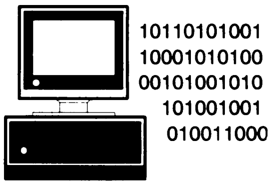
ENCRYPTING CONTROVERSY



A fierce debate erupts over cryptography and privacy

By IVARS PETERSON

With a little encryption to hide their words, Prince Charles and Princess Diana might never have suffered the embarrassing spectacle of having transcripts of their private telephone conversations splashed across the front pages of newspapers around the world.

The royal couple has not been alone in learning the painful lesson that modern technology has made eavesdropping – whether officially sanctioned, inadvertent, or illegal – remarkably easy. Today, cellular and cordless telephones transmit conversations via radio waves that can be readily intercepted. Electronic-mail messages pass openly from one computer to another across a network accessible to innumerable people.

"We take for granted that by sealing the envelope or closing the door, we can achieve privacy in our communications," says Whitfield Diffie of Sun Microsystems in Mountain View, Calif. "The challenge of modern security technology is to transplant these familiar mechanisms from the traditional world of face-to-face meetings and pen-and-ink communications to a world in which digital electronic communications are the norm and the luxury of personal encounters or handwritten messages [is] the exception."

Modern technology has provided a solution in the form of sophisticated schemes for encrypting digitized sounds and text. Only a recipient with the proper key for unlocking the secret code can hear or read the otherwise unintelligible, encrypted string of digits.

Nonetheless, few telephones and computers used by the general public come equipped with either software or microelectronic circuitry for encrypting speech or text. Indeed, some critics charge that the U.S. government has actively discouraged wide dissemination of cryptographic technology.

"Conflicting signals from a succession of administrations have led many to be very confused as to what U.S. citizens have a right to expect from cryptographic technologies and what capabilities the U.S. government would prefer its citizens have available," says Stephen T. Walker, president of Trusted Information Systems, Inc., in Glenwood, Md.

In April, the Clinton administration added a new ingredient that set the cryptographic-policy pot boiling. The White House proposal called for the adoption of a novel encryption scheme as a federal standard. It would incorporate a "front door" through which properly authorized government officials could readily decrypt intercepted messages for reasons of law enforcement or national security.

The proposal ignited a firestorm of protest from large segments of the computer community. Since then, angry debate over this issue and the more general question of privacy in an electronic age has dominated discourse on many electronic bulletin boards, where individuals can post their queries and opinions on a smorgasbord of concerns.

"Not everybody is saying this is terrible, terrible, terrible, but nobody is happy about it," Walker says. The list of dissatisfied parties ranges from major computer manufacturers and telephone companies to privacy activists belonging to organizations such as the Electronic Frontier Foundation and Computer Professionals for Social Responsibility.

The administration's scheme has also attracted congressional scrutiny and focused attention on the need to formulate a coherent national cryptographic policy. Many see the resolution of privacy issues as one of the key elements in developing a national information infrastructure, which would allow anyone using a networked computer unprecedented access to libraries, data repositories, and other information sources throughout the United States.

"Recent years have seen a succession of technological developments that diminish the privacy available to the individual," Diffie stated last month in testimony before the House science subcommittee. "Cryptography is perhaps alone in its promise to give us more privacy rather than less. But here we are told that we should forgo this technical benefit and accept a solution in which the government will retain the power to intercept our ever more valuable and intimate communications."

For many decades, cryptography remained largely a government matter – an arcane discipline of interest to military organizations and to the secretive National Security Agency (NSA), which routinely monitors foreign communications. But the subject also captured the attention of a few enthusiasts outside government. In the 1970s, the development of electronic communication via the first national computer networks spurred these people to look for ways to protect information in this new, wide-open environment.

In 1975, Diffie, working with computer scientist Martin E. Hellman of Stanford University, invented a novel, revolutionary cryptographic technique now known as public-key cryptography. Developed entirely outside of government, it offered a high level of security and privacy to any individual using the system.

In conventional cryptographic schemes, the user typically has a "key" that changes all the digits of a message into an unintelligible string. The recipient then uses the same key to unscramble the code and read the message.

