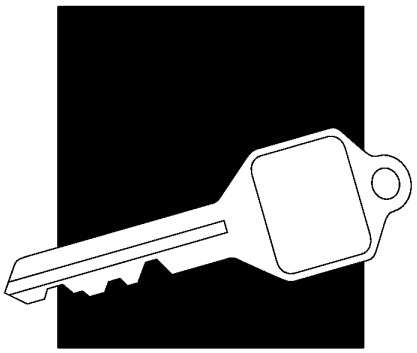
Overview of the 1994 OTA Report on Information Security and Privacy

2

This chapter highlights the importance of information security and privacy issues, explains why cryptography policies are so important, and reviews policy findings and options from the September 1994 OTA report *Information Security and Privacy in Network Environments*. Chapter 3 reviews the December 1994 OTA workshop and identifies key points that emerged from the workshop discussion, particularly export controls and the international business environment, federal cryptography policy, and information-security "best practices." Chapter 4 presents implications for congressional action, in light of recent and ongoing events.

This background paper is a companion and supplement to the September 1994 OTA report and is intended to be used in conjunction with that report. For the reader's convenience, however, pertinent technical and institutional background material, drawn from the September 1994 report and updated where appropriate, is included in appendices B ("Federal Information Security and the Computer Security Act"), C ("U.S. Export Controls on Cryptography"), and D ("Summary of Issues and Options from the 1994 OTA Report").



INFORMATION SECURITY AND PRIVACY IN A NETWORKED SOCIETY

Information technologies are transforming the ways in which we create, gather, process, and share information. Rapid growth in computer networking is driving many of these changes; electronic transactions and electronic records are becoming central to everything from business to health care. Government connectivity is also growing rapidly in scope and importance. Within the feder-

al government, effective use of information technologies and networks is central to government restructuring and reform.[1]

The transformation being brought about by networking brings with it new concerns for the security of networked information and for our ability to maintain effective privacy protections in networked environments.[2] Unless these concerns can be resolved, they threaten to limit networking's full potential in terms of both participation and usefulness. Therefore, information safeguards (countermeasures) are achieving new prominence.[3] Appropriate safeguards for the networked environment must account for—and anticipate—technical, institutional, and social changes that increasingly shift responsibility for security to the end users.

Computing power used to be isolated in large mainframe computers located in special facilities; computer system administration was centralized and carried out by specialists. In today's networked environment, computing power is decentralized to diverse users who operate desktop computers and who may have access to computing power and data at remote locations. Distributed computing and open systems can make every user essentially an "insider." In such a decentralized environment, responsibility for safeguarding information is distributed to the users, rather than remaining the purview of system specialists. The increase in the number and variety of network service providers also requires that users take responsibility for safeguarding information, rather than relying on intermediaries to provide adequate protection.[4]

The new focus is on safeguarding the *information* itself as it is processed, stored, and transmitted. This contrasts with older, more static or insulated concepts of "document" security or "computer" security. In the networked environment, we need appropriate rules for handling proprietary, copyrighted, and personal information—and tools with which to implement them.[5] Increased interactivity means that we must also deal with transactional privacy, as well as prevent fraud in electronic commerce and ensure that safeguards are integrated as organizations streamline their operations and modernize their information systems.

REVIEW OF THE 1994 OTA REPORT

In September 1994, the Office of Technology Assessment released the report *Information Security*

---

[1] See U.S. Congress, Office of Technology Assessment, *Making Government Work: Electronic Delivery of Government Services*, OTA-TCT-578 (Washington, DC: U.S. Government Printing Office, September 1993). See also Elena Varon, "Senate Panel Takes up IT Management Issues," *Federal Computer Week*, Feb. 6, 1995, p. 6; and Charles A. Bowsher, Comptroller General of the United States, "Government Reform: Using Reengineering and Technology To Improve Government Performance," GAO/T-OCG-95-2, testimony presented before the Committee on Governmental Affairs, U.S. Senate, Feb. 2, 1995.

[2] For example, measures to streamline operations via information technology require careful attention both to technical safeguards and to related institutional measures, such as employee training and awareness. Similarly, computer networks allow more interactivity, but the resulting transactional data may require additional safeguards to protect personal privacy.

[3] See Michael Neubarth et al., "Internet Security (Special Section)," *Internet World*, February 1995, pp. 31-72. See also Russell Mitchell, "The Key to Safe Business on the Net," and Amy Cortese et al., "Warding Off the Cyberspace Invaders," *Business Week*, Mar. 13, 1995, pp. 86, 92-93.

[4] The trend is toward decentralized, distributed computing, rather than centralized, mainframe computing. Distributed computing is relatively informal and "bottom up," compared with mainframe computing, and systems administration may be less rigorous. See U.S. Congress, Office of Technology Assessment, *Information Security and Privacy in Network Environments*, OTA-TCT-606 (Washington, DC: U.S. Government Printing Office, September 1994), pp. 3-5, 25-32. Available from OTA Online via anonymous file transfer protocol (ftp://otabbs.ota.gov/pub/information.security/) or World Wide Web (http://www.ota.gov).

[5] See ibid., chapter 3. "Security" technologies like encryption can be used to help protect privacy and the confidentiality of proprietary information; some, like digital signatures, could be used to facilitate copyright-management systems.

and Privacy in Network Environments.[6] The report was prepared in response to a request by the Senate Committee on Governmental Affairs and the House Subcommittee on Telecommunications and Finance that OTA study the changing needs for protecting unclassified information and for protecting the privacy of individuals.[7] The request for the study was motivated by the rapid increase in connectivity within and outside government and the growth in federal support for large-scale networks. The report focused on safeguarding *information* in networks, not on the security or survivability of the networks themselves, nor on the reliability of network services to ensure information access.

The report identified policy issues and options in three areas: 1) cryptography policy, including federal information processing standards and export controls; 2) guidance on safeguarding unclassified information in federal agencies; and 3) legal issues and information security, including electronic commerce, privacy, and intellectual property. The report concluded that Congress has a vital role in formulating national cryptography policy and in determining how we safeguard information and protect personal privacy in an increasingly networked society (see outline of policy issues and options in the last section of this chapter and the expanded discussion in appendix D).

Importance of Cryptography

Cryptography (see box 2-1) and related federal policies (e.g., regarding export controls and standards development) were a major focus of the report.[8] That focus was due in part from the widespread attention being given the so-called Clipper chip and the Clinton Administration's *escrowed-encryption* initiative. Escrowed encryption, or *key-escrow encryption,* refers to a cryptosystem in which the functional equivalent of a "spare key" must be deposited with a third party, in order to ensure easy access to decryption keys pursuant to lawful electronic surveillance. The Clinton Administration's escrowed-encryption initiative, first announced in 1993, required the "spare keys" to be held within the executive branch. The Escrowed Encryption Standard (EES), promulgated as a federal information processing standard (FIPS) in 1994, is approved for use in encrypting unclassified voice, fax, or data communicated in a telephone system.[9]

However, a focus on cryptography was inevitable, because in its modern setting, cryptography has become a fundamental technology with broad applications. Modern, computer-based cryptography and cryptanalysis began in the World War II era.[10] Much of this development has been shrouded in secrecy; in the United States, governmental cryptographic research has historically been the purview of the "national security" (i.e., defense and intelligence) communities.[11]

Now, however, cryptography is a technology whose time has come—in the marketplace and in society. Cryptography is not arcane anymore. Despite two decades of growth in nongovernmental research and development, in the United States,

---

[6] Ibid.

[7] Ibid., pp. 5-6 and appendix A (congressional letters of request).

[8] Ibid., pp. 8-18 and chapter 4.

[9] The EES is implemented in hardware containing the Clipper chip. The EES (FIPS-185) specifies use of a classified, symmetric encryption algorithm, called "Skipjack," which was developed by the National Security Agency. The "Capstone chip" implements the Skipjack algorithm for use in computer network applications. The Defense Department's "FORTEZZA card" (a PCMCIA card formerly called "TESSERA") contains the Capstone chip.

[10] See, e.g., David Kahn, *The Codebreakers* (New York, NY: MacMillan, 1967).

[11] Although there has always been some level of nongovernmental cryptography research in the United States, from the end of WWII through the mid-1970s the federal government was almost the sole U.S. source of technology and know-how for modern cryptographic safeguards. The government's former near-monopoly in development and use of cryptography has been eroding, however.

BOX 2-1: Cryptograph

During the long history of paper-based "information systems" for commerce and communication, a number of safeguards were developed to ensure the confidentiality, integrity, and authenticity of documents and messages. These traditional safeguards included secret codebooks and passwords, physical "seals" to authenticate signatures, and auditable bookkeeping procedures. Mathematical analogues of these safeguards are implemented in the electronic environment. The most powerful of these are based on cryptography.

The recorded history of cryptography is more than 4,000 years old, Manual encryption methods using codebooks, letter and number substitutions, and transpositions have been used for hundreds of years—for example, the Library of Congress has letters from Thomas Jefferson to James Madison containing encrypted passages. Modern, computer-based cryptography and cryptanalysts began in the World War II era, with the successful Allied computational efforts to break the ciphers generated by the German Enigma machines, and with the British Colossus computing machines used to analyze a crucial cipher used in the most sensitive German teletype messages.

