would be better spent on research, and that libraries feel constrained to "buy every journal published irrespective of its overall quality" [see C. J. Ballhausen *et. al.*, *Chem. Eng. News* **51** (No. 50), 44 (1973)].
21. J. B. Cohen, Ed. *CUNY Checklist of Scientific, Technical and Medical Periodicals* (Hunter College Library, New York, 1975).
22. *Journal Citation Reports, Journal Ranking Package* (Institute for Scientific Information, Philadelphia, 1973).
23. *Am. Libr.* **7**, 609 (1976).
24. It [*Coll. Res. Libr. News* **68** (No. 3), 72 (1977)] is reported that the National Commission on Library and Information Science (NCLIS) is at work on a plan for a national periodicals system, which would operate within the copyright law. A feature of this system would be one or more national periodical centers with a comprehensive collection, which would lend periodicals or supply photocopies of articles. A final report of the task force at work on this plan is due early in 1977. A national periodicals system may help to alleviate problems posed by the new copyright law as well as by the high cost of scientific journals. But we will not know until such a plan is put into operation. In the meantime, we must deal with the problems described in this article.
25. We have no assurance that alternative forms of publications will be inexpensive. The *Journal of Chemical Research*, which began in 1977, and which is a joint publication of the British, German, and French chemical societies, for example, publishes synopses of papers in full-size copy, with complete texts of the summarized papers available in miniprint or microfiche. The 1977 subscription price of $140 per year for this journal is not much lower than the 1976 average subscription price of $148.81 for the chemistry journals shown in Table 2.
26. Fry and White (*14*, p. 9) also maintain that subsidies are needed for scholarly journals and that the most likely source of such subsidies is the federal government. They suggest that subsidies could be made either to libraries, to publishers of journals, or to authors of scholarly papers. Their proposal, however, applies to all scholarly journals, not just to those in the sciences. R. De Gennaro [*Am. Libr.* **8**, 71 (1977)], objects strongly to the now common practice of charging libraries significantly higher rates for journal subscription—which are called institutional rates—as compared with rates charged to individuals. He views this as a form of subsidy by libraries to the scholarly publishing enterprise. He points out that research libraries no longer have the funds to subsidize scholarly publication.
27. H. S. White [*Libr. Q.* **46**, 377 (1976)], convinced of the need for subsidy of scholarly publication, probably by the federal governmment, calls for a thorough study of the problem to determine how much subsidy is required and to whom it should be given. We believe that our proposal merits the most serious consideration in any such study.
28. The fact that information is an inherent part of research and the conviction that more of the resources of science, both financial and human, must be used to make scientific and technical information more readily available to those who need it is one of the themes of the Weinberg report [A. M. Weinberg, *Science Government and Information*, a report of the President's Science Advisory Committee (U.S. Government Printing Office, Washington, D.C., 1963), p. 14]. White observes that "To provide financial incentive for the completion of research, but to stop short of enabling the researcher adequately to report and disseminate his findings, appears to be inconsistent and even foolish" (*27*).
29. *Mon. Labor Rev.* **100** (No. 2), 117 (1977).

NEWS AND COMMENT

Computer Encryption and the National Security Agency Connection

Theft of sensitive or private computer data has become a serious threat to many federal agencies and private corporations. This threat is magnified by the increasing use of computers to do such things as transfer large sums of money between banks. In order to foil the would-be computer-tappers, many federal agencies as well as bankers and corporations are now buying computer equipment that converts their private data to a secret code. All government users of such secret codes and a large proportion of private users as well plan to employ a new coding system put forth by the National Bureau of Standards (NBS) and designed by IBM. But some critics suspect that this coding system was carefully designed to be just secure enough so that corporate spies outside the government could not break a user's code and just vulnerable enough so that the National Security Agency (NSA) could break it. Presumably, foreign governments could too.

The NBS encryption equipment, known as the Data Encryption Standard (DES), has just come onto the market. Federal agencies that want to encrypt nonclassified computer data are required by law to use it. Manufacturers of the equipment also see a burgeoning market in banks, insurance companies, oil firms, and other commercial concerns.

Each user of the DES—a device that can be attached to a computer—will have its own key. The key (which is a string of 56 "bits" or 0's and 1's) is used to inform the computer how to encode data with this system and how to decode it as well. Each user of the DES generates its own key, preferably by choosing the 56 digits randomly. Once a user's key is known, all of its encrypted data can be decoded. A contingent of computer scientists, led by Martin Hellman and Whitfield Diffie of Stanford University, warn that a machine could be built to determine any user's key. The catch is that the machine would be expensive to build and operate. Private corporations, presumably, would not find it economically feasible to buy such a machine. But a government agency such as NSA might find it very worthwhile to build one.