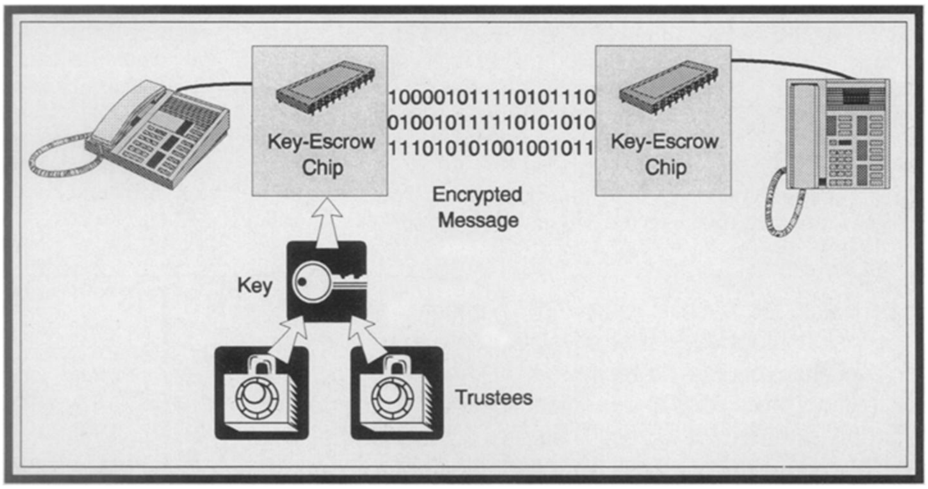
In a public-key system, the user has one key – kept secret – for encrypting the message and the recipient has a different but mathematically related key to decrypt the message. There's no need to keep the second key secret because, in principle, there should be no way to figure out the private key from knowledge of the public key. Thus, everyone has a private key and a public key, which they can then use to encrypt or decrypt messages.

Almost simultaneously, the U.S. government offered an alternative, singlekey method, known as the Data Encryption Standard (DES), for coding information. Although experts outside of government initially harbored suspicions that the NSA had deliberately weakened the scheme to make code-breaking easier, 15 years of concerted effort to find flaws have failed to turn up any serious problems. Many banks and other institutions now routinely use this technique to maintain the confidentiality and integrity of communications involving financial transactions and other matters.

One of the first hints of something new in the works came early this year. Last fall, Walker heard about a new AT&T telephone equipped with a lightweight electronic device, based on DES, for turning a telephone signal into a digital stream of encrypted information. He ordered five of these secure telephones for his business.

In January, AT&T representatives told Walker they could only loan him the telephones he wanted; something better would become available in April, they said. Walker noticed they no longer mentioned DES as the encryption scheme.

"So I knew there was something coming," Walker says. "But I didn't know what the details were." When the White House announcement finally came, the details caught just about everyone in the computer community by surprise.



The government's key-escrow cryptographic scheme allows a properly authorized third party to obtain a "key" that would decipher an encrypted message.

In essence, the proposed "key-escrow" technology takes the form of two specially fabricated, tamper-resistant integrated-circuit chips – one, known as Clipper, for encrypting digital telephone signals and another, known as Capstone, for encrypting the output of computers. Information from any telephone or computer would pass through the chip to be encrypted, and a corresponding chip attached to the recipient's telephone or computer would decipher the message.

However, the scheme is designed to include another key, divided into two parts, that when reconstituted will also unlock the message. The administration's plan is to deposit these pieces – unique to each chip – in two separate, secure databases. The two pieces of a particular key would be released only to officials at such agencies as the Federal Bureau of Investigation who are authorized to tap a particular telephone line.

This technology improves "the security and privacy of telephone communications while meeting the legitimate needs of law enforcement," the White House stated in announcing the Clipper chip.

"The effect," says Diffie, "is very much like that of the little keyhole in the back of the combination locks used on the lockers of schoolchildren. The children open the locks with the combinations, which is supposed to keep the other children out, but the teachers can always look in the lockers by using the key."

"Because the key-escrow chip enables lawful intercepts, the government for the first time in history is in a position to promote encryption without putting public safety at risk," says Dorothy E. Denning, a cryptography expert at Georgetown University in Washington, D.C. "As a result of the government's efforts, I expect to see greater use of encryption and, consequently, greater protection of sensitive communications."

Administration officials insist the Clipper-Capstone scheme is voluntary. Initially, only certain departments and agencies of the government will be required to use it. But clearly, the administration hopes that various companies will start incorporating this technology into commercial products, at first to supply the government market and then to meet the security needs of businesses and private individuals.

This approach puzzles many observers. "If you're not going to force it on people, then it's going to be largely irrelevant for the computer community," says Walker. "DES and RSA [a public-key cryptosystem] are already so widely used in software versions that most users will not even consider converting to Clipper or Capstone, simply because of the additional hardware expense."

"Anyone who is seriously seeking to protect sensitive information will use alternative methods, either instead of or in addition to the Clipper-Capstone chips," he adds. That leaves the possibility that the government may eventually ban the use of certain types of cryptography, though officials presently deny any such intent.

"Encryption is a technology that could be constrained legally in the same way that other technologies are constrained," Denning argues. "Congress should consider legislation that would impose such constraints."

Debating the technical merits of the administration's proposal has proved tricky. Many of the details of the scheme's implementation remain fuzzy, and the government has insisted on keeping secret the actual mathematical recipe, or algorithm, for generating the required keys.

"It's very hard to assess something when you don't know what you're assessing," notes Lance J. Hoffman, a computer scientist at George Washington University in Washington, D.C.

In contrast, the government made public the DES algorithm, giving cryptography experts a chance to examine and test the scheme thoroughly to vouch for its security. Developed secretly at the NSA, the new algorithm used for the Clipper and Capstone chips will receive no such scrutiny.

