United States General Accounting Office

GAO

Report to the Honorable
Jack Brooks, Chairman, Committee on
the Judiciary, House of Representatives

November 1993

COMMUNICATIONS PRIVACY

Federal Policy and Actions

GAO/OSI-94-2

GAO

United States
General Accounting Office
Washington, D.C. 20548

Office of Special Investigations

B-253647

November 4, 1993

The Honorable Jack Brooks
Chairman, Committee on the Judiciary
House of Representatives

Dear Mr. Chairman:

In April 1992, we testified before your Subcommittee on Economic and Commercial Law about the threat of "economic espionage"—the unauthorized acquisition of U.S. proprietary or other information by a foreign government to advance the economic position of that country—against U.S. industry. Subsequently, you requested that we further examine whether federal policies negatively affect U.S. corporations' ability to protect themselves against economic espionage.

On the basis of your request, we focused on the following issues:

- the need for information privacy in computer and communications systems—through such means as encryption, or conversion of clear text to an unreadable form—to mitigate the threat of economic espionage to U.S. industry;
- federal agency authority to develop cryptographic standards for the protection of sensitive, unclassified information and the actions and policies of the National Security Agency (NSA), Department of Defense, and of the National Institute of Standards and Technology (NIST), Department of Commerce, regarding the selection of federal cryptographic standards;
- roles, actions, and policies of NSA and the Department of State related to export controls for products with encryption capabilities and industry rationale for requesting liberalization of such controls; and
- the Federal Bureau of Investigation's (FBI) legislative proposal regarding telephone systems that use digital communications technology.

Background

In July 1990, you requested that we determine if industrial espionage against U.S. industry by foreign entities was a problem and, if so, the federal government's response. We found that with the end of the Cold War and the resulting shift in focus from military to economic power, there was evidence that economic espionage has become a growing problem for U.S. companies at home and abroad. However, the extent of the problem in the United States cannot be quantified for a number of reasons: First, U.S. companies are reticent to disclose such information to the public for fear of disclosing information to competitors or of losing their stockholders' confidence. Also, once it is determined that a company has been victimized, it is often difficult to place an approximate value on the proprietary data and trade secrets that have been lost. Third, foreign intelligence agencies often use sophisticated techniques that may go undetected, making it difficult for companies to prove theft or compromise.

In our April 29, 1992, testimony before your Subcommittee,[1] we stated that economic espionage hurts U.S. industry. U.S. vendors of products with encryption capabilities and telecommunications-service providers also testified that U.S. government policy hinders both the safekeeping of U.S. industry's competitive secrets and international competitiveness. They further testified that because products with commercial encryption technology are available internationally, the U.S. government should relax restrictions on the export of such products to improve their ability to compete in the world marketplace.

The growth in reliance upon computer and communications technologies for commerce has led to increased international attention to securing information through cryptography. Powerful cryptographic techniques have been published for years and are increasingly available in products worldwide. This increased availability is causing concern for law enforcement and national security entities worldwide, relative to the performance of their missions. For decades, governments around the world have used statutory and regulatory powers to restrict the use and dissemination of cryptographic technologies. However, these restrictions are generally not published or available for study.

U.S. vendors expressed concern about policies regarding (1) federal cryptographic standards for communications privacy of sensitive, unclassified information and (2) the FBI's digital telephony legislative proposal and public comments on encryption. They stated that to be consistent with prevailing standards, the U.S. industry has made substantial investment in secure technology products that might not be compatible with evolving federal standards. The lack of industry input in the evolving standards, representatives believed, would cause the industry to follow two sets of standards in its technology development: one set to protect against unauthorized access and to compete in the international marketplace; the other to interact with the federal sector. Further, U.S. vendors were concerned that restrictions would be placed on the

[1] Economic Espionage: The Threat to U.S. Industry (GAO/T-OSI-92-6).

development and the use of communications and encryption technologies to meet law enforcement requirements and national security concerns, thus hampering their ability to compete in the global marketplace. The FBI and NSA, on the other hand, were concerned that such technologies might interfere with the performance of their missions, causing serious law enforcement and national security problems. (See app. I.)

Results in Brief

Increased use of computer and communications networks, computer literacy, and dependence on information technology heighten U.S. industry's risk of losing proprietary information to economic espionage. In part to reduce the risk, industry is more frequently using hardware and software with encryption capabilities. However, federal policies and actions stemming from national security and law enforcement concerns hinder the use and the export of U.S. commercial encryption technology and may hinder its development.[2]

NIST and NSA have invested several years of effort in developing certain federal cryptographic policies and federal standards relating to communications privacy for sensitive, unclassified information. These policy issues are formulated and announced to the public, however, with very little input from directly affected business interests, academia, and others. Although the Computer Security Act of 1987 reaffirmed NIST's responsibility for developing federal information-processing standards for the security of sensitive, unclassified information, NIST follows NSA's lead in developing certain cryptographic standards.

Although the Departments of State and Commerce are responsible for the U.S. export control system, NSA plays a major role in determining rules for exporting U.S. products with encryption capabilities. NSA affects such decisions as (1) whether individual products are placed on the more restrictive State-controlled "munitions list" or the less restrictive Commerce-controlled list and (2) whether particular products on the munitions list can be licensed for export. Industry representatives stated that stringent export controls restrict U.S. industry's ability to compete for market share in international markets for products with encryption capabilities.

The export controls (for products with encryption) of many countries may be similar in stringency to those of the United States. However, industry

[2] We did not evaluate the validity of the law enforcement or national security concerns relative to federal cryptographic policy or export control.

representatives cited examples of products exported from other countries that would be restricted for export from the United States. Thus, it appears that the controls of several countries are less stringent than are U.S. controls.

The FBI, in 1992, proposed legislation designed to ensure wiretapping capabilities in the face of emerging digital telecommunications technology. The proposal was to compel telecommunications service providers and private branch exchange operators to ensure that wiretapping needs could be met. It sought to prohibit the use of any technology by these entities that would impede the government's ability to intercept electronic communications when authorized by law. In early 1993, the FBI informed us that it was reevaluating its position on this proposal.

Thus, national security, law enforcement, and business concerns—plus the effectiveness of U.S. export controls—are all factors to be considered in determining what U.S. policies should be.

Use of Encryption to Protect Against Economic Espionage

During your Subcommittee's spring 1992 hearings, the Director, Central Intelligence Agency (CIA), testified that the communications and computer systems of U.S. industry were attractive targets for sophisticated foreign intelligence attacks. While it is well recognized that industry is increasingly using encryption to protect proprietary information, U.S. industry's development of products with encryption capabilities—as well as their use and export—is hindered by federal policy responding to national security and law enforcement concerns. (See app. I.)

NIST and NSA Actions Regarding Development of Cryptographic Standards

Over the past decade, hardware and software industry representatives, cryptographers outside NSA, academia, and others have had little opportunity to participate in or contribute to the selection or the development of cryptographic algorithms, or mathematical procedures, for proposed federal standards related to cryptography. One type of cryptographic standard would support the privacy of communications and provide for both the verification of a sender's identity and the integrity of the message. It is referred to as a public-key cryptographic[3] standard, in which the word "key" relates to the code for unlocking encrypted messages. NSA and NIST discuss the development or the selection of cryptographic algorithms for the development of these standards primarily

[3] Public-key cryptography uses two matched keys—a shared public key and a private key. See glossary.

in classified meetings, such as those of the Technical Working Group.[4] As a result, federal agencies invest years in developing proposed cryptographic standards for sensitive, unclassified information before public input is solicited. (See app. II.)

