# 9

# Cryptography in the 1990s

## Pretty Good Privacy

In 1990, a programmer from Boulder, Colorado, Philip Zimmermann, wrote Pretty Good Privacy (PGP), a program for protecting the privacy of email, and made it available over the Internet. Under the State Department's interpretation of the Arms Export Control Act, this constituted an illegal export.

Zimmermann might not have had any trouble had he not offended another vested interest. The PGP program was in blatant infringement of the Rivest-Shamir-Adleman patent and it bore a remarkable resemblance to a program called Mailsafe (written by Ron Rivest) marketed in the mid 1980s by RSA Data Security. Zimmermann recalls receiving a visit from puzzled customs investigators, who told him they had received a complaint from RSA Data Security alleging the theft and international shipment of stolen intellectual property. The customs inspectors did not really understand what was at issue. Patent infringement wasn't their responsibility. Disks stolen out of warehouses and smuggled out of the country were, however, and this is how Zimmermann believed they had interpreted the complaint. A federal prosecutor in San Jose, California, began an investigation, and a grand jury in that city heard testimony on the subject for over a year. The experience was disquieting for all involved —not least the prosecutor and the grand jury, who were not used to investigating in a fish bowl. Many witnesses reported their experiences on the Internet and the cryptography community followed the events attentively.

Meanwhile, PGP spread out of anyone's control. Because the RSA patent held only in the United States, foreign users were not at risk of being sued for contributory infringement. A worldwide group of programmers began further development on the program and later versions were said to have been developed abroad and imported to the US Midway through the course of criminal investigation, the patent-infringement aspect of the case became moot when RSA Data Security changed the license for its reference implementation of the RSA cryptosystem in a way that permitted a "legal" US version of PGP (PGP 2.6).

The investigation, of which the grand jury was only the most visible part, ended when the Department of Justice decided not to prosecute. The government's reasoning is not known. Quite independent of the central legal issue (whether posting code on the Internet, where foreigners can get at it, constitutes export under American law or is merely the exercise of a free-speech right to publish), the case was an evidential nightmare. Zimmermann had not actually posted the code himself; someone else had done it with his permission. More important than this, however, was an unquestioned act of publication. The MIT Press, with its thumb firmly on its nose, published the code of PGP as a 600-page hardbound book (Zimmermann 1995) printed in an OCR font, and sold it though its usual worldwide distribution channels. Had the government prosecuted Zimmermann and not gone after MIT, it would have invited scorn. But MIT was three times as old as NSA, just as well funded, and even more influential in the military-industrial complex. The Department of Justice let the case drop.

Free of the threat of prosecution, Zimmermann founded a company and began to expand his product line. Today, PGP has a worldwide following, and it has entered the mainstream by means of an easy-to-use interface to the popular Eudora email program. In writing PGP, Phil Zimmermann did something for cryptography that no technical paper could do: he gave people who were concerned with privacy but were not cryptographers (and not necessarily even programmers) a tool they could use to protect their communications.

## A National Encryption Policy

In the period immediately following the 1989 NIST/NSA Memorandum of Understanding, from a public vantage point encryption policy seemed to be lurching along without direction. At the FBI's request, the chairman of the Senate Judiciary Committee, Joseph Biden, introduced a nonbinding sense-of-the-Congress resolution recommending that, under appropriate legal authorization, telephone companies provide the plaintext of encrypted messages they encountered while wiretapping. Biden later withdrew the resolution, which had been part of an anti-terrorism measure (Markoff 1991). Industry complaints about restrictive export controls on cryptography resulted in agreement on a slightly loosened export policy: seven-day approval for software employing RC2 and RC4, RSA Data Security algorithms that used 40-bit keys. Meanwhile DES continued to be restricted for export. The lack of clear direction complicated the situation for industry and thus vastly slowed the development of secure systems.

Various groups sought a clarification of federal encryption policy. The Computer System Security and Privacy Advisory Board, a NIST review committee created through the Computer Security Act,[1] requested a national review of cryptography (Brooks 1992, p. C-13). A bill in Congress included a requirement for presidential analysis of aspects of encryption policy (ibid.).