In the post-WWll era, the premiere locus of U.S. cryptographic research and (especially) research in cryptanalysts has been the Defense Department's National Security Agency (NSA). NSA's preeminent position results from its extensive role in U.S. signals intelligence and in securing classified communications, and the resulting need to understand cryptography as a tool to protect information and as a tool used by adversaries.

In its modern setting, cryptography is a field of applied mathematics/computer science. Cryptographic algorithms—specific techniques for transforming the original input into a form that is unintelligible without special knowledge of some secret (closely held) information—are used to encrypt and decrypt messages, data, or other text. The encrypted text is often referred to as *ciphertext;* the original or decrypted text is often referred to as *plaintext* or *cleartext.* In modern cryptography, the secret information is the cryptographic key that "unlocks" the ciphertext and reveals the plaintext.

The encryption algorithms and key or keys are implemented in a *cryptosystem.* The key used to decrypt can be the same as the one used to encrypt the original plaintext, or the encryption and decryption keys can be different (but mathematically related), One key is used for both encryption and decryption in *symmetric, or* "conventional" cryptosystems; in *asymmetric,* or "public-key" cryptosystems, the encryption

the federal government still does have the most expertise in cryptography. Nevertheless, cryptography is not just a "government" technology anymore, either. Because it is a technology of broad application, the effects of federal policies about cryptography are not limited to technological developments in the field, or even to the health and vitality of companies that produce or use products incorporating cryptography. Instead, these policies will increasingly affect the everyday lives of most Americans.

Encryption (see box 2-2) transforms a message or data files (called "plaintext") into a form (called "ciphertext") that is unintelligible without special knowledge of some secret information (called the "decryption key"). Figures 2-1 and 2-2 illustrate two common forms of encryption: 1) secret-key, or symmetric, encryption and 2) public-key, or asymmetric, encryption. Note that key management—the generation of encryption and decryption keys, as well as their storage, distribution, cataloging, and eventual destruction-is crucial for the overall security of any encryption system. In some cases (e.g., for archival records), when files or databases are encrypted, the keys have to remain cataloged and stored for very long periods of time.

Encryption can be used as a tool to protect the confidentiality of information in messages or files-hence, to help protect personal privacy. Other applications of cryptography can be used to protect the *integrity* of information (that it has not

BOX 2-1 (cont'd.): Cryptography

and decryption keys are different and one of them can be made public. With the advent of "public-key" techniques, cryptography also came into use for *digital signatures* that are of widespread interest as a means for electronically authenticating and signing commercial transactions like purchase orders, tax returns, and funds transfers, as well as ensuring that unauthorized changes or errors are detected.

Cryptanalysis is the study and development of various "codebreaking" methods to deduce the contents of the original plaintext message. The strength of an encryption algorithm is a function of the number of steps, storage, and time required to break the cipher and read any encrypted message, without prior knowledge of the key. Mathematical advances, advances in cryptanalysts, and advances in computing, all can reduce the security afforded by a cryptosystem that was previously considered "unbreakable" in practice.

The strength of a modern encryption scheme is determined by the algorithm itself and the length of the key, For a given algorithm, strength increases with key size. *However,* key size *alone is a not a valid means of comparing the strength of two different encryption systems.* Differences in the properties of the algorithms may mean that a system using a shorter key is stronger overall than one using a longer key.

Key *management* is fundamental and crucial to the security afforded by any cryptography-based safeguard. Key management includes generation of the encryption key or keys, as well as their storage, distribution, cataloging, and eventual destruction. If secret keys are not closely held, the result is the same as if a physical key is left "lying around" to be stolen or duplicated without the owner's knowledge. Similarly, poorly chosen keys may offer no more security than a lock that can be opened with a hairpin. Changing keys frequently can limit the amount of information or the number of transactions compromised due to unauthorized access to a given key. Thus, a well-thought-out and secure key-management infrastructure is necessary for effective use of encryption-based safeguards in network environments. Such a support infrastructure might include means for issuing keys and/or means for registering users' public keys and linking owner-registration certificates to keys so that the authenticity of digital signatures can be verified. This might be done by a *certificate authority* as part of a *public-key infrastructure.*

SOURCE: Office of Technology Assessment, 1995; drawing from OTA, *Information Security and Privacy in Network Environments* (OTA-TCT-606, September 1994), pp. 112-113 and sources cited therein.

been subject to unauthorized or unexpected changes) and to *authenticate* its origin (that it comes from the stated source or origin and is not a forgery).

Thus, cryptography is a technology that will help speed the way to electronic commerce. With the advent of what are called *public-key* techniques, cryptography came into use for *digital signatures (see* figure 2-3) that are of widespread interest as a means for electronically authenticating and signing commercial transactions like purchase orders, tax returns, and funds transfers, as well as for ensuring that unauthorized changes or errors are detected (see discussion of message authentication and digital signatures in box 2-2).[12] These functions are critical for electronic commerce. Cryptographic techniques like digital signatures can also be used to help manage copyrighted material in electronic form. 13

[12]OTA, op. cit., footnote 4, pp. 69-77. See also Lisa Morgan, "Cashing In: The Rush Is on To Make Net Commerce Happen," *Internet World,* February 1995, pp. 48-51; and Richard W. Wiggirts, "Business Browser: A Tool To Make Web Commerce Secure," *Internet World,* February 1995, pp. 52-55.

[13] OTA, ibid., pp. 96- 110. For example, digital signatures can be used to create compact "copyright tokens" for use in registries; encryption could be used to create personalized "copyright envelopes" for direct electronic delivery of material to customers. See also Working Group on Intellectual Property Rights, IITF, "Intellectual Property and the National Information Infrastructure (Green Paper)," July 1994, pp. 139-140.

BOX 2-2: Encryption, Authentication, and Digital Signatures

Different cryptographic methods are used to authenticate users, protect confidentiality, and assure integrity of messages and files. Most systems use a combination of techniques to fulfill these functions.

Encryption

Cryptographic algorithms are either *symmetric* or *asymmetric,* depending on whether or not the same cryptographic key is used for encryption and decryption. The key is a sequence of symbols that determines the transformation from unencrypted *plaintext* to encrypted *ciphertext,* and vice versa.

"Symmetric" cryptosystems---also called secret-key or single-key systems—use the same key to encrypt and decrypt messages. Both the sending and receiving parties must know the secret key that they will use to communicate (see figure 2-1 in the main text). Secret-key algorithms can encrypt and decrypt relatively quickly, but systems that use only secret keys can be difficult to manage because they require a courier, registered mail, or other secure means for distributing keys. The federal Data Encryption Standard (DES) and the new Escrowed Encryption Standard (EES) each use a different secret-key algorithm.

"Asymmetric" cryptosystems---also called public-key systems—use one key to encrypt and a different, but mathematically related, public key to decrypt messages (see figure 2-2). For example, if an associate sends Carol a message encrypted with Carol's public key, in principle only Carol can decrypt it, because she is the only one with the correct private key This provides confidentiality and can be used to distribute secret keys, which can then be used to encrypt messages using a faster, symmetric cryptosystem (see figure 2-3).

The security of public-key systems rests on the authenticity of the public key (that it is a valid key for the stated individual or organization, not "recalled" by the owner or presented by an impostor) and the secrecy of the private key, much as the security of symmetric ciphers rests on the secrecy of the single key. Although the public key can be freely distributed, or posted in the equivalent of a telephone directory, its authenticity must be assured (e.g., by a certificate authority as part of a public-key infrastructure).

Commonly used public-key systems encrypt relatively slowly, but are useful for digital signatures and for exchanging the session keys that are used for encryption with a faster, symmetric cryptosystem. The Rivest-Shamir-Adleman (RSA) algorithm is a well-known, commercial public-key algorithm.

Authentication

The oldest and simplest forms of message authentication use "secret" authentication parameters known only to the sender and intended recipient to generate "message authentication codes. " So long as the secret authentication parameter is kept secret from all other parties, these techniques protect the sender and the receiver from alteration or forgery of a message by all such third parties. Because the same secret information is used by the sender to generate the message authentication code and by the receiver to validate it, these techniques cannot settle "disputes" between the sender and receiver as to what message, if any, was sent. For example, message authentication codes could not settle a dispute between a stockbroker and client in which the broker claims the client issued an order to purchase stock and the client claims he never did so.

For authentication, if a hypothetical user (Carol) uses her private key to sign messages, her associates can verify her signature using her public key. This method authenticates the sender, and can be used with hashing functions (see below) for a *digital signature* that can also check the integrity of the message.

Digital Signatures

Digital signatures provide a higher degree of authentication by allowing resolution of disputes. Although it is possible to generate digital signatures from a symmetric cipher like the DES, most interest centers on signature systems based on public-key cryptosystems.

BOX 2-2 (cont'd.): Encryption, Authentication, and Digital Signatures

In principle, to sign a message using a public-key encryption system, a user could transform it with his private key, and send both the original message and the transformed version to the intended receiver. The receiver would validate the message by acting on the transformed message with the sender's public key (obtained from the "electronic phone book") and seeing that the result matched the original message. Because the signing operation depends on the sender's private key (known only to him or her), it is impossible for anyone else to sign messages in the sender's name. But everyone can validate such signed messages, since the validation depends only on the sender's "public" key.