The Computer Security Act of 1987 reaffirmed NIST as the responsible federal agency for developing federal cryptographic information-processing standards for the security of sensitive, unclassified information. However, NIST has followed NSA's lead when developing certain cryptographic standards for communications privacy. For example, in 1982, NIST began developing a public-key cryptographic standard. NIST terminated the project at NSA's request. Then, in 1989, in accordance with a 1989 NIST/NSA Memorandum of Understanding, NIST requested NSA assistance in another effort to develop such a standard. This standard was to provide for verification of signature—the sender's identity; provide for integrity of the message; and support communications privacy using one algorithm. In 1991, NIST proposed the Digital Signature Standard (DSS), a standard based on an algorithm developed by NSA that, because of NSA and FBI concerns, provides for verification of the sender's identity and the integrity of the message but does not support communications privacy. When public input was solicited in 1991, industry representatives stated that a federal public-key standard was needed that (1) supported privacy in communications and (2) was compatible with other U.S. and international standards. They stated that delay in developing such a federal standard has hindered industry's development of products with encryption capabilities.

In April 1993, the administration announced its telecommunications privacy initiative and plan to develop a comprehensive policy on encryption. The President directed the Secretary of Commerce, in consultation with other federal agencies, to develop an encryption standard based on a key-escrow system.[5] This standard, proposed by NIST in July 1993, is to facilitate the use of a chip[6] that incorporates a classified encryption algorithm. Use of the chip will allow legally authorized government officials to have access to the clear (plain) text of encrypted communications. The Attorney General is tasked to establish two

[4] A Technical Working Group was established pursuant to the 1989 Memorandum of Understanding between NIST and NSA to coordinate NIST's cryptographic efforts.

[5] A key-escrow system involves third-party organizations that, together, have the means for decoding communications and the responsibility for maintaining the privacy of encrypted communications, except when interception of electronic communications is legally authorized. See glossary.

[6] The administration previously referred to this computer chip as Clipper Chip. It was developed on the basis of NSA technology.

cooperating third parties to maintain computer databases that will enable government officials to access the clear text of encrypted communications. According to a Justice Department official in September 1993, key-escrow candidates were to be discussed with Members of Congress prior to being publicly announced. This official confirmed that NIST and a nonlaw-enforcement agency of the Treasury Department were among those being considered. As of October 28, 1993, the key-escrow agents had not been publicly announced. Although NSA began developing this key-escrow system over 3 years ago, public input was not requested until June 1993. (See app. II.)

Federal Policy Regarding Export Control of Products With Encryption Capabilities

The U.S. export control system is divided into two regimes: the Department of State controls a list of munitions items under the authority of the Arms Export Control Act, and the Department of Commerce controls a list of dual-use items, i.e., items having both military and civilian applications, under the Export Administration Act.[7] Controls on munitions items are generally more restrictive than those on dual-use items. Therefore, industry generally prefers to have products on the dual-use list controlled by Commerce.

NSA plays a major role in determining rules for exporting U.S. products with encryption capabilities. The scope of NSA's review is generally limited to those products and technologies whose export could affect the performance of NSA missions. The review affects such decisions as (1) whether individual products are placed on the more restrictive State-controlled "munitions list" or the less restrictive Commerce-controlled dual-use list and (2) whether particular products on the munitions list may be licensed for export.

State is required to periodically review the munitions list to see if certain items can be transferred to Commerce's jurisdiction. Any changes to the munitions list, however, must have the concurrence of the Department of Defense. NSA plays an extensive role in this concurrence when encryption products are being considered for removal from the munitions list. Responding to a 1990 executive order, State led an interagency review of the munitions list to identify items that could be transferred to Commerce's jurisdiction. Mass-market software with encryption capabilities was one item reviewed.

[7] Export Controls: Issues in Removing Militarily Sensitive Items From the Munitions List (GAO/NSIAD-93-67, Mar. 31, 1993).

The software industry pressed for the transfer of mass-market software with encryption capabilities from State to Commerce, claiming that export controls reduced U.S. international sales of products with encryption capabilities and might hinder the pace at which these products were developed. State proposed to transfer export-control jurisdiction of mass-market software to Commerce on the condition that Commerce impose foreign policy controls on the licensing of such products. One reason for the request is that State believed that it would be impossible to control the export of mass-market software because the products were widely available. NSA successfully argued against the proposal on national security grounds.

To allay industry's concern that such software continues to be controlled on the munitions list, State amended its regulation in July 1992. It established a procedure to expeditiously transfer to the Commerce list those mass-market software products with encryption capabilities that met certain criteria. Industry representatives continue to press for the transfer of additional mass-market software and other products with encryption capabilities to the Commerce list to improve the possibility and the predictability of export approval. (See app. III.)

Although the extent is not possible to quantify, U.S. industry representatives stated that stringent U.S. export control of products with encryption capabilities reduced their international sales.[8] An example of a product type for which export controls affect U.S. global competitiveness is software with encryption capabilities used in international commercial networks. As an example of less stringent foreign controls, a German company contracts with a Japanese company to manufacture a high-speed encryption chip for export to Germany. In contrast, U.S. export controls prevent U.S. companies from exporting such a chip to the German company. Although the United States may not export such chips to this German company, U.S. companies may purchase secure products that contain these chips.

[8] The Software Publishers Association has estimated that (1) the foreign market for mass-market software with encryption capabilities is growing at least 20 percent each year and (2) the potential U.S. share of the foreign market could total $3-5 billion annually by 1997.

FBI-Proposed Digital Telephony Legislation and Comments on Encryption

In 1992, the FBI proposed legislation to ensure its wiretapping capabilities in a digital communications environment. The proposed legislation would have required electronic communications service providers—such as local telephone companies and cellular service providers—to ensure the ability of government agencies to implement lawful orders or authorizations to intercept communications. Communications providers would have been prohibited from employing communications technology that would bar the government's ability to intercept electronic communications when authorized by law. However, according to FBI representatives in early 1993, the FBI was reevaluating its position on the proposal. In the meantime, industry has been working with the FBI to improve the capability of intercepting telephone traffic when legally authorized.

Additionally, in April 1993, the administration announced that a comprehensive policy on encryption would be developed. The FBI publicly announced that it supported the administration's key-escrow system, which would allow government officials, when legally authorized, access to the clear text of encrypted communications. (See app. IV.)

A dilemma exists between the growing need for communications privacy in today's global competitive environment and the need for access to communications by our law enforcement and national security agencies. Extensive debate has occurred during the past several decades over how to meet these competing needs and whether a civilian organization or a military intelligence agency should control the development of federal information-processing standards for sensitive, unclassified information.

The Computer Security Act of 1987 reaffirmed the role of a civilian organization—NIST, Department of Commerce—in developing such standards, albeit in consultation with NSA. Because national security and law enforcement concerns have been driving significant NIST decisions related to these standards and because the demand for encryption is increasing, the debate endures.