The Brooks-Kammer briefings[2] of the FBI had created a confluence of interest in law-enforcement and national-security circles. NSA urged discussion and adoption of a "national encryption policy." What NSA had in mind was a "national policy" decreeing that "because of legitimate law enforcement needs in the US the US government will have to have a carefully controlled means of being able to decrypt information when legally authorized to do so" (ibid., p. C-12).

The FBI was pursuing passage of the Digital Telephony bill, and NSA was working on an algorithm to satisfy the FBI's need for strong but accessible cryptography. The Digital Telephony effort was known to the public; the encryption work was not. NSA opposed any public debate on cryptography.[3]

The US government's technique for attacking the spread of strong

cryptography was also changing. The Clipper program attempted to use standardization and federal buying power to influence civilian use of cryptography. After the effective failure of this program, the government turned to the only other tool available without new legislation: export control. The most notable reason for this shift was that, as cryptography entered the mainstream market, exportability became essential for successful mass-market products.

NSA's work with NIST had been directed toward cryptography used in computers, so it was with some surprise that in 1992 the federal government faced the threat of deployment of strong, relatively inexpensive cryptography in telephones.[4]

## Cryptography and Telephony

In the past decade, secure telephones using advanced key management have become widespread in the national-security community. During the 1980s, approximately 10,000 second-generation (STU-II) secure telephones used by the US government were replaced with third-generation STU-IIIs. By the mid 90s more than 300,000 STU-IIIs had been produced, and the unit price had dropped from several thousand dollars to about $1500. Each of the three producers of STU-IIIs—AT&T, Motorola, and Lockheed Martin[5]—also made commercial derivatives using DES and exportable versions using trade-secret algorithms. These versions are generally presumed to be less secure than STU-IIIs, and because of smaller production volumes they are more expensive. At least one, however, has a flexible key-management system that makes it more suitable to the commercial environment than a STU-III.[6]

The secure-phone market is plagued by the existence of too many different kinds of secure telephones, most of which will not interoperate. (It has been jokingly said that the number of types of secure phones exceeds the number of instruments.) The US government now has several and is in the process of introducing more. The centerpiece of the new efforts has been the ISDN-based Secure Terminal Equipment (STE) designed to interoperate with and ultimately replace the STU-III. Unlike the STU-III, the STE is not a controlled cryptographic item. All of the secret components

are contained in a PCMCIA card (the Type I cousin of Fortezza) along with the keying material. There are also a number of other Type I voice security devices—some working over traditional phone lines, some using Voice over IP, and some wireless—with various sorts of interoperability.[7]

Voice-encryption systems for the commercial market have also been a staple of companies such as Gretag and Crypto AG in Switzerland and Datotek, Cylink, and TCC in the United States. It was only in 1992, however, that an attempt at selling a modern piece of equipment for secure telephony to a mass market occurred. AT&T announced the Telephone Security Device Model 3600 (TSD 3600) for an initial price of $1295.

In the fall of 1991, David Maher, an AT&T engineer who had been the chief architect of the AT&T STU-III, realized that it had become possible to design a secure phone using a single digital signal processing chip.[8] This permitted a piece of equipment for secure telephony to be built at a total cost of between $100 and $200. Like all modern secure telephones, it works by digitizing the voice signal and then encrypting the bitstream, using keys negotiated by public-key techniques. The beauty of the TSD 3600 is its size and simplicity: it is a 1-pound box smaller than this book. After installing it in the cord between the handset and the body of a standard phone, the user has only to push a "go secure" button to operate it.

As the development of the TSD 3600 proceeded, the head of Maher's division, who had been hired in part for his excellent connections in the intelligence community, discussed AT&T's new security venture with NSA.

NSA was interested in using the TSD 3600 in government applications, but also expressed concern over the problems it might pose for law enforcement. The agency suggested a key-escrow scheme for the phones, promising to deliver the appropriate chips to AT&T by the fall of 1992 so as not to delay the project. AT&T agreed to incorporate the escrow algorithm in some models of the TSD.