Such a code-breaking machine might not even be necessary, some critics charge. The NSA was involved in the development of the DES and it classified some critical features of the encryption scheme. The critics cannot shake the feeling that these features were classified because to reveal them would be to reveal far simpler ways to break the code.

Critics of the DES say they can well understand why NSA would find it useful to break the code. Computer equipment incorporating the DES hardware will be sold abroad as well as in the United States. The NSA would not want to encourage the sale to foreign countries of an unbreakable encryption scheme. Of course, NSA would then also have the capacity to decode domestic computer data encrypted by the DES.

The most alarming possibility, according to Jeremy Stone of the Federation of American Scientists, is that foreign governments might decode U.S. computer data. For if NSA can build a machine to break the DES code, so can the Soviet Union and others. Stone is concerned that other countries would use information from the computer data to wage economic warfare. The Soviet Union manipulated the grain market during the wheat deal, he says, and it spends large sums of money to intercept telephone messages transmitted by microwaves. The capability and motivation exist for it to build a machine to break the DES code.

Although many private companies are convinced that the DES is sufficiently secure for their purposes, some have decided not to use this scheme. For example, Robert Morris of Bell Laboratories in Murray Hill, New Jersey, says that officials of the Bell Telephone Company have decided that the DES is too insecure to be used in the Bell System. Andrew Del Preore of Banker's Trust Company in New York says that his company will not use the DES because it "did not meet all the bank's requirements."

The purported problems with the DES were first pointed out 2 years ago by Hellman and Diffie. The NBS published a description of its proposed encryption scheme in the *Federal Register* and solicited comments. Hellman and Diffie sent in several comments, among them that the key size, which determines how easy it is to break the code, seemed too small. At little extra expense, these investigators pointed out, the key size could be increased and the standard

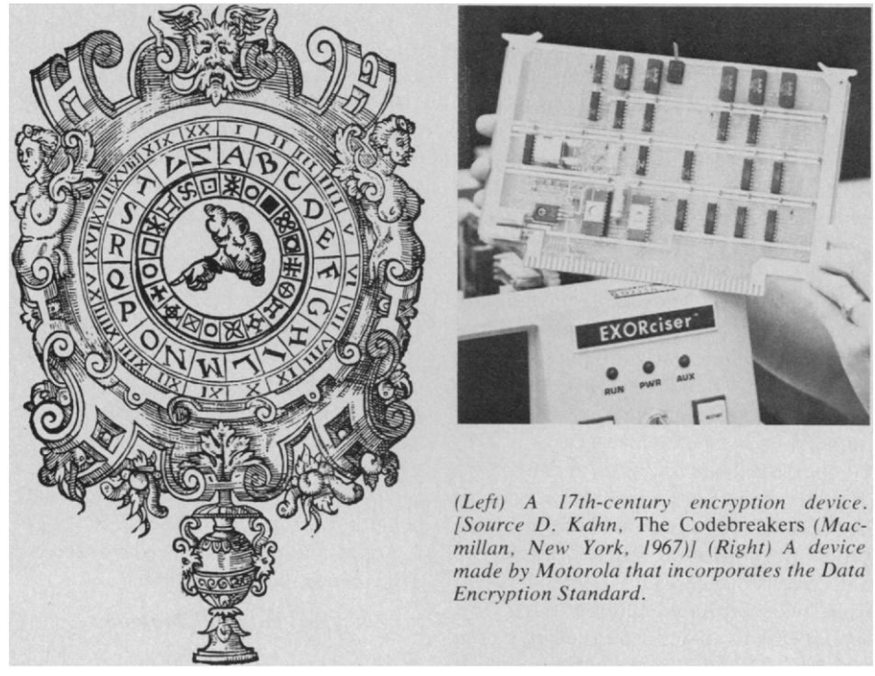
made much more secure. The military routinely uses key sizes nearly 20 times as large as that of the DES, Hellman says.

According to Hellman, the NBS politely replied to all of his and Diffie's comments except for their remark about the key size. Despite repeated letters and phone calls by Hellman and Diffie, the NBS remained elusive about the key size question. Morris says that the NBS tried its best to discredit Hellman and Diffie, referring to them privately as "the radical fringe."

The ideal way to break a code is to find some weakness in the encryption procedure. Failing that, some codes can be broken by the mathematical equivalent of brute force—by trying all possible ways to decipher an encoded message until an appropriate key is found. Hellman and Diffie contend that even if the DES has no internal weaknesses, it can be broken by brute force. Every possible combination of 56 0's and 1's can be tried until one is found that enables a known enciphered message to be transformed into a known deciphered message by means of the DES procedure. It is a standard practice in cryptography to assume that a spy can obtain a deciphered message and compare it to a coded one. Hellman and Diffie point out that, especially in commercial systems, it would be impractical to require that all old deciphered messages be kept secret or that they be paraphrased if declassified. And the NBS specifically states that the DES must be secure against this sort of attack.