In practice, digital signatures sign shorter "message digests" rather than the whole messages. In most public-key signature techniques, a one-way hash function is used to produce a condensed version of the message, which is then "signed. " For example, Carol processes her message with a '(hashing algorithm" that produces a shorter *message* digest—the equivalent of a very long checksum. Because the hashing method is a "one-way" function, the message digest cannot be reversed to obtain the message. Bob also processes the received text with the hashing algorithm and compares the resulting message digest with the one Carol signed and sent along with the message. If the message was altered in any way during transit, the digests will be different, revealing the alteration (see figure 2-4).

Signature Alternatives

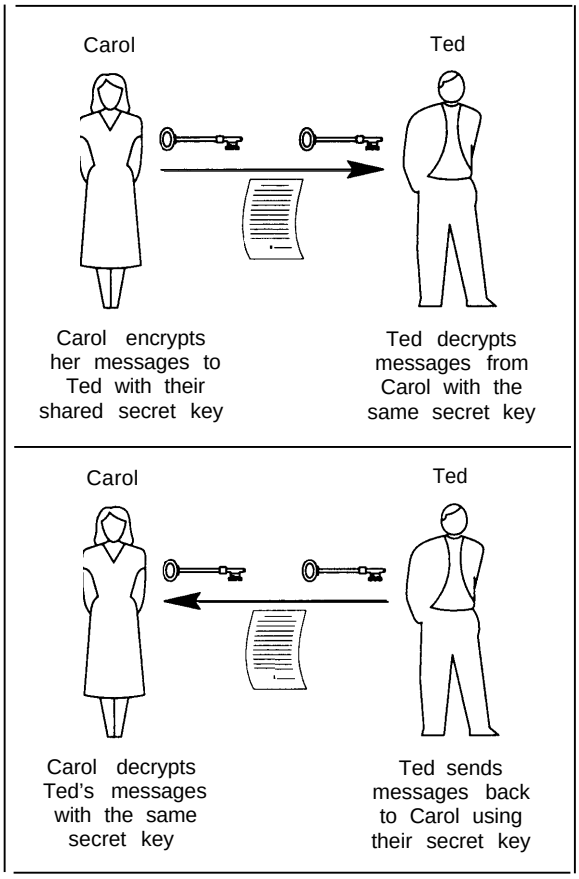
With the commercial RSA system, the signature is created by encrypting the message digest, using the sender's private key. Because in the RSA system each key is the inverse of the other, the recipient can use the sender's public key to decrypt the signature, thereby recovering the original message digest. The recipient compares this with the one he or she has calculated using the same hashing function—if they are identical, then the message has been received exactly as sent and, furthermore, the message did come from the supposed sender (otherwise his or her public key would not have yielded the correct message digest).

The federal Digital Signature Standard (DSS) defines a somewhat different kind of public-key cryptographic standard for generating and verifying digital signatures. The DSS is to be used in conjunction with a federal hashing standard that is used to create a message digest, as described above. The message digest is then used, in conjunction with the sender's private key and the algorithm specified in the DSS, to produce a message-specific signature. Verifying the DSS signature involves a mathematical operation on the signature and message digest, using the sender's public key and the hash standard.

The DSS differs from the RSA digital signature method in that the DSS signature operation is not reversible, and hence can only be used for generating digital signatures. DSS signature verification is different than decryption. In contrast, the RSA system can encrypt, as well as do signatures. Therefore, the RSA system can also be used to securely exchange cryptographic keys that are to be used for confidentiality (e.g., "secret" keys for use with a symmetric encryption algorithm like the DES). This lack of encryption capability for secure key exchange was one reason why the government selected the DSS technique for the standard.

SOURCE: Office of Technology Assessment, 1995; drawing from OTA, *Information Security and Privacy in* Network Environments (OTA-TCT-606, September 1994), pp. 39 and 124-125 and sources cited therein See also U.S. Department of Commerce, National Institute of Standards and Technology, "Data Encryption Standard (DES), " FIPS Publication 46-2, Dec 30, 1993; "Digital Signature Standard (DSS)," FIPS Publication 186, May 19, 1994; and "Escrowed Encryption Standard (EES), " FIPS Publication 185, February 1994.

FIGURE 2-1: Secret-Key (Symmetric) Encryption



NOTE: Security depends on the secrecy of the shared key.

SOURCE: Office of Technology Assessment, 1994.

The nongovernmental markets for cryptography-based safeguards have grown over the past two decades, but are still developing. Good commercial encryption technology is available in the United States and abroad. Research in cryptography is international. Absent government regulations, markets for cryptography would also be international. However, export controls create "domestic" and "export" markets for strong encryption products (see section on export controls below and also appendix C.[14] User-friendly cryptographic safeguards that are integrated into products (as opposed to those that the user has to acquire separately and add on) are still hard to come by—in part, because of export controls and other federal policies that seek to control cryptography.[15]

Government Efforts To Control Cryptography

In its activities as a developer, user, and regulator of safeguard technologies, the federal government faces a fundamental tension between two policy objectives, each of which is important: 1) fostering the development and widespread use of cost-effective information safeguards, and 2) controlling the proliferation of safeguard technologies that can impair U.S. signals-intelligence and law enforcement capabilities. Cryptography is at the heart of this tension. Export controls and the federal standards process (i.e., the development and promulgation of federal information processing standards, or FIPS) are two mechanisms the government can use to control cryptography.[16]

Policy debate over cryptography used to be as arcane as the technology itself. Even five or 10 years ago, few people saw a link between government decisions about cryptography and their daily lives. However, as the information and communications technologies used in daily life have changed, concern over the implications of policies traditionally dominated by national security objectives has grown dramatically.

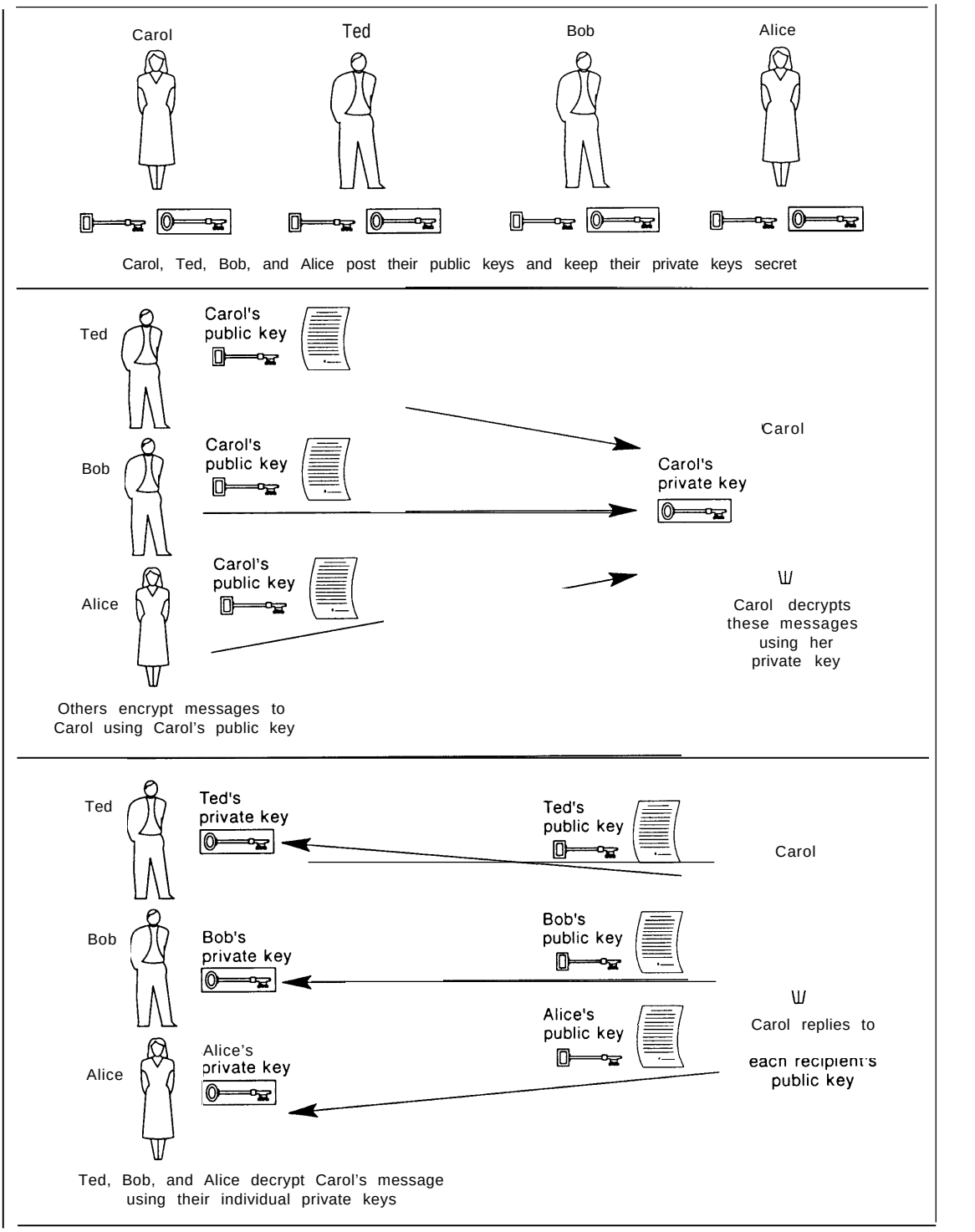
Previously, control of the availability and use of cryptography was presented as a national security issue focused outward, with the intention of maintaining a U.S. technological lead over other countries and preventing encryption devices from

[14] OTA, ibid., pp. 11-13, 150-160.