The promised chips did not arrive on schedule, and sample TSD 3600s using DES were lent to prospective customers in the fall of 1992. At the time AT&T promised that the DES version would shortly be joined by another model containing a yet-to-be-announced federal encryption


**Figure 9.1**
The AT&T TSD 3600. (Photograph by Eric Neilsen.)

standard. The model with the new "Type IIE" encryption algorithm would enjoy the benefit of easy exportability and certification for use in government applications.

Bill Clinton became president on January 20, 1993. Six days after the inauguration, Clinton's Senior Advisor for Intelligence was briefed by the FBI on encryption and "the AT&T problem" (Sessions 1993a). The new administration agreed with the current plans. On April 16, 1993, the White House announced the Escrowed Encryption Initiative, a Federal Information Processing Standard intended to "improve security and privacy of telephone communications" (White House 1993).

## The Escrowed Encryption Standard

The Escrowed Encryption Standard (EES) was designed to fit a set of seemingly contradictory requirements: strong cryptography, yet readily exportable, with messages accessible to law enforcement under proper legal authorization. The trick was key escrow.

EES consisted of a classified algorithm (Skipjack) that was to be implemented on tamper-resistant chips (Clipper) with escrowed keys. The chips were to be fabricated in a secure facility (the original facility was run by Mykotronx), and escrow agents would be present during the process. Keys would be split into two components, with each piece stored at a secure facility under the control of a federal executive-branch agency. Each half of the key would be worthless without the other. Only under "proper legal authorization" would keys be released to law-enforcement agents. According to Senate testimony, the escrow agents would cost $14 million to set up and $16 million per year to run (USS 103a, p. 95).

When a Clipper chip prepares to encrypt a message, it generates a short preliminary signal called the Law Enforcement Access Field (LEAF).[9] Before another Clipper chip will decrypt the message, this signal must be fed into it. The LEAF is tied to the key in use, and the two must match for decryption to be successful. The LEAF, when decrypted by a government-held key that is unique to the chip, will reveal the key used to encrypt the message.

The proposed standard was limited to encryption of voice, fax, and computer information transmitted over a telephone system (USDoC 1994b, p. 6003). At the initial Clipper announcement, the administration stated that it was neither prohibiting encryption outright, nor acknowledging Americans' right to unbreakable commercial encryption (White House 1993). In later briefings, the administration gave assurances that it would not seek legislation limiting the use of encryption products (USDoC 1994b, p. 5998; McConnell 1994, p. 102).

The key-escrow program provided a widely available form of cryptography of sufficient strength to satisfy the "Type II" requirement for protection of sensitive but unclassified government communications.[10]

This program had two essential elements: the algorithm was secret and was available to approved manufacturers in the form of tamper-resistant integrated circuits and the cryptosystem contained a trap door that permitted US authorities to exploit intercepted traffic when required.

Packaging cryptography in hardware provides the best security and has always been standard practice in the Type I systems used to protect classified information. In such environments, the restriction to isolated (separate chip) hardware implementations represents less additional cost,

since the isolated implementation would be necessary for security reasons anyway.

## The Clipper Controversy

As required by law, NIST provided a period for public comments on the newly proposed Escrowed Encryption Standard.[11] The response was vociferous and loud. Supporters outside the government were few, while opponents were many and varied, ranging from the American Civil Liberties Union to Citicorp bankers to a large segment of the computer industry. During the public comment period NIST received 320 letters on the proposed standard. With the exception of letters from Motorola (a major manufacturer of secure telephones that may have been contemplating developing devices to meet the new standards), a professor of computer science at Georgetown University, and "no comment" statements from a number of government agencies, the remainder of the letters were negative—including several from government agencies.[12]

The major objection to key escrow was that the mechanism compromises an individual's privacy *even if the escrowed keys are never accessed*. The knowledge that the government has the technical ability to read all communications creates a perception that no communication is private, even if the vast majority of communications are never intercepted or read.

Concern with privacy was not, however, the only ground for objection. Escrowed keys represented a major step back from the encryption techniques that had been developed in the mid 1970s. One purpose of public-key cryptography is to facilitate secure communication in a diverse community by reducing the trust that must be placed in centralized resources. Another is to limit the lifetimes of keys; by extending these, escrow creates vulnerabilities both for society and for the individual.