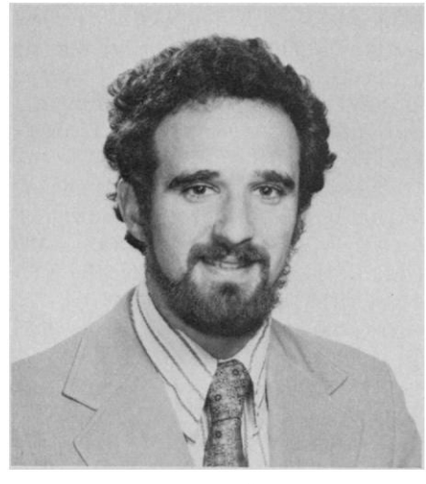
With a key size of 56 bits, the total number of possible keys is 2^{56}, or about 10^{17}. It seems hard to imagine a machine sorting through 2^{56} possibilities, but Hellman and Diffie argue that it can be done. With today's technology, it is possible to build a special search chip that can try 1 million keys per second. If one of those chips were used each second, it would still take about 10^{11} seconds or about 3000 years to complete the search. But if 1 million of these search chips were used in parallel, the entire range of possible keys could be searched in 1 day. On the average, though, only about half of the keys would be tried before the appropriate key was found, so the average search would take only a half day.

What would such a code-breaking machine cost? Hellman and Diffie estimate that the search chips would cost about $10 each or a total of about $10 million. They allow a factor of 2 for design, control hardware, power supplies, and similar expenses and conclude that the machine would cost about $20 million. When they depreciate the cost of the machine over 5 years, they conclude that the daily operating cost would be about $10,000 and that each solution would cost about $5,000.



(Left) A 17th-century encryption device. [Source D. Kahn, The Codebreakers (Macmillan, New York, 1967)] (Right) A device made by Motorola that incorporates the Data Encryption Standard.

Hellman and Diffie say further that their proposed code-breaking machine would most likely become far less costly to build and operate in the near future. They point out that the cost of computation and hardware has decreased by a factor of 10 every 5 years since the 1940's. If this trend continues, the code-breaking machine would cost only $200,000 in 10 years and each solution would cost about $50. A larger key size, however, would make it impossible to break the code in the foreseeable future. For example, if the key size were 128 bits, a search would cost $\$2 \times 10^{25}$ rather than $5000 with today's technology. On the other hand, a key size smaller than 56 bits would be totally insecure. A machine to break a 48-bit key would cost only about $78,000 and a solution about $39.



Martin Hellman

Partly in response to the criticisms raised by Hellman and Diffie and to increasing pressure from other computer specialists, the NBS held two workshops to consider the security of the 56-bit key. At the first workshop, held on 30 and 31 August 1976, computer hardware manufacturers concluded that the DES is sufficiently secure. They said that the proposed code-breaking machine could not be built before 1990 and that even then the probability that the machine could be built is only 10 to 20 percent. But at the second workshop, held on 21 to 22 September, 1976, Walter Tuchman of IBM at Kingston, New York, revealed that IBM had also conducted a study of the cost of breaking the DES code. According to participants at the workshop, Tuchman reported that IBM could deliver a code-breaking machine by 1981 and that its total price, including profit, would be $200 million. (Tuchman was out of the country and unavailable for comment when called by *Science*. IBM officials have since repudiated his report.)

Dennis Branstad of NBS, who is the leader of the computer security project there, contends that "the DES is better than any comparable encryption device I have seen anywhere." (Branstad, a former employee of NSA, presumably has seen many other encryption schemes.) He believes that Hellman and Diffie's estimates of the cost of the machine are off base. The special search chips, he says,

would be more likely to cost $400 than $10. Furthermore, the machine would require an enormous amount of power—he estimates about 16 million watts per day. All of NBS uses 16 million watts of power each day, he says. Hellman and Diffie, on the other hand, estimate that the machine would use only about 2 million watts per day. This power would cost about $1500, which is not much compared to the $10,000 per day amortization costs, they contend. Branstad says that the proposed code-breaking machine would be so large, require so many resources to build, and use so much power that not even NSA would be able to keep its existence a secret.

Alan Konheim of IBM at Yorktown Heights, New York, cites another reason to believe the code-breaking machine would never be built. Those who believe the code is insecure could encipher their data twice, with two different keys. This would effectively increase the key size to 112 bits. "Would the government invest in a machine to break the code if people could easily foil the machine by enciphering twice?" Konheim asks. Lewis Branscomb of IBM at Armonk, New York, says that the real problems for most users will be to generate random strings of digits for their keys and to ensure that security is not breached when they distribute their keys among a network of users.

