds several efforts to treat AIDS with ribozymes.

Unlike most enzymes, which are proteins, ribozymes are made of RNA, a single-stranded, DNA-like molecule consisting of sequences of chemical components called nucleotides. The ribozymes used in the gene therapy experiments have the unusual ability to splice part of their nucleotide sequence onto other RNA molecules, explains Bruce A. Sullenger of Duke University Medical Center in Durham, N.C., who heads the team that performed the recent gene therapy experiments.

That splicing talent has therapeutic potential because RNA is a vital cog in the cell's protein-building machinery. When a cell makes a gene's protein, it first copies the instructions stored in the gene's DNA into an RNA strand. This messenger RNA, or mRNA, then travels to sites in the cell where it directs the assembly of amino acids into proteins.

Two years ago, Sullenger and Thomas R. Cech of the University of Colorado in Boulder showed that in bacteria, ribozymes can repair the mRNA of a deliberately shortened gene. The ribozymes, engineered to include the missing portion of mRNA, match part of their sequence to a complementary sequence on the faulty mRNA and add on the absent nucleotide sequence.

Almost the same results have now been achieved in mouse cells, Sullenger and his colleagues reported last week at the RNA Society meeting in Madison, Wis., and in the June NATURE MEDICINE. Even though they clearly observed the correction of mRNA in the mammalian cells, the researchers have not yet established that the repaired mRNA produces a functioning protein, as it did in their bacterial studies.

In addition to repairing the mRNAs for which they were intended, the ribozymes frequently spliced their cargo onto the mRNAs of other genes. That "sloppiness" can be overcome, asserts Sullenger. "We know so much about these ribozymes there's some obvious things to try to increase their specificity."

Though many genetic diseases are caused simply by a dearth of a gene's normal protein, ribozyme-based gene therapy would be especially useful for diseases in which a genetic mutation results in the production of a damaging protein. RNA-correcting ribozymes would both eliminate these deleterious proteins and restore synthesis of the correct protein.

"You swap out the bad information and put in the good information," says Sullenger.

Correcting genetic diseases at the RNA level instead of the DNA level offers another potential advantage—timing. A disease produced by a mutant gene will not necessarily be corrected by adding a copy of a normal gene into a patient's cells; investigators cannot yet ensure that the inserted gene will turn on and off when it should. In contrast, using ribozymes to repair mRNAs made by a mutant gene preserves the normal timing of the gene's activity, says Sullenger. —*J. Travis*