The decision to escrow keys as part of the standard and to include the LEAF led naturally to the implementation of the algorithm in a tamper-resistant chip. But such a contrivance was most unusual for a Federal Information Processing Standard, and the implicit inclusion of classified portions in a Federal Information Processing Standard effectively changed it from a mechanism for promoting interoperability among communication products to one for exercising control over those products

and the industry that produces them. Rather than being able to read the standard, implement conforming products, and submit samples for certification, companies would be required to purchase tamper-resistant chips from authorized suppliers. Both the diversity of sources and the availability lifetime of parts would be outside the company's control.

Formal government secrecy of a technology amounts to the most extreme form of regulation and to a great extent removes both the government and a segment of industry from accountability to the public. The EES stated that the government would regulate which companies would be allowed to include the new encryption product.[13] Companies would not only be beholden to the authorized suppliers of Clipper chips; they would be beholden to the government for permission to purchase them. The computer industry has been characterized by rapid and nimble developments; to many observers, this federal standard seemed to bode steep bureaucratic hurdles for any product that included security.

If the introduction of key-escrow technology were successful, a vast body of traffic would be transmitted under its "protection." Much of this would have been sent by radio or satellite, and there would be no way of estimating how much of it was recorded and by whom. Under these circumstances, escrow agents become an intelligence target of unprecedented proportions. Compromise them and all that has been recorded can be read.[14]

There is also a vulnerability that does not depend on even the continued existence of the escrow agents. Although the standard contains no statement as to the length of either the device-unique key or the family key, it has been stated elsewhere that, like the session keys, these will both be 80 bits. Under these circumstances, it appears that an opponent who knows the Skipjack algorithm, the LEAF creation method, and the escrow authenticator can recover the device-unique key in at most a small multiple of $2^{80}$ operations. A message so valuable that someone would attempt to perform $2^{80}$ operations to read it strains the imagination today. It is less strain to imagine a cipher chip whose history is such that after it has been in service a decade or more someone might perform a similar number of operations to acquire easy access to its lifetime traffic.[15]

Despite the strong protests, on February 9, 1994, NIST adopted the Escrowed Encryption Standard as a Federal Information Processing Stan-

dard (USDoC 1994b). To objections that the standard was a first step toward prohibition of non-escrowed encryption, NIST responded that the standard was voluntary. To concerns that the system might infringe on individual rights, NIST responded that decryption would occur only when legally authorized. To protests over the secrecy of the algorithm, NIST responded that there are no known trap doors or weaknesses in it. To objections that the standard would be ignored by people engaged in criminal activity, NIST responded that EES would make strong encryption widely available and that, to the degree that it was successful, non-escrowed encryption would become harder to obtain. Escrow agents remained undetermined, and NIST acknowledged that the standard lacked sufficient detail to function as an interoperability standard.

The standard was limited to voice, fax, and computer information communicated over a telephone system. But at the very last minute, NSA had attempted to scuttle that limitation. In memos between NIST and NSA days before EES was approved, NSA modified the standard to cover "telecommunications systems" instead of "telephone communications." NSA also expanded the coverage of the standard to include PCMCIA (Personal Computer Memory Card International Association) cards (USDoD 1994). Apprised of the changes, NIST scientists objected, and the modifications disappeared. Had they remained, EES would have become a standard for both voice and data communications. In addition, EES would have given Fortezza—a PCMCIA card that performs key exchange, computes digital signatures, and encrypts using Skipjack—a free pass around the laborious exception-approval process.[16]

AT&T ultimately developed half a dozen models of the TSD 3600, only some of which could interoperate. These included the D model, which used DES with a 768-bit modulus for Diffie-Hellman key exchange. D models were able to interoperate only with other D models. There were exportable F models that used a Datotek algorithm with a 512-bit modulus, and non-exportable P models running an algorithm developed by the Swiss company Gretag AG. The S models had Clipper, P, and F algorithms, so they could interoperate with the F model, the P model, and the government G model (equipped with Clipper).