[15] Ibid., pp. 115-123, 128-132, 154-160.

[16] For more detail, see ibid., chapters 1 and 4, and appendix C. Other means of control have historically included include national security classification and patent-secrecy orders (see ibid., p. 128 and footnote 33).

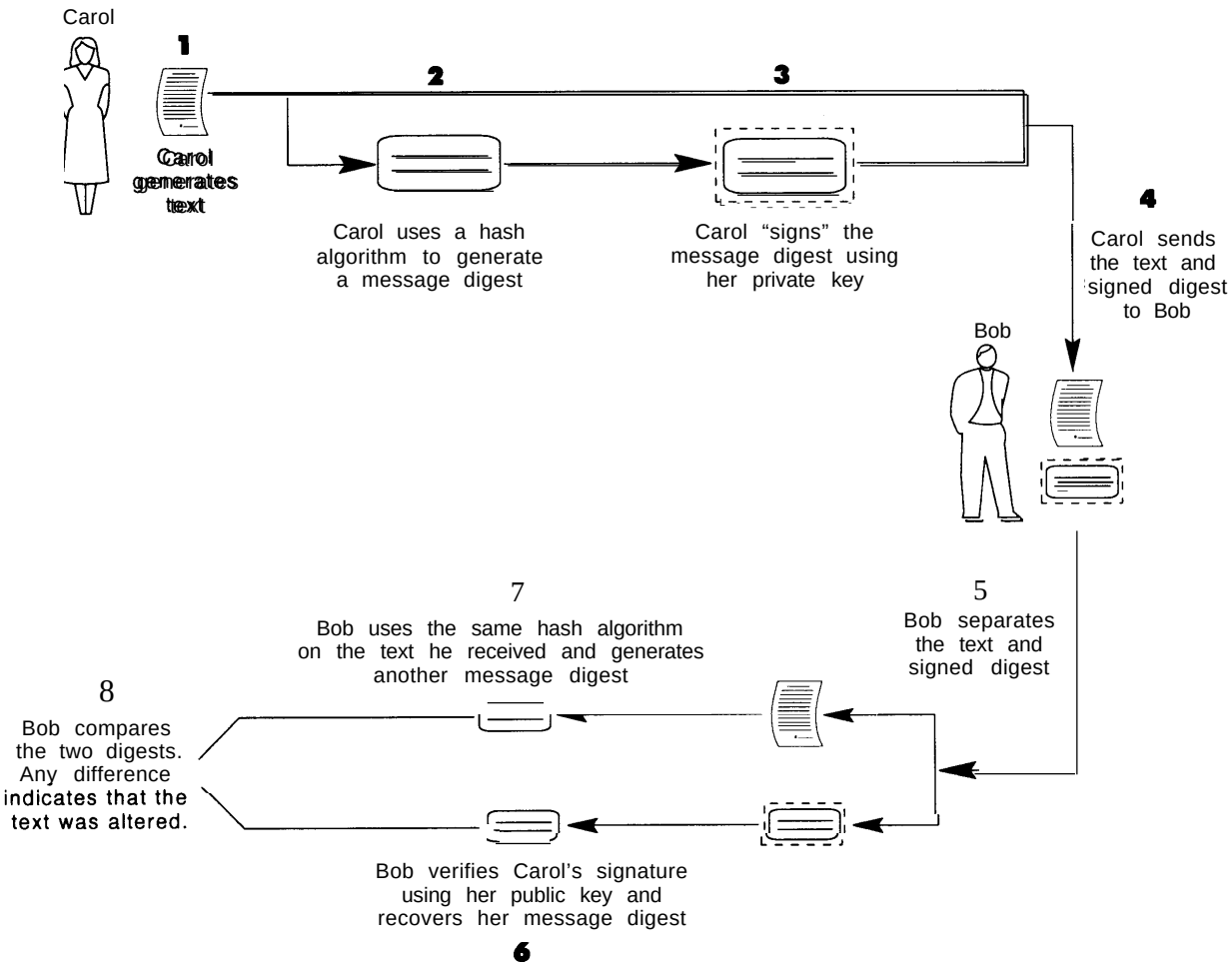
FIGURE 2-2: Public-Key (Asymmetric) Encryption



NOTE: Security depends on the secrecy of the private keys and the authenticity of the public keys.

SOURCE: Office of Technology Assessment, 1994

FIGURE 2-3: Example of a Hashing and Digital Signature Scheme



NOTE: Different methods for generating and verifying signatures (as in the federal Digital Signature Standard) are possible. Measures to protect the signature and text may also be used.

SOURCE: Office of Technology Assessment, 1994

falling into the "wrong hands" overseas. More widespread foreign use—including use of strong encryption by terrorists and developing countries—makes U.S. signals intelligence more difficult.

Now, with an increasing policy focus on domestic crime and terrorism, the availability and use of cryptography has also come into prominence as a domestic-security, law enforcement issue. Within the United States, strong encryption is increasingly portrayed as a threat to domestic security (public safety) and a barrier to law enforcement if it is readily available for use by terrorists or criminals. There is also growing recognition of potentials for misuse, such as by disgruntled employees as a means to sabotage an employer's databases. Thus, export controls, intended to restrict the international availability of U.S. cryptography technology and products, are now being joined with domestic cryptography initiatives, like key-es-

crow encryption, that are intended to preserve U.S. law enforcement and signals-intelligence capabilities (see box 2-3).

Standards-development and export-control issues underlie a long history of concern over leadership and responsibility (i.e., *"who should be in charge?"* and *"who is in charge?"*) for the security of unclassified information government-wide.[17] Most recently, these concerns have been revitalized by proposals (presented by the Clinton Administration's Security Policy Board staff) to centralize information-security authorities government-wide under joint control of the Office of Management and Budget (OMB) and Department of Defense (DOD) (see discussion in chapter 4).[18]

Other manifestations of these concerns can be found in the history of the Computer Security Act of 1987 (Public Law 100-235—see the next section and appendix B) and in more recent developments, such as public reactions to the Clinton Administration's key-escrow encryption initiative and the controversial issuances of the Escrowed Encryption Standard[19] and Digital Signature Standard (DSS)[20] as federal information processing standards. Another important manifestation of these concerns is the controversy over the present U.S. export control regime, which includes commercial products with capabilities for strong encryption, including mass-market software, on the Munitions List, under State Department controls (see below and appendix C).

The Escrowed Encryption Standard has been promulgated by the Clinton Administration as a voluntary federal encryption standard (i.e., a voluntary, rather than mandatory, FIPS). The EES announcement noted that the standard does not mandate the use of escrowed-encryption devices by government agencies or the private sector; the standard provides a mechanism for agencies to use key-escrow encryption without having to waive the requirements of another, extant federal encryption standard for unclassified information, the Data Encryption Standard (DES).[21]

The EES is intended for use in encrypting unclassified voice, facsimile, and computer information communicated over a telephone system. The encryption algorithm (called Skipjack) specified in the EES can also be implemented for data communications in computer networks. At this writing, there is no FIPS specifying use of Skipjack as a standard algorithm for data communications or file encryption.

However, DOD is using Skipjack for encryption in computer networks (e.g., in the "FORTEZZA" PCMCIA card). As of April 1995, according to the National Security Agency (NSA), approximately 3,000 FORTEZZA cards have been produced and another 33,000 are on contract; some 100 to 200 are being tested and used in applications development by various DOD organizations, mostly in support of the Defense Message System.[22] According to the NSA, plans call for

---

[17] Ibid., pp. 8-20 and chapter 4.

[18] U.S. Security Policy Board Staff, "Creating a New Order in U.S. Security Policy," Nov. 21, 1994, pp. II-III, 14-18.

[19] See box 2-3 and OTA, op. cit., footnote 4, ch. 4.

[20] See box 2-2 and OTA, ibid., appendix C.

[21] See *Federal Register*, vol. 59, Feb. 9, 1994, pp. 5997-6005 ("Approval of Federal Information Processing Standards Publication 185, Escrowed Encryption Standard (EES)"), especially p. 5998. Note, however, that the DES is approved for encryption of unclassified data communications and files, while the EES is only a standard for telephone communications at this time.

[22] Bob Drake, Legislative Affairs Office, NSA, personal communication, Apr. 7, 1995.

BOX 2-3: The Escrowed Encryption Standard

The federal Escrowed Encryption Standard (EES) was approved by the Commerce Department as a federal information processing standard (FIPS) in February 1994.[1] According to the standard (described in FIPS PUB 185), the EES is intended for voluntary use by all federal departments and agencies and their contractors to protect unclassified information. Implementations of the EES are subject to State Department export controls. In 1994, however, the Clinton Administration indicated that encryption products based on the EES would be exportable to most end users and that EES products will qualify for special licensing arrangements.[2]

The National Security Council, Justice Department, Commerce Department, and other federal agencies were involved in the decision to propose the EES, according to a White House press release and information packet dated April 16, 1993, the day the EES initiative was announced. The EES algorithm is said to be stronger than the Data Encryption Standard (DES) algorithm, but able to meet the legitimate needs of law enforcement agencies to protect against terrorists, drug dealers, and organized crime.[3]

EES Functions

The EES is intended to encrypt voice, fax, and computer data communicated in a telephone system. It may, on a voluntary basis, be used to replace DES encryption devices now in use by federal agencies and contractors. Other use by the private sector is voluntary. The EES specifies a symmetric encryption algorithm, called "Skip jack." The Skipjack algorithm is a classified algorithm, developed by the National Security Agency (NSA) in the 1980s.[4] An early implementation was called Clipper, hence the colloquial use of Clipper or Clipper Chip to describe the EES technology.[5]

The EES also specifies a method to create a Law Enforcement Access Field (LEAF), in order to provide for easy decryption when the equivalent of a wiretap has been authorized.[6] The Skipjack algorithm and LEAF creation method are implemented only in electronic devices (i.e., very-large-scale integration chips). The chips are "highly resistant" to reverse engineering and will be embedded in tamper-resistant cryptographic modules that approved manufacturers can incorporate in telecommunications or computer equipment. The chips are manufactured by VLSI Logic and are programmed with the algorithms and keys by Mykotronx. The programming is done under the supervision of the two "escrow agents" (see below).