Between November 1992 and June 1993, we reviewed federal actions and policies that affect technologies related to privacy of electronic communications. We relied on our prior work for much of the information on economic espionage, the proposed DSS, digital telephony, and export control. We gathered other information largely from interviews and correspondence with officials of the Departments of Commerce and State, NIST, and NSA, as well as representatives of industry and academia. The FBI declined to provide briefings on economic espionage, digital telephony, and encryption issues for our 1992 testimony and for this report. As requested, we did not obtain official agency comments on a draft of this report.

For the reader's convenience, we have included a glossary of communications, cryptographic, and related terms used in the report.

As arranged with your office, unless you publicly release its contents earlier, we will not make this report available to others until 10 days after the date of this letter. At that time, we will send copies of the report to the appropriate congressional committees and interested parties. We will also make copies available to others on request.

If you have questions concerning this report, please contact me or Assistant Director Donald G. Fulwider of my staff on (202) 512-6722. Major contributors to this report are listed in appendix V.

Sincerely yours,

Richard C. Stiener
Director

Contents

Abbreviations

CIA	Central Intelligence Agency
COCOM	Coordinating Committee for Multilateral Export Controls
DES	Data Encryption Standard
DSS	Digital Signature Standard
FBI	Federal Bureau of Investigation
GAO	U.S. General Accounting Office
IBM	International Business Machines, Inc.
IMTEC	Information Management and Technology Division, GAO
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSDD	National Security Decision Directive
NSIAD	National Security and International Affairs Division, GAO
OSI	Office of Special Investigations, GAO
RC2	Rivest Cipher 2
RC4	Rivest Cipher 4
RSA	Rivest, Shamir, and Adleman

Background and Methodology

Need for Privacy of Information in Computer/ Communications Systems—The Threat of Economic Espionage Against U.S. Industry

The federal government has historically recognized and addressed the international nature of military and intelligence threats. The government is beginning to recognize that a broader international threat to U.S. information resources is emerging with the proliferation of international computer networking and a shift from conventional military conflict to economic competition. During an April 1992 hearing on economic espionage conducted by the Subcommittee on Economic and Commercial Law, House Committee on the Judiciary, the Director of the FBI stated, "Now and in the future, the collection strategies of adversaries and allies alike will not only focus on defense related information, but also include scientific, technological, political and economic information." The Director of the CIA similarly testified that U.S. industry computer and communications systems were attractive targets for sophisticated foreign intelligence attacks.

Increasingly serious threats in the global marketplace require the commercial sector to effectively secure its information resources, according to an Information Systems Security Association paper presented to the Computer System Security and Privacy Advisory Board. While nonelectronic proprietary information can be compromised through the theft of marketing reports or photos of prototypes, the theft of electronic proprietary information can be accomplished through breaking into a computer system—or computer hacking—and message and voice monitoring during data and voice transmission. Individuals can compromise information, for example, by guessing passwords or exploiting operating-system weaknesses. Additionally, message and voice monitoring during data and voice transmission can occur at a number of locations throughout the communications flow, such as where the message recipient is located.

The increased use of computer and communications systems by industry has increased the risk of theft of proprietary information. A 1986 National Telecommunications and Information Systems Security Committee[9] report assessed the security posture of the U.S. government and telecommunications/information systems that process classified or sensitive, unclassified information. The report stated, "Hostile government intelligence collection agencies, terrorist organizations, and criminal elements are undoubtedly exploiting this lack of security to the detriment of U.S. national interests." Although these threats may require a variety of

[9] The Committee was established by National Security Decision Directive 145 to help manage federal information systems security issues. This directive was partially replaced in 1990.

countermeasures, encryption is a primary method of protecting valuable electronic information.

Encryption as a Security Measure

Encryption—the conversion of clear text into an unreadable form—is a tool that can be used to protect valuable information and perform other functions. Encryption can be used to (1) encrypt and decrypt data, (2) send or exchange secret coding and decoding keys securely and electronically without sharing them with a third party, and (3) digitally sign a document. The first two functions provide for privacy and security of messages. The third function, "digital signature," is used to verify both the sender of a message and that a message has not been tampered with.

Encryption requires an algorithm, or a mathematical procedure, which is used in conjunction with at least one key—a long string of bits—to encrypt and decrypt messages. In this report, we discuss six encryption algorithms—Skipjack, the Data Encryption Standard (DES), RC2, RC4, RSA,[10] and the algorithm in the proposed DSS. Skipjack, DES, RC2, and RC4 encrypt and decrypt information but require an additional method for transporting secret keys to other parties. The method can be (1) a courier, (2) an additional algorithm that transports or exchanges secret keys securely and electronically between two parties, or (3) an electronic method requiring a third party with whom the secret keys have been shared. DSS supports digital signature only. RSA supports digital signature, message encryption, and key management—the ability to securely send secret keys electronically without sharing the secret keys.

Key management/exchange—sending or exchanging secret keys securely and electronically without having to share them with a third party—is an important aspect of providing communications privacy for international commerce. Sharing secret keys with a third party can represent added risk and cost.

Encryption algorithms can be compared to locks. Strong encryption algorithms, like strong locks, require more time and effort to break. The design of the algorithm and the length of its keys are two factors that contribute to its strength. In general, the longer an algorithm's keys are, the stronger the security or privacy provided by that algorithm. Keys must be known or guessed to forge a digital signature or read an encrypted message.

[10] The "RC" in RC2 and RC4 is an abbreviation for Rivest Cipher. RSA's name is based on the last initials of its three inventors: Ronald L. Rivest, Adi Shamir, and Leonard M. Adleman.

Scope and Methodology

To respond to the request, we reviewed information collected for our April 1992 testimony (GAO/T-OSI-92-6, Apr. 29, 1992). We also reviewed federal laws, regulations, policies, White House correspondence, a Memorandum of Understanding, hearing records, memorandums of NIST/NSA Technical Working Group meetings, and GAO testimony[11] to understand the history of authority over cryptographic standards, as well as how they are developed.

We reviewed information developed for our report entitled Export Controls: Issues in Removing Militarily Sensitive Items From the Munitions List (GAO/NSIAD-93-67, Mar. 31, 1993). We also interviewed cryptographers working for industry and representatives of NIST and the Bureau of Export Control of the Department of Commerce; NSA; the Department of State; hardware and software manufacturers; and industry associations—e.g., the Information Technology Association of America, the Industry Coalition on Technology Transfer,[12] the Software Publishers Association, and the Computer Business Equipment Manufacturing Association.

Our previous report—FBI: Advanced Communications Technologies Pose Wiretapping Challenges (GAO/IMTEC-92-68BR, July 17, 1992)—provided much of the information regarding the FBI's legislative proposals. The FBI declined to provide briefings on economic espionage, digital telephony, and encryption issues for our 1992 testimony and for this report.

Our work was performed primarily between November 1992 and June 1993 in Washington, D.C.

[11] The Potential Impact of National Security Decision Directive (NSDD) 145 on Civil Agencies, statement by Warren G. Reed, GAO, before the U.S. House of Representatives, Subcommittee on Transportation, Aviation and Materials, Committee on Science and Technology (June 27, 1985). National Institute of Standards and Technology and the National Security Agency's Memorandum of Understanding on Implementing the Computer Security Act of 1987 (GAO/T-IMTEC-89-7, May 4, 1989).