AT&T anticipated a large market for these devices, expecting them to appeal to executives in businesses facing aggressive international competi-

tion. The original TSD 3600 with DES encryption might have achieved its market objectives. The "improved" Clipper model saw disappointing sales.

By the fall of 1995, total sales of all TSD 3600s were about 17,000. The largest single block were the 9000 Clipper models bought by the FBI in an attempt to seed the market. Most of the remainder were an exportable version exported to buyers in Venezuela and several Middle Eastern countries.[17] According to the government, the Escrowed Encryption Standard was developed to "make strong encryption broadly available and affordable" (USDoC 1994b, p. 6000). The immediate effect of EES, however, was to kill off the first secure phone device targeted at a mass market. By 1997 no secure phone product had come along to take the TSD's place, and telephone conversations remained unencrypted and unprotected. A National Research Council panel cited the lack of encryption between cellular telephones and base stations as a serious problem[18] and recommended it be fixed forthwith (Dam and Lin 1996, p. 327).

## The Larger Plan: Capstone et al.

Far from being the whole of the key-escrow plan, Clipper was only the beginning. Paralleling its development, and perhaps started earlier,[19] was the data-oriented Capstone program.

Like the Clipper chip, the Capstone chip implemented the Skipjack algorithm and key escrow. It also provided key management via the Key Exchange Algorithm (KEA), a name it has been claimed was merely NSA's way of concealing use of Diffie-Hellman key exchange. The claim was made plausible by Capstone's third major capability: performing the NIST Digital Signature Algorithm, which uses the same arithmetic mechanism as Diffie-Hellman.

The major use for the Capstone chip was as the heart of a PCMCIA card originally called Tessera[20] and later renamed Fortezza. The initial use of the Fortezza card to provide security for the Military Messaging System (a form of email used by the Department of Defense) was expected to "bootstrap" the use of Fortezza cards for a wide range of computer applications.

## Clipper II, III, IV

By the fall of 1995, it was clear that the Clipper chip was not popular. Only the AT&T product was using it, and only a few thousand of these had been sold. During the previous year, joint work between NIST, Georgetown University, and Trusted Information Systems (a small security company with headquarters in Maryland) had produced a software mechanism remarkably similar in function to the Clipper chip, using public-key cryptography where the Clipper chip had used physical tamper resistance. NIST issued a set of ten principles for software key escrow and scheduled two meetings to discuss the idea with industry representatives.

The project had a certain oddity to it. The promise was that systems complying with the ten principles would be exportable, but the meetings were hosted by an organization (NIST) without any role in the export process, and even its parent, the Department of Commerce, plays a role secondary to the Department of State in the issue of cryptography export. (Everyone in the game knows that if the Department of State agrees to "Commerce jurisdiction" for a product, export permission follows.) There was talk of a Federal Information Processing Standard for key escrow, but this too was odd. Each of the two extant cryptographic FIPS says, in effect, "This system is good enough for some category of government traffic." The proposal for software key escrow said nothing about cryptographic quality; indeed, it only specified a particular type of weakness. In the end no FIPS was ever proposed.

The essence of the "Ten Commandments," as they came to be known, was to limit the keys of exportable cryptosystems to 64 bits. Such systems must allow recovery of the key from traffic in either direction. They must not interoperate with unescrowed versions of the same systems.[21] Most important, the escrow agents would have to be in the United States[22] or in countries having bilateral agreements with the United States that guaranteed the US government access to the keys.

In 1996, derivatives of the software key escrow proposal evolved and eventually became part of the export regime. Technical developments included dropping the key-length restriction and relaxing the non-interoperability requirements, but the real developments were in marketing.

Intentionally blurring the distinction between communication and storage, proponents of key escrow have pushed the notion that key escrow is something that users need in order to be able to recover their data if they lose their keys. Along with this notion goes a new name, "key recovery," and a claim that key recovery is substantively different from key escrow. In respect to stored data, there is much to be said for this view. If you have encrypted all the copies of a file, then the keys are as valuable as the information the file contained. If you lose the keys, you lose the information. Under these circumstances, spare keys are more than a good idea; they are essential. On the other hand, the same is not true of communication. There is no reason to want to decrypt the ciphertext of a secure phone call after the call has ended. If either of the callers wanted a recording of the call, the right thing would be to record the plain text at one end of the line; that does not require escrowing any keys. Some forms of communication, such as email, do blur the distinction between key escrow and key recovery. Encrypted email is sometimes decrypted and reencrypted in a local storage key and sometimes left encrypted in the transit key (which is retained).