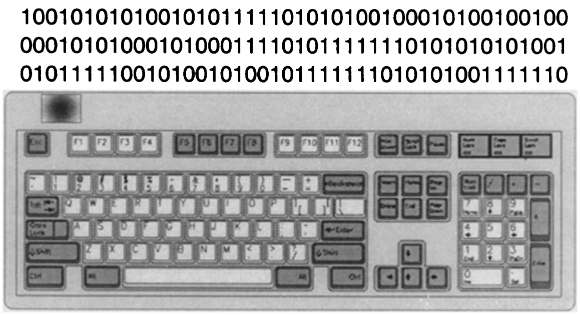
The government's reluctance to release the algorithm stems from the possibility that some people might then use the algorithm without its accompanying key-escrow provision to create a formidable encryption scheme. "This is a powerful algorithm," says NSA's Clint Brooks. "You need some kind of control mechanism . . . to ensure the law-enforcement capability is preserved."

The Clipper and Capstone chips also represent only one possible approach to achieving a reasonable balance between unconstrained privacy and the needs of law enforcement and national security. Silvio Micali of the Massachusetts Institute of Technology has proposed an alternative scheme – developed well before the Clipper chip announcement – that eschews complicated chips and special hardware in favor of a considerably more flexible, inexpensive software solution.

Like the administration, Micali favors an approach that includes a cryptographic escape hatch in case of dire emergency. "Scientists ought to be socially responsible," he argues. "We have to ask ourselves what would be the social impact of widespread cryptography."

Micali has demonstrated that it's possible with his technique to transform any public-key cryptosystem into one that includes a provision for third-party access to encrypted information, if a court deems such access essential for reasons of law enforcement or national security. He calls the transformed version a "fair" public-key cryptosystem.

"The transformed systems preserve the security and efficiency of the original ones," Micali says. "Thus, one can still use whatever system [he or she] believes to be more secure and enjoy the additional property of fairness."



But to many others, the real debate is not about the technical merits of the Clipper and Capstone proposals. "The fundamental issue that people are talking about is the question of whether people have a right to have privacy in a conversation . . . something that cryptography can provide," says Ronald L. Rivest, a computer scientist at MIT.

Denning contends that it would be irresponsible for either government or industry to promote the widespread use of strong encryption. "I do not believe our laws grant an 'absolute right' to a private conversation," she says.

But Rivest and others reject the notion that the public should have access only to cryptography that the U.S. government can decipher. They feel shut out of the government decision-making process that brought forth the Clipper chip.

"I don't know anyone inside the government who is fighting for the average citizen's protection here," Walker says. "It's the national security and law enforcement guys that are running the show, and the administration has bought in to their side."

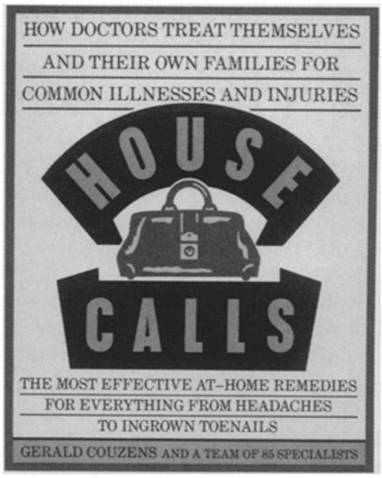
"I don't think we have a fair situation at all," he adds. "That's why I keep insisting we've got to have a national review involving . . . private citizens and private organizations."

The administration already has an internal review of cryptographic policy under way. This task force is supposed to have its final report ready by the end of the summer. In addition, earlier this month, the Computer System Security and Privacy Advisory Board, which advises the administration on matters of security and privacy, held a three-day meeting to hear public comments on a variety of cryptographic issues.

Many people question the sudden rush to implement Clipper-Capstone, given the major ethical and constitutional questions at issue. "There hasn't been a serious public discussion," Hoffman says. "Nobody has been given enough time."

Faced with such criticisms, the government now shows signs of slowing implementation of its key-escrow plan until the scheme's ramifications have been studied further. At the same time, computer users already have access to chips and software incorporating DES or the RSA public-key cryptosystem.

"For the first time in history, we have a situation in which individuals can use cryptography good enough that even governments can't read [the encrypted messages]," Hoffman says. "That is a big change. The administration is ultimately going to have to address the issue of whether people can use their own cryptography and keep the keys secret themselves." □


HOW DOCTORS TREAT THEMSELVES
AND THEIR OWN FAMILIES FOR
COMMON ILLNESSES AND INJURIES
HOUSE
CALLS
THE MOST EFFECTIVE AT-HOME REMEDIES
FOR EVERYTHING FROM HEADACHES
TO INGROWN TOENAILS
GERALD COUZENS AND A TEAM OF 85 SPECIALISTS