---

[1] See Federal Register, vol. 59, Feb. 9, 1994, pp. 5997-6005.

[2] Martha Harris, Deputy Assistant Secretary of State for Political-Milltary Affairs, "Statement on Encryption-Export Control Reform, " Feb. 4, 1994 *[OTA note The anticipated reforms had not all materialized as of this writing.]*

[3] Because the EES algorithm IS classified, the overall strength of the EES cannot be examined except under security clearance (see below). Thus, unclassified, public analyses of its strengths and weaknesses are not possible. The only public statements made by the Clinton Administration concerning the strength of the EES relative to the DES refer to the secret-key size: 80 bits for the EES versus 56 bits for the DES

[4] The NSA specifications for Skipjack and the LEAF creation method are classified at the Secret level. (OTA project staff did not access these, or any other classified information.)

[5] The Clipper Chip implementation of Skipjack is for use in secure telephone communications. An enhanced escrowed-encryption chip with additional functions, called Capstone, is used in data communications. Capstone is in the FORTEZZA PCMCIA card being used in the Defense Message System

[6] See Jo Ann Harris, Assistant Attorney General, Criminal Division, Department of Justice, testimony before the Subcommittee on Technology and the Law, Committee on the Judiciary, U.S. Senate, May 3, 1994; and James K. Kallstrom, Special Agent in Charge, Special Operations Division, Federal Bureau of Investigation, testimony before the Subcommittee on Technology, Environment, and Aviation, Committee on Science, Space, and Technology, U.S. House of Representatives, May 3, 1994 For a discussion of law enforcement concerns and the rationale for government key escrowing, see also Dorothy E. Denning, "The Clipper Encryption System, " *American Scientist, vol. 81,* July-August 1993, pp. 319-322; and "Encryption and Law Enforcement, " Feb. 21, 1994, available from denning@cs.georgetown.edu

BOX 2-3 (cont'd.): The Escrowed Encryption Standard

After electronic surveillance has been authorized, the EES facilitates law enforcement access to encrypted communications. This is accomplished through what is called a "key escrowing" scheme. Each EES chip has a chip-specific key that is split into two parts after being programmed into the chips. These parts can be recombined to gain access to encrypted communications. One part is held by each of two designated government keyholders, or "escrow agents." Attorney General Reno designated the National Institute of Standards and Technology (NIST) and the Treasury Department's Automated Systems Division as the original escrow agents. The only public estimate (by NIST, in early 1994) of the costs of establishing the escrow system was about $14 million, with estimated annual operating costs of$16 million.

When surveillance has been authorized and the intercepted communications are found to be encrypted using the EES, law enforcement agencies can obtain the two parts of the escrowed key from the escrow agents. These parts can then be used to obtain the individual keys used to encrypt (and, thus, to decrypt) the telecommunications sessions of interest.[7] The LEAF is transmitted along with the encrypted message; it contains a device identifier that indicates which escrowed keys are needed.

EES History

The proposed FIPS was announced in the Federal Register on July 30, 1993, and was also sent to federal agencies for review. The EES was promulgated after a comment period that generated almost universally negative comments. According to NIST, comments were received from 22 government organizations in the United States, 22 industry organizations, and 276 individuals. Concerns and questions reported by NIST include the algorithm itself and lack of public inspection and testing, the role of NSA in promulgating the standard, use of key escrowing, possible infringement of individual rights, effects of the standard on U.S. firms' competitiveness in foreign markets, cost of establishing the escrowing system, and cost-effectiveness of the new standard.[8]

During the review period, the Skipjack algorithm was evaluated by outside experts, pursuant to President Clinton's direction that "respected experts from outside the government will be offered access to the confidential details of the algorithm to assess its capabilities and publicly report their findings. " Five reviewers accepted NIST's invitation to participate in a classified review of Skipjack and publicly report their findings: Ernest Brickell (Sandia National Laboratories), Dorothy Denning (Georgetown University), Stephen Kent (Bolt Beranek and Newman, Inc.), David Maher (AT&T), and Walter Tuchman (Amperif Corp.). Their interim report on the algorithm itself found that: 1) there is no significant risk that Skipjack will be broken by exhaustive search in the next 30 to 40 years; 2) there is no significant risk that Skipjack can be broken through a shortcut method of attack; and 3) while the internal structure of Skipjack must be classified in order to protect law enforcement and national security objectives, the strength of Skipjack against a cryptanalytic attack does not depend on the secrecy of the algorithm.[9]

---

[7] Requirements for federal and state law enforcement agents to certify that electronic surveillance has been authorized, and for what period of time, as well as requirements for authorized use of escrowed key components are explained in Department of Justice, "Authorization Procedures for Release of Encryption Key Components in Conjunction with Intercepts Pursuant to Title Ill, " "Authorization Procedures for Release of Encryption Key Components in Conjunction with Intercepts Pursuant to State Statutes, " and "Authorization Procedures for Release of Encryption Key Components in Conjunction with Intercepts Pursuant to FISA, " Feb. 4, 1994.

[8] *Federal Register* (Feb. 9, 1994), op. cit. footnote 1, pp. 5998-6002.

[9] E. Brickell (Sandia National Laboratories) et al., "SKIPJACK Review Interim Report-The SKIPJACK Algorithm, " July 28, 1993. See also "Fact Sheet—NIST Cryptography Activities," Feb. 4, 1994

(continued)

BOX 2-3 (cont'd.): The Escrowed Encryption Standard

Based on its review of the public comments, NIST recommended that the Secretary of Commerce issue the EES as a federal information processing standard.[10] NIST noted that almost all of the comments received during the review period were negative, but concluded that, "many of these comments reflected misunderstanding or skepticism that the EES would be a *voluntary* standard."[11] The Clinton Administration also carried out a 10-month encryption policy review that presumably played a role in choosing to issue the EES as a FIPS, but the substance of that review has not been made public and was not available to OTA. Additionally, the Clinton Administration created an interagency working group on encryption and telecommunications that includes representatives of agencies that participated in the policy review. The interagency group was to "work with industry on technologies like the Key Escrow chip [i. e., EES], to evaluate possible alternatives to the chip, and to review Administration policies regarding encryption as developments warrant. "[12]

In early 1995, an alternative, commercial key-escrow encryption system being developed by Trusted Information Systems, Inc. (TIS) was undergoing internal government review to determine whether such an approach could meet national security and law enforcement objectives. The TIS key-escrow system does software-based escrowing and encryption using the "triple-DES" version of the Data Encryption Standard.[13] The initial version of the system is designed for use in encrypting files or email, but the TIS approach could also be used for real-time telecommunications.

In January 1995, AT&T Corp. and VLSI Technology, Inc., announced plans to develop chips implementing the RSA algorithm and "triple DES" for encryption. The chips would be used in a personal computers, digital telephones, and video decoder boxes.[14]

[10] Ibid., and *Federal Register (* Feb. 9, 1994), OP. Cit., footnote 1.

[11] Ibid.

[12] White House press release and enclosures, Feb. 4, 1994, "Working Group on Encryption and Telecommunications. "

[13] Stephen T. Walker et al., "Commercial Key Escrow: Something for Everyone Now and For the Future, " TIS Report No. 541, Trusted Information Systems, Inc., Jan. 3, 1995.

[14] Jared Sandberg and Don Clark, "AT&T, VLSI Technology To Develop Microchips That Offer Data Security, *The Wall Street Journal,* Jan. 31, 1995.

SOURCE: Off Ice of Technology Assessment, 1995; drawing from OTA, *Information Security And Privacy in Networked Environments* (OTA-TCT-606, September 1994), pp. 118-119 and sources cited therein and below.

eliciting and aggregating bulk orders for FORTEZZA in order to support the award of a large-scale production contract in the fall, ideally for 200,000 to 400,000 units in order to achieve the target unit price of $100.[23]

The algorithm specified in the EES has not been published. The secret encryption key length for Skipjack is 80 bits; a key-escrowing scheme is built into ensure "lawfully authorized" electronic surveillance.[24] The algorithm is classified and is intended to be implemented only in tamper-resistant, hardware modules.[25] This approach makes the confidentiality function of the Skipjack en-

[23] Ibid. According to the NSA, unit prices for FORTEZZA cards in small quantities are on the order of $150, of which about $98 is for the Capstone chip. The Capstone chip implements the Skipjack algorithm, plus key-exchange and digital-signature (DSS) functions.

[24] *Federal Register,* ibid., p. 6003.