The other marketing angle was to present key recovery as an essential capability of the key-management infrastructure.[23] The message here is that users won't trust cryptographic systems unless they are sure that they can always get their data back.

These notions were set forth in the late spring of 1996 in the report of an interagency committee assembled to study cryptographic policy (White House 1996). In the fall, a proposed set of regulations containing a new sort of incentive followed. For two years, beginning on January 1, 1997, the government would allow export of unescrowed systems with 56-bit keys (mostly DES systems, presumably) in return for promises from the exporters that they would implement key-recovery systems in their products. Essentially simultaneously, IBM formed a coalition with other companies to implement key-recovery technology and announced what it claimed were fundamentally new and secure techniques for satisfying everybody. For nearly a year, IBM treated its new techniques as trade secrets, but in September 1997 they were made public in a technical report (Gennaro et al. 1997).

## The Multi-level Information Systems Security Initiative

After the success of the STU-III project, NSA broadened its objectives and began a project that was originally called the Future Secure Data System (paralleling Future Secure Voice System, the developmental name of STU-III) and later the Secure Data Network System (SDNS). The SDNS project developed protocols for security at several levels of network architecture, addressing such issues as network layer encryption and key management.

The Secure Data Network System evolved into a substantial program called the Multi-level Information System Security Initiative (MISSI), the main goal of which is to solve a much broader range of computer security problems using encryption embodied in individually carried PCMCIA cards. A user sitting down at a workstation on the Defense Message System inserts a PCMCIA card that encrypts and decrypts email, for example. The Type II portion of the program uses the Fortezza card from the Capstone program and is entirely tied to key escrow.[24] After a brief flirtation with a Fortezza+ card, the Type I portion evolved a new PCMCIA card (called Krypton) with much higher performance.

The Computer Security Act of 1987 appeared to have put NSA out of the mass-market cryptography business in the late 1980s, but MISSI certainly looked like an attempt to get back in.

## The National Research Council Report

The Clipper controversy convinced Congress that an independent study was needed. In 1994 the National Research Council (NRC) was asked to conduct a "comprehensive independent review of national encryption policy" (PL 103-160, Sec. 267). Everything was to be considered, including the effect of cryptography on the national-security, the law-enforcement, commercial, and privacy interests of the United States, and the effect of export controls on US commercial interests.

The NRC put together a panel of 16 experts from government, industry, and science, 13 of whom had received security clearances.[25] The chairman, Kenneth Dam, had been Deputy Secretary of State under President Reagan; other panelists included General William Smith (former Deputy Commander in Chief of the European Command, and President

Emeritus of the Institute for Defense Analyses), Ann Caracristi (former Deputy Director of NSA), and Benjamin Civiletti (Attorney General under President Carter).[26] Many opponents of the government's policies anticipated that such a group would support the Clinton administration's conservative directions in cryptography policy, but in its 1996 report it did not. Arguably its most important finding was that "the debate over national cryptography policy can be carried out in a reasonable manner on an unclassified basis" (Dam and Lin 1996, p. 298). The NRC panelists declared that, although classified information was often important in operational decisions, it was not essential to deciding how cryptography policy should evolve. This ran counter to the long-standing position of the intelligence community, and it was a striking conclusion to have come from a panel that included so many members of the national-security establishment.

The panel argued for broader use of cryptography ("on balance, the advantages of more widespread use of cryptography outweigh the disadvantages") and emphasized that there should be "broad availability of cryptography to all legitimate elements of US society." Current US policy, they said, was inadequate for the security requirements of an information society (ibid., p. 300–301), and current export policy hampered the domestic use of strong cryptosystems.[27] The panel urged that the market be allowed to decide the development and use of commercial cryptography.