[12] The coalition represents 10 information technology associations, such as the Computer and Business Equipment Manufacturers Association.

Federal Agency Authority and Actions Concerning Cryptographic Standards

Conflict Over Federal Agency Authority for Cryptographic Standards to Protect Sensitive, Unclassified Information

An information-processing standard is a set of detailed technical guidelines used to support specific functions and/or interoperability in hardware, software, or telecommunications development, testing, and/or operation. Federal information-processing standards often significantly affect the widespread adoption of technology and can result in lower unit costs to the user. Although federal agencies are required to comply with federal information-processing standards, industry voluntarily has adopted many of these standards.

One of the missions given to NIST[13] when established by the Congress was to help industry develop technology and to facilitate rapid commercialization of products. NIST became responsible for federal standards for information systems, including the security of unclassified information in 1965, when the Brooks Act (P.L. 89-306) was enacted.

In 1984, the President signed National Security Decision Directive 145[14] —developed by the Department of Defense—that authorized the Director of NSA to review and approve all security-related standards for information systems, including those set by NIST. We testified in 1985 that this directive could significantly affect the management of systems by civil agencies and commercial interests[15] because it established a new category of "sensitive, unclassified government or government-derived information, the loss of which could adversely affect the national security interest . . . " without clearly defining the types of information in this category.

During hearings in the mid-1980s, the Congress raised the issue about having NSA or NIST—a military or a civilian agency—control federal information-processing standards to protect sensitive, unclassified information. One concern that was raised related to the appropriateness of giving NSA a role in developing or approving standards for the privacy of sensitive, unclassified information because of its national security role with respect to cryptography. The Computer Security Act of 1987 was enacted, in part, to address this concern. The act reaffirmed NIST's responsibility for developing standards to help government agencies protect sensitive, unclassified information. The act authorized NIST to draw upon the technical advice and assistance of NSA, when appropriate, to avoid unnecessary and costly duplication of effort and ensure that

[13] NIST was formerly the National Bureau of Standards.

[14] In 1990, National Security Directive 42 replaced National Security Decision Directive (NSDD) 145, except for ongoing telecommunications protection activities mandated by NSDD 145 and Presidential Directive 24.

[15] Reed, GAO, June 27, 1985.

standards for protecting sensitive, unclassified information were consistent and compatible, to the maximum extent feasible, with standards for classified systems. The act required that NIST draw upon NSA guidelines to the extent that NIST determined that such guidelines were consistent with requirements to protect sensitive, unclassified information in federal computer systems.

In March 1989, NSA and NIST signed a Memorandum of Understanding that is still in effect. The memorandum requires that NIST request NSA's assistance on all matters related to cryptographic algorithms, not solely NIST-selected cryptographic matters.[16] If NIST and NSA disagree on an issue, the memorandum states that the matter may be appealed to the Secretaries of Commerce and Defense. Unresolved matters may be referred through the National Security Council to the President. At a number of Technical Working Group meetings, NIST and NSA representatives have disagreed over whether to develop a public-key standard for key management/exchange. NSA and NIST have not elevated any issues of disagreement to their Secretaries, as allowed by the process outlined in the Memorandum of Understanding.

We testified[17] in 1989 that this Memorandum of Understanding made NSA appear to be more influential in NIST's standard-setting processes relative to cryptographic systems than was intended by the Congress in the Computer Security Act of 1987. We further testified, "The [memorandum] appears to increase the burden of leadership which the Secretary of Commerce must exercise in implementing the Computer Security Act of 1987. . . ."

[16] According to the Memorandum of Understanding, both agencies are to share project updates quarterly, as well as project reviews upon request. The memorandum also established a Technical Working Group of three NIST and three NSA representatives to review and analyze technical issues of mutual interest.

[17] GAO/T-IMTEC-89-7, May 4, 1989.

NIST, NSA, and Administration Actions Related to Standards for Communications Privacy and for Digital Signature

NSA, because of its expertise and national security concerns, has significantly participated in NIST's development of federal cryptographic standards. NIST has insufficient resources to develop and evaluate cryptographic algorithms for federal standards without assistance, according to a NIST representative. Further, national security and law enforcement concerns have hindered the development of standards related to (1) a specific secret-key encryption standard—DES—and (2) public-key encryption.

Secret-key cryptography uses an algorithm and the same secret key for encrypting and decrypting data. Public-key cryptography uses an algorithm and two matched keys—a public key and a private key—and can perform (1) digital signature, (2) secure transmission or exchange of secret keys, and/or (3) encryption and decryption.

We did not evaluate the validity of law enforcement or national security concerns related to national cryptographic policy.

The Data Encryption Standard and Communications Privacy

DES, published in 1977 after extensive NSA involvement, is the most widely known modern encryption algorithm. The U.S. and international financial communities and others use DES to provide communications security. For example, Fedwire and the Clearing House Interbank Payment System, which process over 350,000 messages daily valued at $1-2 trillion, use DES to protect messages from unauthorized modification. DES has withstood the test of publicly known attempts to break it. However, DES has been the subject of controversy since its inception.

Initial Controversy and 1983 Reaffirmation

In May 1973, NIST issued a solicitation through the Federal Register for interested parties to submit cryptographic algorithms for possible consideration as a data encryption standard. NIST requested NSA's assistance in evaluating the few cryptographic algorithms received, and NSA reported that no suitable algorithms had been submitted.

NIST solicited for algorithms again in August 1974. At NSA's suggestion, IBM (International Business Machines, Inc.) submitted one of its algorithms to NIST. On the basis of NSA advice, IBM shortened the key length and, at NSA's request, did not publicly disclose all the design criteria used in creating its candidate algorithm.

The lack of public disclosure of design criteria and the shortened key length became the subjects of controversy. NIST held two workshops prior to publishing the DES algorithm, which was based on the IBM-submitted algorithm. One workshop was related to the design of the algorithm and focused on whether a "trapdoor"—a secret entry point to DES through which a developer or other entity could bypass security controls and decrypt messages—existed. The other workshop focused on the economic and security trade-offs of modifying the implementation of the algorithm to increase its key length. In 1977, NIST adopted DES as a federal standard, with the provision that NIST review it every 5 years.

Because of several allegations by cryptographers in industry and academia, including one that NSA had been improperly involved in the development of DES, the Senate Select Committee on Intelligence conducted an investigation. In 1978, the staff report concluded that NSA had acted properly and that the agreed-upon key size was more than adequate for commercial applications. NIST reaffirmed DES in 1983.

Renewed Controversy and 1988 Reaffirmation

In 1985, NSA announced that it would not endorse new products with DES implementations after 1987. Although there were no publicly known security problems or risks related to DES use and about 20 vendors had produced numerous products implementing the DES algorithm, NSA planned to endorse a new classified algorithm, which it would control, for industry's use with sensitive, unclassified information. The major reason that NSA cited for wanting industry to use a nonpublic algorithm was that it would be more secure if it was not published and available to the public. However, a representative of the American Bankers Association testified in 1987 before the Legislation and National Security Subcommittee, House Committee on Government Operations regarding bankers' concerns. These included that (1) NSA might control the encryption keys, (2) financial institutions would bear considerable cost in switching algorithms, (3) DES was still considered secure, and (4) the classified algorithm could not be used internationally.