[25] *Federal Register,* ibid., pp. 5997-6005.

cryption algorithm available in a controlled fashion, without disclosing the algorithm's design principles or thereby increasing users' abilities to employ cryptographic principles. One of the reasons stated for specifying a classified, rather than published, encryption algorithm in the EES is to prevent independent implementation of Skipjack without the law enforcement access features.

The federal Data Encryption Standard was first approved in 1976 and was most recently reaffirmed in 1993. The DES specifies an algorithm that can be used to protect unclassified information, as needed, while it is being communicated or stored.[26] The DES algorithm has been made public (i.e., it has been published). When the DES is used, users can generate their own encryption keys; the secret encryption key for DES is 56 bits long. The DES does not require the keys to be "escrowed" or deposited with any third party.

The 1993 reaffirmation of the DES—now in software, as well as hardware and firmware implementations—may be the last time it is reaffirmed as a federal standard. FIPS Publication 46-2 ("Data Encryption Standard") noted that the algorithm will be reviewed within five years to assess its adequacy against potential new threats, including advances in computing and cryptanalysis:

> At its next review (1998) [the DES algorithm] will be over twenty years old. NIST [National Institute of Standards and Technology] will consider alternatives which offer a higher level of security. One of these alternatives may be proposed as a replacement standard at the 1998 review.[27]

Given that the Skipjack algorithm was selected as a standard (the EES) for telephony, it is possible that an implementation of Skipjack (or some other form of key-escrow encryption) will be selected as a FIPS to replace the DES for computer communications and/or file encryption.

An alternative successor to the DES that is favored by nongovernmental users and experts is a variant of DES called *triple-encryption DES*. In "triple DES," the algorithm is used sequentially with three different keys, to encrypt, decrypt, then re-encrypt. Triple encryption with the DES offers more security than having a 112-bit DES key. Therefore, nongovernmental experts consider that triple DES "appears inviolate against all adversaries for the foreseeable future."[28] There is, however, no FIPS for triple-encryption DES.

Unlike the EES algorithm, the algorithm in the federal Digital Signature Standard has been published.[29] The public-key algorithm specified in the DSS uses a private key in signature generation, and a corresponding public key for signature verification (see box 2-2). However, the DSS technique was chosen so that public-key encryption functions would *not* be available to users.[30] This is significant because public-key encryption is extremely useful for key management and could, therefore, contribute to the spread and use of nonescrowed encryption.[31] At present, there is no FIPS for key exchange.

While other means of exchanging electronic keys are possible,[32] none is so mature as public-

---

[26] NIST, "Data Encryption Standard (DES)," FIPS PUB 46-2 (Gaithersburg, MD: U.S. Department of Commerce, Dec. 30, 1993).

[27] Ibid., p. 6.

[28] Martin Hellman, Professor of Electrical Engineering, Stanford University, personal communication, May 24, 1994; also see box 4-3 of the 1994 report.

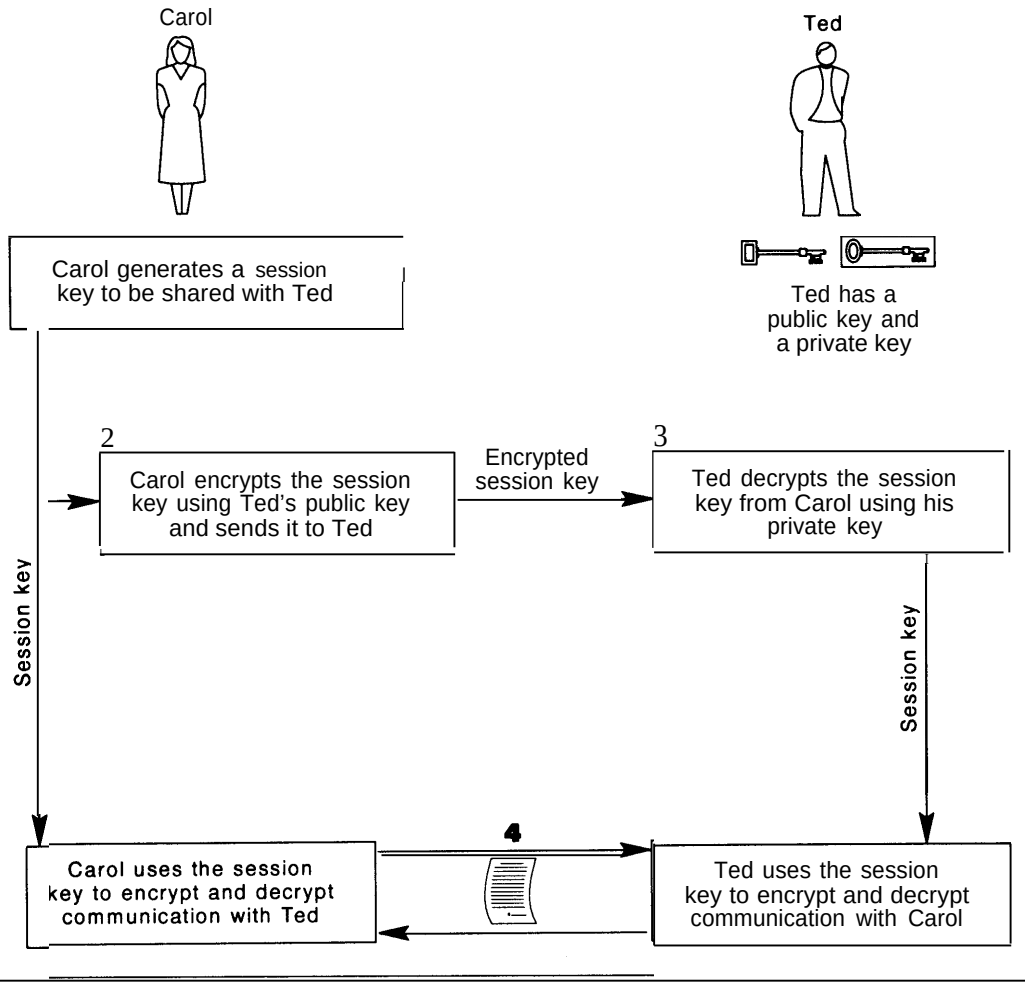
[29] See appendix C of OTA, op. cit., footnote 4, for a history of the DSS.

[30] According to F. Lynn McNulty, NIST Associate Director for Computer Security, the rationale for adopting the technique used in the DSS was that, "We wanted a technology that did signatures—and nothing else—very well." (Response to a question from Chairman Rick Boucher in testimony before the Subcommittee on Science of the House Committee on Science, Space, and Technology, Mar. 22, 1994.)

[31] Public-key encryption can be used for confidentiality and, thereby, for secure key exchange. Thus, public-key encryption can facilitate the use of symmetric encryption methods like the DES or triple DES. See figure 2-3.

[32] See, e.g., Tom Leighton (Department of Mathematics, Massachusetts Institute of Technology), and Silvio Micali (MIT Laboratory for Computer Science), "Secret-Key Agreement Without Public-Key Cryptography (extended abstract)," obtained from S. Micali, 1993.

FIGURE 2-4: Secret-Key Distribution Using Public-Key Cryptography



NOTE: Security depends on the secrecy of the session key and private keys, as well as the authenticity of the public keys.

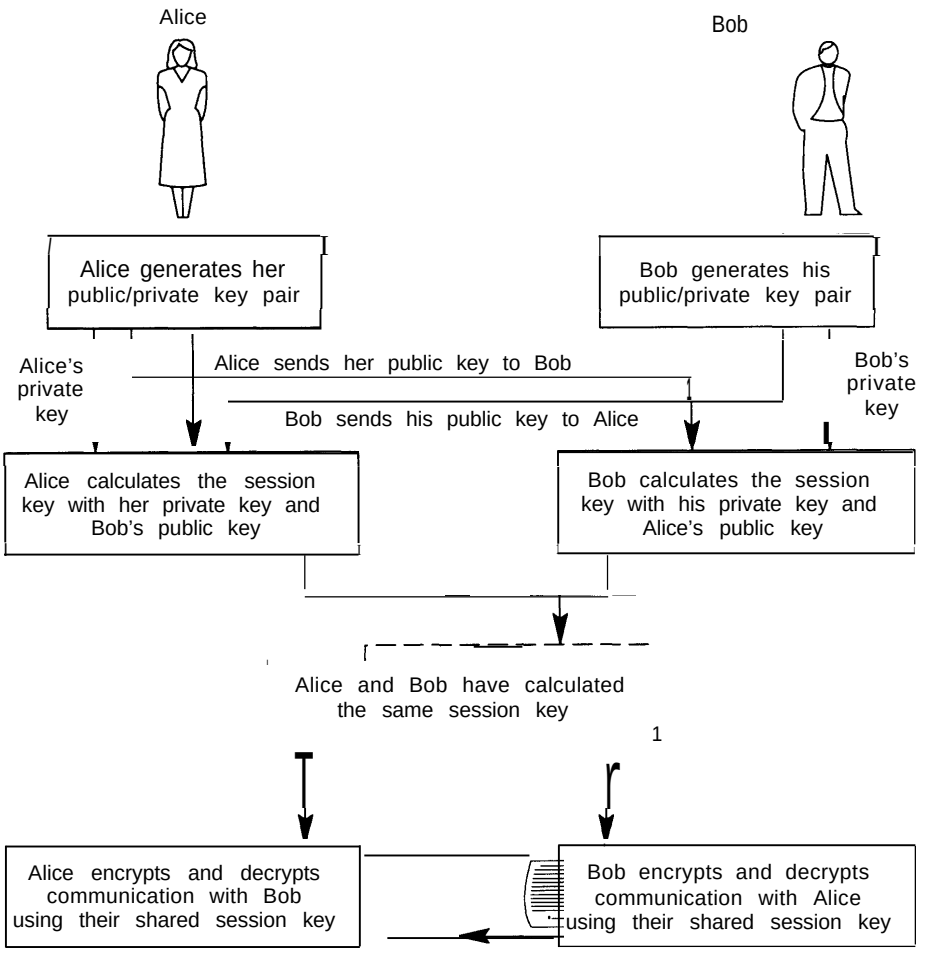
SOURCE: Office of Technology Assessment, 1994.