Panelists urged an immediate loosening of export-control regulations. They recommended that products using DES for confidentiality purposes immediately be made easily exportable (ibid., p. 312). Observing that escrowed encryption was a new technology, and that new technologies come with potential flaws, the panel urged the US government to go slow with escrowed encryption—to experiment with the technique, but not to aggressively promote the concept until it had experimented with it on a small scale and knew how to adapt it for large-scale practice (ibid., pp. 328–329). Echoing the First Amendment and contradicting FBI Director Louis Freeh, the panel said that "no law should bar the manufacture, sale, or use of any form of encryption within the United States" (ibid., p. 303).

The panelists recognized that some of their recommendations would complicate law enforcement and they urged that the government take

steps to assist those responsible for law enforcement and national security in adjusting to the new technical realities (ibid., p. 322). In an analogy to the statute that criminalizes the use of the mails in commission of a crime, they suggested that the government consider legislation that would criminalize the use of encryption in interstate commerce with criminal intent. They also urged that law-enforcement agencies be given resources to help them handle the challenges posed by new technologies.

The short message of the report was that the United States would be better off with widespread use of cryptography than without it (ibid., p. 299). This was not a message the Clinton administration wanted to hear.

Soon thereafter, the insecurity of DES was shown decisively. Using custom-designed chips and a personal computer, the Electronic Frontier Foundation created "DES Cracker," a $250,000 dollar machine built in less than a year. In July 1998 DES Cracker broke a DES-encoded message in 56 hours. There was some luck involved; the key was found after only a quarter of the key space was searched (rather than the expected half). There was nothing particularly novel about the decryption machine except that it was actually built rather than merely designed. DES Cracker was scalable: with an additional $250,000 dollars and a link between the resulting machines, there would be a DES "Double-Cracker" capable of decoding DES-encrypted messages twice as fast.

## International Lobbying

When the Clipper effort ran into problems at home, US government officials began lobbying for it—quietly—in other countries. In 1994, under the influence of such lobbying, the Australian government reported that the biggest *current* threats to telecommunications interception were digital telephony and encryption (Barrett 1994, p. 4). This was at a time when the only mass-market telephone encryption device available was the TSD 3600, most examples of which were either Clipper models bought by the FBI or export models with weak encryption.

The US lobbying had more profound success in Great Britain.[28] Beginning shortly after the announcement of the Clipper program in the United States, the Department of Trade and Industry began to sponsor research

on public-key-based escrow schemes at the Cryptologic Research Unit of the University of London. At the same time, development was going on behind the scenes on a draconian legal framework that would effectively outlaw the use of non-escrowed cryptography.[29]

Bilateral agreements on key escrow did not materialize, and the White House took a more public route through the Organization for Economic Cooperation and Development. The OECD is an association of industrialized democracies[30] that seeks to foster—not impede—international trade.

Cryptography was a natural topic for the OECD, which had a distinguished history in privacy policy.[31] Having developed policy guidelines for transborder data flows in 1980 and for information security in 1992, the OECD tackled encryption in early 1996.

The Clinton administration saw the OECD's efforts as a chance to get an international stamp of approval on its key-escrow plans and sent a delegation glaringly different from those usually seen at meetings of international economic-development organizations. Most often, Scott Charney, head of the Department of Justice's Computer Crime Unit, acted as chairman of this delegation. Also included were current and former members of the security establishment, such as Stewart Baker, former general counsel of NSA (who at one point took minutes for the OECD Secretariat), and Edward Appel of the National Security Council staff. With members representing the White House viewpoint, the US delegation pressed for adoption of key escrow. Initial reactions by the other delegates ranged from skepticism (the Japanese delegation wanted to know what would prevent criminals from using their own cryptography systems—see Baker 1997) to mild support for the US position (most notably from the British delegation).

In the economic-development setting of the OECD, key escrow was difficult to sell. Unlike law enforcement, business has little need for real-time access to communications, encrypted or otherwise. Other nations did not see the issues as the United States did. The Danish government's Information Technology panel recommended that no limits be placed on a citizen's right to use encryption (ITSC 1996). The Dutch delegate spoke in opposition (Rotenberg 1996, p. 7). The Nordic countries argued for strong cryptography without trap doors.[32] Meanwhile, German

companies, taking advantage of the restrictions on their US competitors, were selling strong cryptography, and the German government had little interest in restricting such sales.[33] Behind the scenes, and kept very much in the background, was Phil Reitinger, a member of the US Department of Justice Computer Crime Division, who was seconded to the OECD to write a draft policy. Yet even this influence was insufficient to convince OECD member nations to support the US policy.