In 1987, NSA recommended to NIST that DES be used to protect only electronic financial transactions, not other electronic information. NSA stated that reducing DES use would also reduce the potential attractiveness of DES as an intelligence target. NSA offered to work with DES chip manufacturers and develop pin-for-pin replaceable circuits employing the NSA-developed cryptography. However, none expressed interest. After much discussion, NIST reaffirmed DES—without limiting its use to financial transactions—in 1988.

1989 NIST Request for NSA Assistance in Developing Key-Generation Standard

In 1989, NIST requested NSA assistance in developing a federal information-processing standard for generating pseudorandom (good) cryptographic keys for DES and began to discuss this issue at the NSA/NIST Technical Working Group meetings. NIST did not develop this standard because NSA disapproved of the effort and did not provide the requested assistance. This standard was intended to help users select DES keys that could not be easily compromised. NIST stated that the system should be able to (1) generate pseudorandom keys for DES and (2) verify that a generated key could not be predicted by examining any sequence of previously generated keys.

According to a NIST issue paper, commercial organizations do not want to use cryptographic keys generated by the federal government. The paper stated that to maximize security, each agency should generate its own keys. NSA did not believe that NIST had the responsibility to publish a standard on key generation, according to a NIST memorandum. The memorandum further recorded that NSA had stated it was prepared to generate DES keys for federal agencies and provide private sector DES users that had government sponsors with keying material. Finally, the memorandum stated that NSA's chief concerns with this standards effort were that it would help the private sector develop stronger key-management systems and hence they would have better security.

1993 Review and Possible Reaffirmation

In September 1992, NIST requested comments, through the Federal Register, for NIST's review of DES. NIST requested comments on three alternatives: (1) reaffirm DES, (2) withdraw DES and possibly issue another standard, and (3) revise the applicability and/or implementation of DES. All 38 respondents favored DES reaffirmation; about two-thirds recommended reaffirmation and revision. Six government and six industry respondents proposed that the standard be revised to allow DES implementation in software—currently DES is limited to hardware implementation, and federal agencies are required to get a waiver to implement DES in software. DES continues to be a strong algorithm, according to NIST. NIST has proposed the reaffirmation of DES with the above-mentioned revision to the Secretary of Commerce. However, as of September 14, 1993, the Secretary had not approved it. NIST will consider DES alternatives over the next 5 years.

Public-Key Management/Exchange and Digital Signature Standards

NIST has not proposed a key-management/exchange standard based on public-key cryptography—to support the secure transmission, or the exchange, of secret keys electronically without sharing them with a third party—because of NSA and FBI concerns. Such a standard would support communications privacy.

Early 1980s

In 1982, NIST solicited, through a Federal Register notice, for public-key algorithms—the basis of public-key cryptography, which can provide message encryption, key management/exchange, and digital signature. RSA Data Security, Inc., was willing to negotiate the rights to use RSA—the most widely accepted public-key algorithm—as a federal standard, according to a NIST representative. NSA and NIST representatives met several times to discuss NSA concerns regarding the 1982 solicitation. However, NIST terminated the public-key cryptographic project because of an NSA request, according to a 1987 NIST memorandum. The 1982 NIST solicitation was the last formal opportunity provided for industry, academia, and others to offer public-key algorithms for a federal standard and to participate in the development of a federal public-key standard that could support key management/exchange.

Late 1980s

In 1989, NIST requested that NSA assist it in evaluating NIST-proposed candidate algorithms for a set of public-key encryption standards. NIST stated that the selected algorithm must be public, unclassified, and implementable in both hardware and software. NIST preferred one algorithm to perform both digital signature and key distribution (management/exchange), which is the ability to send secret keys securely and electronically without sharing them with a third party. According to NIST memorandums, the NIST members of the Technical Working Group preferred RSA because it performed both functions. NSA and NIST met frequently to discuss these standards.

NSA briefed NIST on its work regarding the public-key encryption algorithms 7 months after NIST's first request for assistance in 1989. NIST representatives noted that NSA had excluded RSA as a candidate algorithm. For the proposed DSS, NSA developed an algorithm that performs digital signature but not key management/exchange, which supports communications privacy.

Early 1990s—The Proposed Digital Signature Standard

In an August 1991 Federal Register, NIST announced a proposed federal DSS. Impact on national security and law enforcement were factors considered in selecting the proposed DSS, as cited in the Federal Register notice. The majority of private sector comments on the proposed DSS were negative, according to a NIST representative. Responding to one industry security concern, NIST agreed to provide the capability for longer keys. However, other concerns, including the following, have yet to be resolved:

- Many large U.S. software producers and other companies (e.g., IBM, Apple, Lotus, and Microsoft) had already obtained licenses to use RSA, commonly referred to as the de facto, international standard for digital signature. (RSA is the most well-known algorithm that complies with the international standard for digital signature.) Several of these companies have produced, or are in the process of evaluating or producing, mass-market software with encryption capabilities—such as Lotus Notes—that uses RSA for digital signature and/or public-key management support of message privacy.
- A number of industry representatives stated that most of their customers will want to use RSA for digital signature to support international commerce. Thus, industry may be required to develop and support two different versions of products to support digital signature—one for government users (DSS) and one for nongovernment and international users (RSA).
- For a broad range of digital signature applications, it appears that DSS, as proposed, may be less efficient than RSA. According to a number of industry representatives and cryptographers, this is because RSA can verify signatures faster. Signature verification, in general, is the most frequent, and thus most time-consuming, operation in the digital signature process. One example of the frequency of signature verification versus that of signature is check processing. Although a check is signed once, the signature may be verified numerous times while the check is being processed.

Early 1990s—No Proposal for a Key-Management/Exchange Standard

NIST has not yet proposed a key-management/exchange standard based on public-key cryptography because of NSA requests. Although in May 1990 NSA proposed a key-management/exchange technique to NIST, the technique did not meet two of NIST's requirements—that the algorithm be made public and be capable of implementation in software.

In December 1991, the Computer System Security and Privacy Advisory Board—composed of representatives from the computer and telecommunications industry, independent experts in telecommunications, and federal employees and established by the Computer Security Act of 1987—voted to inform the NIST Director that DSS had grave problems. Board members stated that DSS was a drain on NIST's resources, inconsistent with international standards, and technically inadequate without a key-management functionality. In 1992, they also resolved that the Secretary of Commerce should approve DSS only on conclusion of a national review—to include the national security, law enforcement, "government sensitive unclassified," and commercial communities—to discuss the widespread use of cryptography.

In a statement before your Subcommittee on May 7, 1992, the NIST Director stated that a key-distribution (management/exchange) technique was needed. He further stated that public-key cryptography, if implemented properly, better satisfied this need, although law enforcement and national security concerns were to be considered. NIST plans to submit DSS to the Secretary of Commerce for approval as a Federal Information Processing Standard in 1993, although the Board's concerns have not been resolved.

Announcement of a Proposed Standard for Encryption With a Key-Escrow System Based on NSA-Developed Technology

In July 1993, NIST proposed a cryptographic Federal Information Processing Standard—the key-escrow system[18]—that would enable decryption of lawfully intercepted telecommunications. This system would allow legally authorized government officials to access the plain text of encrypted communications. NSA proposed this technique to NIST in 1990. However, NIST rejected the technique because NIST required that the algorithm be made public and capable of being implemented in software. In April 1993, the President directed NIST, in consultation with other federal agencies, to begin writing standards to facilitate the procurement and the use of the key-escrow technique in federal communications systems.

