CHAPTER ONE

The Role of Cryptography in Electronic Data Processing

CRYPTOGRAPHY, PRIVACY, AND DATA SECURITY

Organizations in both the public and private sectors have become increasingly dependent on electronic data processing. Vast amounts of digital data are now gathered and stored in large computer data bases and transmitted between computers and terminal devices linked together in complex communications networks. Without appropriate safeguards, these data are susceptible to interception (e.g., via wiretaps) during transmission, or they may be physically removed or copied while in storage. This could result in unwanted exposures of data and potential invasions of privacy. Data are also susceptible to unauthorized deletion, modification, or addition during transmission or storage. This can result in illicit access to computing resources and services, falsification of personal data or business records, or the conduct of fraudulent transactions, including increases in credit authorizations, modification of funds transfers, and the issuance of unauthorized payments.

Legislators, recognizing that the confidentiality and integrity of certain data must be protected, have passed laws to help prevent these problems. But laws alone cannot prevent attacks or eliminate threats to data processing systems. Additional steps must be taken to preserve the secrecy and integrity of computer data. Among the security measures that should be considered is *cryptography*, which embraces methods for rendering data unintelligible to unauthorized parties.

Cryptography is the only known practical method for protecting information transmitted through communications networks that use land lines, communications satellites, and microwave facilities. In some instances it can be the most economical way to protect stored data. Cryptographic procedures can also be used for message authentication, digital signatures, and personal identification for authorizing electronic funds transfer and credit card transactions.

Attack Scenarios

The possibility exists that unauthorized individuals can intercept data by eavesdropping. In fact, there are several methods of eavesdropping.

Wiretapping. Interception of individual transmissions over communication lines by using hardwire connections.

Electromagnetic Eavesdropping. Interception of wireless transmissions, for example, radio and microwave transmissions, or information-bearing electromagnetic energy emanating from electronic devices.

Acoustic Eavesdropping. Interception of sound waves created by the human voice or by printing, punching, or transmitting equipment. (This method of eavesdropping is listed for reference only. In almost all cases, physical security measures rather than cryptography are effective against this threat.)

Eavesdropping is completely passive: the opponent only listens to or records information being transmitted.[1] An attack involving only eavesdropping is called a *passive attack.* If, in addition, the opponent modifies transmitted information or injects information into the communication path, the attack is called an *active attack.*

In a passive attack, a tape recording of digitial data intercepted from a communication path is made. The data can be reconstructed by analyzing the recording tape or playing it back into suitable receiving equipment (e.g., a modem[2] and terminal). In an active attack, a terminal and modem compatible with the transmission line are necessary, and, in some cases, a minicomputer that can quickly modify intercepted information may be required.

Cables running between building offices and telephone company junction boxes located inside the user's premises are particularly vulnerable to wiretapping. The many lines of a telephone cable are separated at the boxes and usually are labeled. A wiretap can be performed by almost anyone; no special technical skills are required and the necessary equipment is relatively inexpensive. However, once the lines are outside the building, and until they reach telephone company switching facilities, access to selected lines becomes more difficult.[3] Effective attacks are nevertheless still possible.

Interception of radio and microwave transmissions poses a particularly subtle threat because a physical connection (tap) to the transmission link is not required. However, because microwave links, including those used in satellite communications, can contain several thousand channels, sophisticated and expensive equipment [1] may be required to intercept and separate channel signals. Despite this cost, the reward for a successful attack can be extremely great.

[1] It is common practice to use the term wiretapping to refer to the interception of all forms of voice and data communications, regardless of whether that information is transmitted via communication lines, radio, or microwave.

[2] A *modem* is a device used to link a terminal (or other transmitting device) and the communication channel. It modulates and demodulates, i.e., converts digital signals to analog, and vice versa.

[3] Within telephone company switching facilities, interception may require collusion with telephone company personnel.

According to a July 1977 article in *The New York Times* [2]:

> the Russians, using advanced scientific equipment, have been "plucking" from the air many long-distance [telephone] calls transmitted by microwaves, or ultrahigh-frequency radio signals. They then used massive high-speed computers to locate sensitive information in the transmissions.[4]

The Russian Embassy in Washington, D.C. and at least five other locations were purportedly used as listening posts to monitor many private and government telephone calls.