key technology. In contrast to the technique chosen for the DSS, the technique used in the most widely used commercial digital signature system (based on the Rivest-Shamir-Adleman, or RSA, algorithm) can also encrypt. Therefore, the RSA techniques can be used for secure key exchange (i.e., exchange of "secret''keys, such as those used with the DES), as well as for signatures (see figure 2-4). Another public-key technique, called the Diffie-Hellman method, can also be used to generate encryption keys (see figure 2-5), but does not encrypt.[33]

The 1994 OTA report concluded that both the EES and the DSS are federal standards that are part of a long-term control strategy intended to re-

[33] The public-key concept was first published by Whitfield Diffie and Martin Hellman in "New Directions in *Cryptography,''IEEE Transactions on Information Theory*, vol. IT-22, No. 6, November 1976, pp. 644-654. Diffie and Hellman described how such a system could be used for key distribution and to "sign" individual messages.

FIGURE 2-5: Diffie-Hellman Key Exchange



NOTE: An authentication scheme for the public keys may also be used

SOURCE: Office of Technology Assessment, 1994.

tard the general availability of "unbreakable" or "hard to break" encryption within the United States, for reasons of national security and law enforcement.[34] OTA viewed the EES and DSS as complements in this overall control strategy, intended to discourage future development and use of encryption without built-in law enforcement access, in favor of key-escrowed and related encryption technologies. If the EES and/or other key-escrow encryption standards (e.g., for use in computer networks) become widely used-or enjoy a large, guaranteed government market—this could ultimately reduce the variety of alternative cryptography products through market dominance that makes alternatives more scarce or more costly.

[34]See OTA, op.cit., footnote 4, ch. 4.

Federal Standards and the Computer Security Act of 1987

The Computer Security Act of 1987 (Public Law 100-235) is fundamental to development of federal standards for safeguarding unclassified information, to balancing national security and other objectives in implementing security and privacy policies within the federal government, and to other issues concerning government control of cryptography. Implementation of the Computer Security Act has been controversial, especially regarding the respective roles of NIST and NSA in standards development and the chronic shortage of resources for NIST's computer security program to fulfill its responsibilities under the act (see detailed discussion in chapter 4 of the 1994 OTA report).[35]

The Computer Security Act of 1987 was a legislative response to overlapping responsibilities for computer security among several federal agencies, heightened awareness of computer security issues, and concern over how best to control information in computerized or networked form. The act established a federal government computer-security program that would protect all unclassified, sensitive information in federal government computer systems and would develop standards and guidelines to facilitate such protection.

Specifically, the Computer Security Act assigned responsibility for developing government-wide, computer-system security standards (e.g., the FIPS) and guidelines and security-training programs to the National Bureau of Standards (NBS). NBS is now the National Institute of Standards and Technology, or NIST. According to its responsibilities under the act, NIST recommends federal information processing standards and guidelines to the Secretary of Commerce for approval (and promulgation, if approved). These FIPS do not apply to classified or "Warner Amendment" systems.[36] NIST can draw on the technical expertise of the National Security Agency in carrying out its responsibilities, but the NSA's role according to Public Law 100-235 is an advisory, rather than leadership, one.

Section 21 of the Computer Security Act established a Computer System Security and Privacy Advisory Board. The board, appointed by the Secretary of Commerce, is charged with identifying emerging safeguard issues relative to computer systems security and privacy, advising the NBS (NIST) and Secretary of Commerce on security and privacy issues pertaining to federal computer systems, and reporting its findings to the Secretary of Commerce, the Director of OMB, the Director of NSA, and Congress. Additionally, the act required federal agencies to identify computer systems containing sensitive information, to develop security plans for identified systems, and to provide periodic training in computer security for all federal employees and contractors who manage, use, or operate federal computer systems. Appendix B, drawn from the 1994 OTA report, provides more background on the purpose and implementation of the Computer Security Act and on the FIPS.

Federal Standards and the Marketplace

As the 1994 OTA report noted, not all government attempts at influencing the marketplace through the FIPS and procurement polices are successful. For example, the government made an early commitment to the Open Systems Interconnection (OSI) protocols for networking, but it is the ubiquitous Transmission Control Protocol/Internet

---

[35] Ibid., chapter 4 and appendix B. NIST's FY 1995 computer-security budget was on the order of $6.5 million, with $4.5 million of this coming from appropriated funds for "core" activities and the remainder from "reimbursable" funds from other agencies, mainly the Defense Department.

[36] Tha Warner Amendment (Public Law 97-86) excluded certain types of military and intelligence "automatic data processing equipment" procurements from the requirements of section 111 of the Federal Property and Administrative Services Act of 1949 (40 U.S.C. 795). Public Law 100-235 pertains to federal computer systems that come under section 111 of the Federal Property and Administrative Services Act of 1949.

Protocol (TCP/IP) that has enjoyed wide use throughout the world in the Internet and other networks. However, the FIPS usually influence the technologies used by federal agencies and provide a basis for interoperability, thus creating a large and stable, "target market" for safeguard vendors. If the attributes of the standard technology are also applicable to the private sector and the standard has wide appeal, an even larger but still relatively stable market should result. The technological stability means that firms compete less in terms of the attributes of the fundamental technology and more in terms of cost, ease of use, and so forth. Therefore, firms need to invest less in research and development (especially risky for a complex technology like cryptography) and in convincing potential customers of product quality. This can result in higher profits for producers, even in the long run, and in increased availability and use of safeguards based on the standard.

In the 1970s, promulgation of the DES as a stable and certified technology—at a time when the commercial market for cryptography-based safeguards for unclassified information was emerging—stimulated supply and demand. Although the choice of the algorithm was originally controversial due to concerns over NSA's involvement, the DES gained wide acceptance and has been the basis for several industry standards, in large part because it was a published standard that could be freely evaluated and implemented. Although DES products are subject to U.S. export controls, DES technology is also widely available around the world and the algorithm has been adopted in several international standards. The process by which the DES was developed and evaluated also stimulated private sector interest in cryptographic research, ultimately increasing the variety of commercial safeguard technologies.

The 1994 OTA report regarded the introduction of an incompatible *new* federal standard—for example, the Escrowed Encryption Standard—as destabilizing. At present, the EES and related technologies have gained little favor in the private sector—features such as the government key-escrow agencies, classified algorithm, and hardware-only implementation all contribute to its lack of appeal. But, if the EES and related technologies (e.g., for data communications) ultimately do manage to gain wide appeal in the marketplace, they might be able to "crowd out" safeguards that are based upon other cryptographic techniques and/or do not support key escrowing.[37]

The 1994 OTA report noted that this type of market distortion, intended to stem the supply of alternative products, may be a long-term objective of the key-escrow encryption initiative. In the long term, a loss of technological variety is significant to private sector cryptography, because more diverse research and development efforts tend to increase the overall pace of technological advance. In the near term, technological uncertainty may delay widespread investments in *any* new safeguard, as users wait to see which technology prevails. The costs of additional uncertainties and delays due to control interventions are ultimately borne by the private sector and the public.

Other government policies can also raise costs, delay adoption, or reduce variety. For example, export controls have the effect of segmenting domestic and export encryption markets. This creates additional disincentives to invest in the development—or use—of robust, but nonexportable, products with integrated strong encryption (see discussion below).

Export Controls

Another locus of concern is export controls on cryptography (see appendix C).[38] The United States has two regulatory regimes for exports, depending on whether the item to be exported is military in nature, or is "dual-use," having both civilian and military uses. These regimes are ad-

[37] Ibid., pp. 128-132. A large, stable, lucrative federal market could divert vendors from producing alternative, riskier products; product availability could draw private sector customers.