The purpose of the currently proposed standard is to promote the use of an NSA-developed classified encryption algorithm, known as Skipjack, as part of a key-escrow system on an NSA-developed chip.[19] The administration also seeks with this same technology to help companies protect proprietary information, protect the privacy of telephone conversations, and prevent unauthorized access to electronically transmitted data.

Under the current proposal, the keys would be secured and controlled as follows: Two databases will be established to hold the two components of each key produced for each chip. These two components are necessary to decrypt the message. According to a Justice Department official in September 1993, key-escrow candidates were to be discussed with Members of Congress prior to being publicly announced. This official confirmed that NIST and a nonlaw-enforcement agency of the Treasury

[18] A key-escrow system is an electronic means of reconstructing a secret key (for secret-key encryption) or a private key (for public-key encryption) for the purpose of decrypting a message.

[19] The current Administration previously referred to this chip as Clipper Chip.

Department were among those being considered. As of October 28, 1993, the key-escrow agents had not been publicly announced. The FBI has publicly announced that it supports the administration's key-escrow proposal.

Actions and Policy Regarding the Export of Products With Privacy Capability

Background

The U.S. export control system is divided into two parts—munitions items and dual-use items, or items having both civilian and military uses. The Department of State controls the export of munitions items under the Arms Export Control Act and is required to have Department of Defense concurrence when adding items to or deleting items from the U.S. Munitions List.[20] The Department of Commerce, on the other hand, controls the export of dual-use items under the Export Administration Act and establishes the Commerce Control List. In general, munitions controls are more stringent than Commerce's dual-use controls.

Defense Refusal to Remove Mass-Market Software With Encryption Capabilities From the U.S. Munitions List

Over the years, the two lists began to overlap and included, among other items, mass-market software[21] with encryption capabilities. In November 1990, the President ordered the removal of Coordinating Committee for Multilateral Export Controls (COCOM)[22] dual-use items from the U.S. Munitions List and its licensing controls unless significant national security interests would be jeopardized. Pursuant to the November 1990 executive order, the Department of State led an interagency review—including State, Commerce, and Defense—to identify overlapping items and determine which could be removed from the munitions list and transferred to Commerce's jurisdiction.

We reviewed the export control jurisdiction decisions the Departments of State and Defense had made regarding certain militarily sensitive items.[23] That review focused primarily on items other than encryption items. However, as a result of the President's order, one dual-use item in the interagency review was mass-market software with cryptographic capabilities. U.S. software exporters pressed the federal government to liberalize U.S. export controls to enhance the international competitiveness of their products.

Nevertheless, in April 1991, the Departments of State and Defense agreed to retain software with cryptographic capabilities on the U.S. Munitions List so that NSA could review all new software with cryptographic capabilities to determine if the products should be controlled on the

[20] GAO/NSIAD-93-67, Mar. 31, 1993.

[21] Mass-market software is software that is (1) generally available to the public by sale, without restriction, from stock at retail selling points through over-the-counter, telephone, and mail transactions and (2) designed for user installation without substantial supplier support.

[22] COCOM is an informal international organization that cooperatively restricts strategic exports to controlled countries.

[23] GAO/NSIAD-93-67, Mar. 31, 1993.

munitions list or the Commerce list. Additional reasons for maintaining this item on the munitions list are classified.

In January 1992, State reversed its position and proposed moving such software to the Commerce list, along with other items. State believed that controlling mass-market software with cryptographic capabilities would be impossible because the products were widely available. However, Defense refused to include such software in any compromise with Commerce, citing the inadequacy of Commerce's control system even with added foreign policy controls. Defense further cited the administration's opposition to the provision in a bill to reauthorize and amend the Export Administration Act as another reason that jurisdiction over this software should not be transferred. NSA's appeal to the Under Secretary of State for International Security Affairs prevailed, according to a State Department representative, and mass-market software with cryptographic capabilities was retained on the munitions list. NSA also presented its case to the President's Assistant for National Security Affairs, according to State Department representatives.

NSA and State Department Export Control Roles

NSA performs the technical review that determines, for national security reasons, (1) if a product with encryption capabilities is a munitions item or a Commerce list item and (2) which munitions items with encryption capabilities may be exported. The Department of State examines the NSA determination for consistency with prior NSA determinations and may add export restrictions for foreign policy reasons—e.g., all exports to certain countries may be banned for a time period.

Neither NSA, the Department of State, nor the Department of Commerce has provided industry with the detailed criteria for determining whether an item is a munitions item or a Commerce list item. The detailed criteria for these decisions are generally classified. However, vendors exporting these items can learn some of the general criteria through prior export approvals or denials that they have received. NSA representatives also advise companies regarding whether products they are planning would likely be munitions items and whether they would be exportable, according to State Department representatives.

Industry Raises Concern About Export License Process

Products with certain algorithms, such as DES, for message encryption require a munitions license and are generally nonexportable to foreign commercial users, except foreign subsidiaries of U.S. firms and international banking concerns. Other algorithms are permitted for export for privacy purposes at restricted key lengths. (DES and other algorithms—for nonprivacy purposes, such as password access control—are exported under control of the Commerce list.)

The Software Publishers Association sought to have export control jurisdiction of mass-market software with encryption capabilities transferred to Commerce. NSA and National Security Council representatives met with representatives of the Association, which specifically sought change regarding controls on DES.

State Establishes a Procedure Expediting Product Reviews for Determining Munitions Items

The Department of State amended[24] the regulations for implementing the Arms Export Control Act. The new regulation established a procedure that permits an expedited review—to determine whether the product is a munitions or a Commerce-controlled item—for certain mass-market software with encryption capabilities.[25]

According to a procedure outlined by the President's Assistant for National Security Affairs, a representative of the National Security Council will host a meeting with software industry representatives twice a year to enable the industry representatives to present their concerns, including whether keys should be lengthened to counteract the threat of increased computer power.

U.S. Export Controls for Products With Encryption Capabilities, in Some Cases, Apparently More Stringent Than Those of Other Countries

U.S. export controls for products with encryption capabilities—in at least some cases—appear more stringent than those of other countries. U.S. and foreign companies and an association provided three examples of such cases.

First, some member countries of COCOM, such as the United Kingdom, permit the export of mass-market software with encryption capabilities. In 1991, the COCOM countries agreed to exclude mass-market software with encryption capabilities or software in the public domain from one of the COCOM embargo lists used for export control. However, the United States maintains export control over this software.

[24] The U.S. Munitions List, 22 C.F.R. section 121.1, Category XIII, note (1993).

[25] The procedure can be applied for products with RSA, RC2, or RC4 when RSA key lengths are limited to 512 bits and RC2 and RC4 key lengths are limited to 40 bits. Key lengths affect the degree of message privacy. For example, an algorithm with a 56-bit key is over 65,000 times stronger against a certain kind of attack than the same algorithm with a 40-bit key. Different algorithms with the same key length are not necessarily equally strong because other factors contribute to strength.