Critics of the DES feel uncomfortable with the system in part because of the generally acknowledged fact that NSA had its hand in the development of the DES from the very beginning. Aaron Wyner of Bell Laboratories in Murray Hill, New Jersey, says "IBM makes no bones about the fact that NSA got into the act before the key size was chosen." Konheim admits that "IBM was involved with the NSA on an ongoing basis. They [NSA employees] came up every couple of months to find out what IBM was doing." But, Konheim says, "The 56-bit key was chosen by IBM because it was a convenient size to implement on a chip."

Morris, Wyner, and their associate Neal Sloane at Bell Laboratories note that when IBM first described the algorithm that later became the DES, a 128-bit key was used. Why and when, they ask, was the key size reduced? Konheim insists that the 128-bit key was designed for a system known as Lucifer, which was not the same as the DES. Lucifer was intended for internal use at IBM. Nonetheless, says Morris, "Lucifer and the DES are substantially identical."

Branscomb says that the key size was chosen with two considerations in mind. The first was to provide the maximum security at the lowest cost. The second was to ensure that the device could be exported for sales abroad.

In order to export cryptographic devices, a license must be obtained from the Office of Munitions Control at the State Department. James Hataway of that office says that it refers all requests for such licenses to the Defense Department. From there, he says, the requests are referred to the NSA for final approval or disapproval. According to Hellman and Morris, it is well known that the Office of Munitions Control routinely approves for export cryptographic devices with key sizes about the same as or smaller than that of the DES, and that it generally balks at approving devices with larger key sizes. One employee at the Office of Munitions Control, who asked not to be named, confirmed this.

Who Can Export the Device?

As it expected, IBM has received permission to export computer equipment incorporating the DES. James Booth of the Government Electronics Division of Motorola, Inc., in Scotsdale, Arizona, says that his company also expects to receive permission, although they have not yet made a request. However, Herbert Bright of Computation Planning, Inc., in Bethesda, Maryland, says the Office of Munitions Control informally gave him the impression that his company would be wasting its time to apply for a license. Since many potential customers, such as banks, have subsidiaries in other countries, denial of a license would greatly restrict a company's ability to market the DES.

Those who question the security of the DES are also bothered by the backgrounds of some of the key figures in its development. Not only Branstad, but also Arthur Levinson, who was an NBS consultant on the project, is a former NSA employee. Moreover, Theodore Linden of NBS, who works in the same group as Branstad, although not directly on the DES project, previously worked for NSA. Branscomb, an IBM vice president and chief scientist, was formerly head of the NBS.

Critics are made even more uncomfortable by the fact that certain crucial aspects of the design and testing of the DES are secret. For example, the NSA asked IBM to classify the way the "S-boxes" are chosen. These S-boxes specify nonlinear functions used in the encryption scheme. Morris, Sloane, and Wyner report that, at the second NBS workshop, a representative from IBM said that the S-boxes were chosen so as to strengthen the DES algorithm. When asked for proof, he said, "You must trust us, we are all good boy scouts."

If it was known that mathematical structure was built into the S-boxes, the DES code could be broken far more easily than by a brute force attack. Although he says he believes that IBM did not intentionally build in structures to weaken the algorithm, Hellman reports that he and his associates found "suspicious structures" in the S-boxes. They conclude that "an explanation and further study are needed before trust can be placed in the DES."

Other information that has not been made public is the result of a test of the strength of the DES. IBM claims to have spent 17 man-years of effort in trying to break the code by something other than a brute force attack. It concludes that there are no substantial shortcuts to breaking the DES. But IBM will release no details of this study. David Snow of the Mitre Corporation in Bedford, Massachusetts, points out that it is good practice in cryptanalysis to document claims about the strength of an encryption algorithm. The opinion at Mitre, he says, is that "it may be a great algorithm, but there is no analysis to support that contention." He questions whether the DES is sufficient to protect nationally sensitive information, such as large fund transfers between banks, without some documentation of the strength of the algorithm.

Some banks, however, do not share these doubts. For example, at Citibank N.A. of New York, said to be among the most sophisticated commercial users of cryptography, officials are fully cognizant of the criticisms of the DES but still plan to use it. M. Blake Greenlee of Citibank says that, compared to other encryption devices used by banks, DES is a great step forward. The main problem with the DES is a psychological one, he says. "Few people in the U.S. trust our intelligence agencies."

In the final analysis, many critics are left wondering why NBS chose an encryption scheme whose security can be questioned and why data that could demonstrate its strength were classified. At little extra cost, it could have increased the key size and dispelled most peoples' qualms about the system. Or it could have allowed users a range of key sizes, depending on the security they desired. Although some manufacturers are beginning to market the DES, it is not too late to have the standard changed, Hellman says. The problem is that, for many users, cryptography is an esoteric subject. And, Hellman says, "If the NBS tells them the DES is secure, they believe it."—GINA BARI KOLATA