In late March of 1997 the OECD issued its cryptography guidelines, which sidestepped key escrow and emphasized the importance of trust in cryptographic products ("Principle 1: Market forces should serve to build trust in reliable systems"). The OECD recommended that cryptography be developed in response to the needs of "individuals, businesses, and [lastly] governments," and urged that "the development and provision of cryptographic methods should be determined by the market in an open and competitive environment, and that the development of international technical standards, criteria and protocols for cryptographic methods should also be market driven" (OECD 1997). Despite the intense lobbying efforts by the Clinton administration, mandatory key escrow did not make it into the OECD's cryptography guidelines.

Seven months later the European Commission dealt a further blow to the US position. In a policy paper on a European framework for digital signatures and encryption, the commission was cool to key escrow. It observed that such schemes are easily circumvented and that the involvement of a third party increases the likelihood of message exposure (European Commission 1997, pp. 16–17). The Commission expressed concern about the difficulty of key escrow across national borders. The report said that any such scheme should be limited to what is "absolutely necessary" (ibid., p. 18)—hardly the ringing endorsement the US was seeking.

## The US Congress' Response

Congress entered the fray in March of 1996 when Senator Patrick Leahy introduced the Encrypted Communications Privacy Act of 1996 (S 1587), a compromise bill that allowed for a relaxation of export controls, affirmed the right to use any form of encryption domestically, created a le-

gal framework for escrow agents, and criminalized the use of encryption in the furtherance of a crime. Less than a month later, Senator Conrad Burns proposed the more strongly pro-cryptography Promotion of Commerce On-Line in the Digital Era (PRO-CODE) Act (S 1726). Burns's bill prohibited mandatory key escrow, enshrined the freedom to sell and use any type of encryption domestically, and liberalized export rules. But 1996 was a presidential-election year, and the complex legislation did not go forward.

Burns reintroduced PRO-CODE in 1997 (S 377). In the House, Representative Bob Goodlatte proposed the Security and Freedom through Encryption Act (SAFE) Act (HR 695). Under both bills, the freedom to sell and use any type of encryption would be unconstrained, and mandatory key escrow would be prohibited. Export of cryptography would be under the control of the Department of Commerce, and export of strong encryption would be permitted if similar products were available overseas. The SAFE bill would criminalize the use of encryption in the furtherance of a crime; the PRO-CODE bill did not address that issue.

In his trademark cowboy hat, Montana Senator Burns seemed like an unusual legislator to be pressing for liberalization of laws on high technology. Burns saw PRO-CODE as having a significant impact on rural areas, where distances preclude face-to-face communication, and where substantial economic growth in recent years has occurred exactly in activities that would greatly benefit from secure electronic communications (Carney 1997).

When Congress reconvened at the end of the summer, the tables turned again. At a Senate Commerce Committee markup, the PRO-CODE bill was sidetracked and replaced by one introduced by Senators Bob Kerrey and John McCain. The Secure Public Networks Act (S. 909), tightened rather than loosened control over the export of encryption products and created incentives for many organizations to introduce key escrow.

Cryptography was also in trouble in the House of Representatives. Despite repeated assurances from the Clinton administration that it would not move for domestic regulation of cryptography, FBI Director Louis Freeh pressed Congress for restrictive laws. The House International Relations and Judiciary Committees had reported the SAFE bill out positively, but the House National Security Committee listened closely to

Freeh's requests, and accepted an "amendment in the nature of a substitute," introduced by Representatives Porter Goss and Norman Dicks, which turned Goodlatte's measure around completely. It not only tightened controls on export, but proposed legal controls on the use of cryptography. With various versions of the SAFE bill in the House, and different measure pending in the Senate, it was far from clear what direction Congress would take.