Second, foreign companies may export products with encryption algorithms for message privacy, such as DES, to user groups and countries that U.S. companies and their foreign subsidiaries may not. According to an industry official, a German company contracts with a Japanese company to manufacture a high-speed encryption chip for export to Germany because U.S. companies are prevented by U.S. export rules from exporting to the German company.

Further, a U.S. subsidiary of a leading British vendor of encryption products uses these chips in a network security system. This U.S. subsidiary may market these products to any user in the United States. In contrast, foreign subsidiaries of U.S. companies are often limited by U.S. export rules to selling such products to designated user groups—the financial industry and foreign subsidiaries of U.S. companies—in countries where they are based, according to a representative of the Computer and Business Equipment Manufacturers Association.

Industry Cites Reasons for Relaxing Export Controls for Products With Encryption Capabilities

A number of industry representatives stated that the international availability of hardware and software with encryption capabilities could not be effectively suppressed because sophisticated, foreign-made encryption products were becoming more available worldwide. Although U.S. firms are restricted in the international sale of these products, vendors in the United Kingdom, Switzerland, Israel, Belgium, and the Commonwealth of Independent States offer a wide variety of secure products that use DES, RSA, and other algorithms, according to a statement by the Computer and Business Equipment Manufacturers Association and the Information Technology Association of America. They stated that about 16 companies in these 5 countries and Holland sold hardware and software products with cryptographic capabilities in their own and/or other countries, including the United States, Germany, Australia, Cyprus, Ireland, Israel, Singapore, and Sweden. As an example of the international availability of RSA and DES in software, ASKRI, a company in the Commonwealth of Independent States, sells an encryption product that implements both RSA and DES, according to its user's manual.

Although the extent is not possible to quantify, U.S. industry representatives stated that stringent U.S. export control of products with encryption capabilities reduced their international sales. International markets are important sources of revenue for U.S. industries.[26] According

[26] The Software Publishers Association has estimated that (1) the foreign market for mass-market software with encryption capabilities is growing at least 20 percent each year and (2) the potential U.S. share of the foreign market could total $3-5 billion annually by 1997.

to a number of industry representatives, export controls also hinder the pace at which these products are developed in the United States. Industry representatives state that because of the cost of development, they are reticent to develop products with encryption capabilities that may not be exported.

FBI-Proposed Digital Telephony Legislation and Comments on Encryption

Since 1986, the FBI has become increasingly aware of the potential loss of wiretapping capability due to the rapid deployment of new technologies, such as cellular and integrated voice and data services. In 1991, the FBI commented on a Senate bill concerning encryption. In 1992, the FBI developed several legislative proposals concerning wiretapping. Both encryption and wiretapping affect the FBI's methods and ability to collect evidence. In early 1993, the FBI told us that it is reevaluating its positions regarding digital telephony legislation and encryption issues until it has discussed these topics with officials in the new administration.

1992 Digital Telephony Proposals

In 1992, the FBI developed a legislative proposal to facilitate law enforcement agency wiretapping operations in a digital telephone network. (The proposal was not introduced as a bill in the Congress.) A law consistent with the proposal would have required compliance by telecommunications service providers and private branch exchanges with Federal Communications Commission regulations within a specified time period and would have prohibited the use of nonconforming equipment. However, according to our July 1992 report,[27] the FBI did not define its wiretapping needs in its original proposal.

The second version of the FBI proposal generally addressed the FBI's needs but did not provide the specifics necessary for the telecommunications industry to determine what would constitute full compliance with the proposal. For example, the version did not specify the time allowed to install a wiretap after receipt of a court order. Further, the second version did not address who should pay the cost of changes to the systems that would ensure the FBI's access. The FBI's third version in 1992 was similar to the second.

Collecting evidence by wiretapping is becoming difficult because of four growing technologies: (1) the integrated services digital network—an emerging communications system to integrate voice and data; (2) extended cellular telephone communications; (3) encryption; and (4) personal communication networks—advanced cellular telephone communications that will offer new communications services via very small, portable handsets.

In the summer of 1990, the FBI began technical discussions with industry experts on wiretapping solutions. The FBI had previously conducted its

[27] GAO/IMTEC-92-68BR, July 17, 1992.

own research on wiretapping but had not coordinated its research with industry research and development.

In May 1992, the FBI formed a technical committee composed of representatives from the FBI and the telecommunications industry. The purpose of this committee was to identify and select the technological alternatives that best met the FBI's needs. According to our July 1992 report, neither the FBI nor the telecommunications industry had a comprehensive analysis of the technological alternatives for wiretapping current and emerging technologies.

The General Services Administration expressed its views on the first and second versions of the FBI-proposed legislation in response to the Office of Management and Budget. The General Services Administration stated, in part, "there would be unknown associated costs to implement the proposed new technological procedures and equipment."

In addition, the Electronic Frontier Foundation—in coalition with communications services providers, computer hardware and software companies, and other groups—published a September 1992 report concerning the proposal.[28] The report expressed concern that a law based on the FBI's legislative proposal would impose new engineering standards with substantial costs.

FBI Comments on Encryption

In January 1991, the Senate Committee on the Judiciary proposed S. 266, the Comprehensive Counter-Terrorism Act of 1991, which addressed government access to "plain text," or decrypted, communications. The FBI supported the bill. However, representatives of industry and academia expressed concern that such a proposal would undermine the security, reliability, and privacy of computer-based communications.

Section 2201 of the bill, "Cooperation of Telecommunications Providers With Law Enforcement," read in part:

> "It is the sense of Congress that providers of electronic communications services and manufacturers of electronic communications service equipment shall ensure that communications systems permit the government to obtain the plain text contents of voice, data, and other communications when appropriately authorized by law."

[28] Electronic Frontier Foundation, et al., "An Analysis of the FBI Digital Telephony Proposal" (Sept. 18, 1992).

On April 26, 1991, the FBI issued a press response expressing its support of section 2201 of S. 266, stating that the bill "seeks to place on the telecommunications industry a sense of duty to design its new digital telecommunications systems so that law enforcement continues to receive only those communications specifically authorized by court order." The press response further stated, "[a]ffording a criminal subject the means, through encryption, of securely communicating in furtherance of an illicit activity is tantamount to providing a sanctuary immune from judicially authorized collection of evidence."

S. 266 was not enacted. Section 2201 of the bill was later included in S. 618, the proposed Violent Crime Control Act of 1991. Neither S. 618 nor its companion bill in the House of Representatives passed.

On April 19, 1993, representatives from the FBI announced support for the administration's key-escrow system. This system would allow legally authorized government officials to obtain access to the plain text of encrypted communications.

Major Contributors to This Report

Office of Special Investigations, Washington, D.C.

Donald G. Fulwider, Assistant Director for Financial and Economic Crimes
Robyn D. Stewart-Murray, Special Agent
Shelia A. James, Report Reviewer
M. Jane Hunt, Special Assistant for Investigative Plans and Reports

Accounting and Information Management Division, Washington, D.C.

Dr. Harold J. Podell, Assistant Director
Beverly A. Peterson, Senior Evaluator

Office of the General Counsel, Washington, D.C.