[38] For more detail, see ibid., chapters 1 and 4.

ministered by the State Department and the Commerce Department, respectively. Both regimes provide export controls on selected goods or technologies for reasons of national security or foreign policy. Licenses are required to export products, services, or scientific and technical data originating in the United States, or to re-export these from another country. Licensing requirements vary according to the nature of the item to be exported, the end use, the end user, and, in some cases, the intended destination. For many items under Commerce jurisdiction, no specific approval is required and a "general license" applies (e.g., when the item in question is not military or dual-use and/or is widely available from foreign sources). In other cases, an export license must be applied for from either the State Department or the Commerce Department, depending on the nature of the item. In general, the State Department's licensing requirements are more stringent and broader in scope.[39]

Software and hardware for robust, user-controlled encryption are under State Department control, unless State grants jurisdiction to Commerce. This has become increasingly controversial, especially for the information technology and software industries.[40] The impact of export controls on the overall cost and availability of safeguards is especially troublesome to business and industry at a time when U.S. high-technology firms find themselves as targets for sophisticated foreign-intelligence attacks and thus have urgent need for sophisticated safeguards that can be used in operations worldwide, as well as for secure communications with overseas business partners, suppliers, and customers.[41] Software producers assert that, although other countries do have export and/or import controls on cryptography, several countries have more relaxed export controls on cryptography than does the United States.[42]

On the other hand, U.S. export controls may have substantially slowed the proliferation of cryptography to foreign adversaries over the years. Unfortunately, there is little public explanation on the degree of success of these export controls[43] and the necessity for maintaining strict controls on strong encryption[44] in the face of for-

---

[39] Ibid., pp. 150-154.

[40] To ease some of these burdens, the State Department announced new licensing procedures on Feb. 4, 1994. These changes were expected to include license reform measures for expedited distribution (to reduce the need to obtain individual licenses for each end user), rapid review of export license applications, personal-use exemptions for U.S. citizens temporarily taking encryption products abroad for their own use, and special licensing arrangements allowing export of key-escrow encryption products (e.g., EES products) to most end users. At this writing, expedited-distribution reforms were in place (*Federal Register* , Sept. 2, 1994, pp. 45621-45623), but personal-use exemptions were still under contention (Karen Hopkinson, Office of Defense Trade Controls, personal communication, Mar. 8, 1995).

[41] See, e.g., U.S. Congress, House of Representatives, Subcommittee on Economic and Commercial Law, Committee on the Judiciary, *The Threat of Foreign Economic Espionage to U.S. Corporations*, hearings, 102d Congress, 2d sess., Apr. 29 and May 7, 1992, Serial No. 65 (Washington, DC: U.S. Government Printing Office, 1992). See also discussion of business needs and export controls in chapter 3 of this background paper.

[42] OTA, op. cit., footnote 4, pp. 154-160. Some other countries do have stringent export and/or import restrictions.

[43] For example, the Software Publishers Association (SPA) has studied the worldwide availability of encryption products and, as of October 1994, found 170 software products (72 foreign, 98 U.S.-made) and 237 hardware products (85 foreign, 152 U.S.-made) implementing the DES algorithm for encryption. (Trusted Information Systems, Inc. and Software Publishers Association, *Encryption Products Database Statistics*, October 1994.) Also see OTA, op. cit., footnote 4, pp. 156-160.

[44] For a discussion of export controls and network dissemination of encryption technology, see Simson Garfinkle, *PGP: Pretty Good Privacy* (Sebastopol, CA; O'Reilly and Assoc., 1995). PGP is a public-key encryption program developed by Phil Zimmerman. Variants of the PGP software (some of which infringe the RSA patent in the United States) have spread worldwide over the Internet. Zimmerman has been under grand jury investigation since 1993 for allegedly breaking the munitions export-control laws by permitting the software to be placed on an Internet-accessible bulletin board in the United States in 1991. (See Vic Sussman, "Lost in Kafka Territory," *U.S. News and World Report*, Apr. 3, 1995, pp. 30-31.)

eign supply and networks like the Internet that seamlessly cross national boundaries.

Appendix C drawn from the 1994 OTA report, provides more background on export controls on cryptography. In September 1994, after the OTA report had gone to press, the State Department announced an amendment to the regulations implementing section 38 of the Arms Export Control Act.[45] The new rule implements one of the reforms applicable to encryption products that were announced on February 4, 1994 by the State Department (see footnote 47 below and also chapter 4 of the 1994 OTA report). It established a new licensing procedure to permit U.S. encryption manufacturers to make multiple shipments of some encryption items covered by Category XIII(b)(1) of the Munitions List (see appendix C) directly to end users in approved countries, without obtaining individual licenses.[46] Other announced reforms, still to be implemented, include special licensing procedures allowing export of key-escrow encryption products to "most end users."[47] The ability to export strong, key-escrow encryption products would presumably increase the appeal of escrowed-encryption products to private sector safeguard developers and users.

In the 103d Congress, legislation intended to streamline export controls and ease restrictions on mass-market computer software, hardware, and technology, including certain encryption software, was introduced by Representative Maria Cantwell (H.R. 3627) and Senator Patty Murray (S. 1846). In considering the Omnibus Export Administration Act of 1994 (H.R. 3937), the House Committee on Foreign Affairs reported a version of the bill in which most computer software (including software with encryption capabilities) was under Commerce Department controls and in which export restrictions for mass-market software with encryption were eased. In its report, the House Permanent Select Committee on Intelligence struck out this portion of the bill and replaced it with a new section calling for the President to report to Congress within 150 days of enactment, regarding the current and future international market for software with encryption and the economic impact of U.S. export controls on the U.S. computer software industry.[48]

At the end of the 103d Congress, the omnibus export administration legislation had not been enacted. Both the House and Senate bills contained language calling for the Clinton Administration to conduct comprehensive studies on the international market and availability of encryption technologies and the economic effects of U.S. export controls. In a July 20, 1994, letter to Representative Cantwell, Vice President Gore had assured her that the "best available resources of the federal government" would be used in conducting these studies and that the Clinton Administration would "reassess our existing export controls based on the results of these studies."[49]

At this writing, the Commerce Department and NSA are assessing the economic impact of U.S. export controls on cryptography on the U.S. computer software industry.[50] As part of the study, NSA is determining the foreign availability of en-

---

[45] Department of State, Bureau of Political-Military Affairs, 22 CFR parts 123 and 124, *Federal Register*, vol. 59, No. 170, Sept. 2, 1994, pp. 45621-45623.

[46] Category XIII(b)(1) covers "Information Security Systems and equipment, cryptographic devices, software and components specifically designed or modified therefore," in particular, "cryptographic and key-management systems and associated equipment, subcomponents, and software capable of maintaining information or information-system secrecy/confidentiality."

[47] Martha Harris, Deputy Assistant Secretary for Political-Military Affairs, U.S. Department of State, "Encryption—Export Control Reform," statement, Feb. 4, 1994. See OTA, op. cit., footnote 4, pp. 159-160.

[48] A study of this type (see below) is expected to be completed in mid-1995.

[49] Vice President Al Gore, letter to Representative Maria Cantwell, July 20, 1994. See OTA, op. cit., footnote 4, pp. 11-13.

[50] Maurice Cook, Bureau of Export Administration, Department of Commerce, personal communication, Mar. 7, 1995.

cryption products. The study is scheduled to be delivered to the National Security Council (NSC) by July 1, 1995. According to the Council, it is anticipated that there will be both classified and unclassified sections of the study; there may be some public release of the unclassified material.[51] In addition, an ongoing National Research Council study that would support a broad congressional review of cryptography (and that is expected to address export controls) is due to be completed in 1996.[52] At this writing, the NRC study committee is gathering public input on cryptography issues.

In the 104th Congress, Representative Toby Roth has introduced the "Export Administration Act of 1995" (H.R. 361). This bill does not include any specific references to cryptography; at this writing, it is not clear whether or when the contentious issue of cryptography export controls will become part of legislative deliberations. Alternatively, the Clinton Administration could ease export controls on cryptography without legislation. As was noted above, being able to export key-escrow encryption products would presumably make escrowed-encryption products more attractive to commercial developers and users. Therefore, the Clinton Administration could ease export requirements for products with integrated key escrowing as an incentive for the commercial development and adoption of such products (see discussion of cryptography initiatives in chapter 4).

Overview of Issues and Options

As noted above, the 1994 OTA report *Information Security and Privacy in Network Environments* focuses on three sets of policy issues:

1. national cryptography policy, including federal information processing standards and export controls;
2. guidance on safeguarding unclassified information in federal agencies; and
3. legal issues and information security, including electronic commerce, privacy, and intellectual property.

Appendix E of this paper, based on chapter 1 of the 1994 report, reviews the set of policy options, about two dozen, developed by OTA. The need for *openness*, *oversight*, and *public accountability*—given the broad public and business impacts of these policies—runs throughout the discussion of possible congressional actions.

Two key questions underlying consideration of many of these options—in particular, those addressing cryptography policy and unclassified information security within the federal government are:

1. **How will we as a nation develop and maintain the balance among traditional "national security" (and law enforcement) objectives and other aspects of the public interest, such as economic vitality, civil liberties, and open government?**
2. **What are the costs of government efforts to control cryptography and who will bear them?**

Some of these costs—for example, the incremental cost of requiring a "standard" solution that is less cost-effective than the "market" alternative in meeting applicable security requirements—may be relatively easy to quantify, compared with others. But none of these cost estimates will be easy to make. Some costs may be extremely difficult to quantify, or even to bound—for example, the impact of technological uncertainties, delays, and regulatory requirements on U.S. firms' abilities to compete effectively in the international marketplace for information technologies. Ultimately, however, these costs are all borne by the public, whether in the form of taxes, product prices, or foregone economic opportunities and earnings.

---

[51] Bill Clements, National Security Council, personal communication, Mar. 21, 1995.

[52] For information about the NRC study, which was mandated by Public Law 103-160, contact Herb Lin, National Research Council, 2101 Constitution Avenue, N.W., Washington, DC, 20418 (crypto@nas.edu). See discussion in chapter 1 and 4 of OTA, op. cit., footnote 4.