James M. Lager, Senior Attorney Adviser

Glossary

Algorithm

A mathematical procedure that can usually be explicitly encoded in a set of computer language instructions that manipulates data. Cryptographic algorithms are mathematical procedures used for such purposes as encrypting and decrypting messages and signing documents digitally.

Bit

Short for binary digit—0 or 1. Keys are strings of bits.

Cellular Transmission

Data transmission via interchangeable wireless (radio) communications in a network of numerous small geographic cells. Most current technology is analog—represented as electrical levels, not bits. However, the trend is toward digital cellular data transmission.

Clipper Chip

A microcircuit that contains a classified secret-key encryption algorithm—"Skipjack." Skipjack can be used in place of DES, RC2, RC4, and other secret-key algorithms to provide message privacy with a "key-escrow" system. (The administration initially referred to the microcircuit as the Clipper Chip and later discontinued using the term.)

COCOM

The Coordinating Committee for Multilateral Export Controls—an informal organization that cooperatively restricts strategic exports to controlled countries. COCOM consists of 17 countries that maintain three export control lists: (1) the International Industrial List, (2) the International Munitions List, and (3) the International Atomic Energy List. Members include the countries of the North Atlantic Treaty Organization, except Iceland, with the addition of Japan and Australia.

Cryptography

The transformation of ordinary text, or "plain text," into coded form by encryption and the transformation of coded text into plain text by decryption. Cryptography can be used to support digital signature, key management or exchange, and communications privacy.

Data Encryption Standard (DES)

A NIST Federal Information Processing Standard and a commonly used secret-key cryptographic algorithm for encrypting and decrypting data and performing other functions. For example, DES can be used to check message integrity. DES specifies a key length of 56 bits.

Digital Signature

A cryptographic method, provided by public-key cryptography, used by a message's recipient or any third party to verify the identity of the message's sender and the integrity of the message. A sender creates a digital signature or a message by transforming the message with his/her private key. A recipient, using the sender's public key, verifies the digital signature by applying a corresponding transformation to the message and the signature.

Digital Signature Standard (DSS)

A NIST-proposed Federal Information Processing Standard that supports digital signature.

Digital Telephony

Telephone systems that use digital communications technology.

Economic Espionage

The unauthorized acquisition of U.S. proprietary or other information by a foreign government to advance the economic position of that country.

Encryption

The process of making information indecipherable to protect it from unauthorized viewing or use, especially during transmission or storage. Encryption is based on an algorithm and at least one key. Even if the algorithm is known, the information cannot be decrypted without the key(s).

Information-Processing Standard

A set of detailed technical guidelines used to establish uniformity to support specific functions and/or interoperability in hardware, software, or telecommunications development, testing, and/or operation.

Integrated Services Digital Network

An emerging communications system enabling the simultaneous transmission of data, facsimile, video, and voice over a single communications link.

Interoperability

The ability of computers to act upon information received from one another.

Key

A long string of seemingly random bits used with cryptographic algorithms to create/verify digital signatures and encrypt/decrypt messages and conversations. The keys must be known or guessed to forge a digital signature or decrypt an encrypted message.

Key-Escrow System

An electronic means of reconstructing a secret key (for secret-key encryption) or a private key (for public-key encryption). The reconstructed key can then be used in a process to decrypt a communication.

Key Management/Exchange

A method of electronically transmitting, in a secure fashion, a secret key for use with a secret-key cryptographic system. Key management can be used to support communications privacy. This method can be accomplished most securely with public-key cryptographic systems, which do not require the sharing of secret keys with third parties. Instead, a secret key is encrypted with a recipient's public key, and the recipient decrypts the result with his/her private key to receive the secret key. A variation of key management that is based on key exchange does not require encrypting the secret key.

Mass-Market Software

Software that is (1) generally available to the public by sale, without restriction, from stock at retail selling points through over-the-counter, telephone, and mail transactions and (2) designed for user installation without substantial supplier support.

Personal Communications Network

Advanced cellular telephone communications and the interworking of both wired and wireless networks that will offer new communications services via very small, portable handsets. The network will rely on microcellular technology—many low-power, small-coverage cells—and a common channel-signaling technology, such as that used in the telephone system, to provide a wide variety of features in addition to the basic two-way calling service.

Private Key

The undisclosed key in a matched key pair—private key and public key—that each party safeguards for public-key cryptography.

Public Key

The key in a matched key pair—private key and public key—that may be published, e.g., posted in a directory, for public-key cryptography.

Public-Key Cryptography

Cryptography using two matched keys (or asymmetric cryptography) in which a single private key is not shared by a pair of users. Instead, users have their own key pairs. Each key pair consists of a matched private and public key. Public-key cryptography can perform (1) digital signature, (2) secure transmission or exchange of secret keys, and/or (3) encryption and decryption. Examples of public-key cryptography are DSS and RSA.

RC2, RC4 (Rivest Cipher 2 and Rivest Cipher 4)

Two secret-key encryption systems that are implemented in mass-market software. These systems are proprietary and are marketed by RSA Data Security, Inc. RC2 and RC4 can be used with various key lengths, such as 40 bits or 56 bits.

RSA

A public-key algorithm invented by Ronald L. Rivest, Adi Shamir, and Leonard M. Adleman. RSA can be used to generate digital signatures; encrypt messages; and provide key management for DES, RC2, RC4, and other secret-key algorithms. RSA performs the key-management process, in part, by encrypting a secret key for an algorithm such as DES, RC2, or RC4 with the recipient's public key for secure transmission to the recipient. This secret key can then be used to support private communications.

Secret Key

The key that two parties share and keep secret for secret-key cryptography. Given secret-key algorithms of equal strength, the approximate difficulty of decrypting encrypted messages by brute force search can be measured by the number of possible keys. For example, a key length of 56 bits is over 65,000 times stronger or more resistant to attack than a key length of 40 bits.

Secret-Key Cryptography

Cryptography based on a single key (or symmetric cryptography). It uses the same secret key for encryption and decryption. Messages are encrypted using a secret key and a secret-key cryptographic algorithm, such as Skipjack, DES, RC2, and RC4.

Skipjack

A classified 64-bit block encryption, or secret-key encryption, algorithm. The algorithm uses 80-bit keys (compared with 56 for DES) and has 32 computational rounds or iterations (compared with 16 for DES). Skipjack supports all DES modes of operation. Skipjack provides high-speed encryption when implemented in a Clipper Chip (initial name).

Trapdoor

A secret entry point to a cryptographic algorithm through which the developer or another entity can bypass security controls and decrypt messages.

Wiretapping

The real-time collection of transmitted data, such as dialed digits, and the sending of that data in real time to a listening device. ("Real time" is defined as the actual time that something, such as the communication of information, takes place.)

Ordering Information

The first copy of each GAO report and testimony is free. Additional copies are $2 each. Orders should be sent to the following address, accompanied by a check or money order made out to the Superintendent of Documents, when necessary. Orders for 100 or more copies to be mailed to a single address are discounted 25 percent.

Orders by mail:

U.S. General Accounting Office
P.O. Box 6015
Gaithersburg, MD 20884-6015

or visit:

Room 1000
700 4th St. NW (corner of 4th and G Sts. NW)
U.S. General Accounting Office
Washington, DC

Orders may also be placed by calling (202) 512-6000
or by using fax number (301) 258-4066.

PRINTED ON ♻ RECYCLED PAPER