Every operating electronic device emits electromagnetic energy. For those devices handling data, it is important to know whether the energy level of any information-bearing emanations is high enough (and distinct enough) for an opponent to detect and interpret the data contained therein. Usually the answer is no. When the equipment in question has integral shielding that can reduce the information-bearing emissions to below threshold levels for all but the most sophisticated detection equipment, such eavesdropping is difficult and expensive [1]. However, for unshielded digital electronic devices employing slow-speed serial data streams, the complexity and costs of eavesdropping diminish.

In the absence of strong cryptographic protection, an eavesdropping opponent may learn enough about the operational procedures of the system, including passwords, to defeat any security mechanisms.

In applications involving automated teller machines (ATMs) that have the capacity to dispense cash, a passive wiretap may permit an opponent to obtain information (personal identifier, password) needed to impersonate legitimate ATM users. With an active wiretap, an opponent could inject unauthorized messages to obtain funds illegally. In other applications involving electronic funds transfer (EFT), the opponent, by masquerading as one bank, could send a message to another bank specifying that money be credited to an account previously established. The opponent could then withdraw from the account before the deception could be detected through normal auditing procedures.

Although there is little evidence publicly available to indicate how much eavesdropping has actually taken place, the potential for such activity has raised concerns about the confidentiality of personal affairs and business transactions. It is reasonable to anticipate problems when eavesdropping is the most practical means to achieve the desired result, especially when the payoff is great enough and the nature of the punishment, if discovered, is small enough to justify the crime!

EFT systems, which move many billions of dollars between financial institutions linked together in a communications network, represent a tempting target. Recognizing the threat, the Federal Reserve System has begun to install cryptographic devices on some of its communication lines [3].

Cryptography is the only practical means for protecting the confidentiality

[4] Computers can locate certain words or sets of words, certain voice prints, and certain dialed numbers for selection of which calls to monitor.

of information transmitted through potentially hostile environments, where it is either impossible or impractical to protect the information by conventional physical means. A cryptographic system properly implemented can prevent much eavesdropping damage. Also, damage resulting from message alteration, message insertion, and message deletion can be avoided. And in some cases a cryptographic system can reduce the severity of problems caused by the accidental exposure of misrouted information.

Administrative and physical security procedures often can provide adequate protection for off-line data transport and storage. However, where file security methods are either nonexistent or weak, encryption may provide the most effective and economical protection.

A more complete treatment of eavesdropping techniques can be found in James Martin's *Security, Accuracy and Privacy in Computer Systems* [1].

Technical Implications of Privacy Legislation

Privacy, as it involves collections of personal data, relates to the right of individuals to control or influence what information about them may be collected and stored, and by whom, for what specific reasons, and to whom that information may then be disclosed. Privacy also relates to the right of individuals to know that information about them has been compiled and that it is correct and complete enough for the intended uses. Furthermore, individuals should be able to expect that information relating to them will not be made available to others they have not authorized, and they should have the right to challenge the accuracy of such information. (See Westin's *Privacy and Freedom* [4]).

From a technical viewpoint, the requirements of privacy legislation, both enacted and pending, generally apply to the categories of data collection (record keeping, information manipulation, communication and storage) and information controls (system accountability and integrity, and information dissemination and presentation). Although privacy is a legal, social, and moral concern, privacy legislation has specific technical implications.

To understand the technical implications of privacy statutes, one must review such legislation and look to concepts borrowed from existing law in an attempt to foresee how courts may interpret and apply new legislation. To date, the Privacy Act of 1974 [5] has been the most significant piece of legislation enacted in the United States concerning computers and data security. The act is prefaced by several congressional findings, such as:

> The increasing use of computers and sophisticated information technology, while essential to the efficient operation of the government, has greatly magnified the harm to individual privacy that can occur from any collection, maintenance, use, or dissemination of personal information.

In view of these findings, the act provides for certain safeguards concerning information systems. Although it is limited to federal agencies and certain government contractors, several provisions are pertinent to a discussion of data security in all computer applications. Each federal agency must accurately record disclosures of certain types of information under that agency's control. The act also requires each agency to establish "rules of conduct" for persons involved in the design, development, operation, or maintenance of any system of records involving personal data.

The act further requires that each agency take certain steps to maintain the confidentiality of records held by that agency. Each agency must

> establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained. [6]

In July 1977, the Privacy Protection Study Commission established under the act urged, in its final report to the President and to Congress, that certain corrections be made to the act so that obligations imposed by the law would be more realistic. For example, the commission recommended that federal agencies should be required to

> establish reasonable administrative, technical, and physical safeguards to assure the integrity, confidentiality and security of its individually identifiable records so as to minimize the risk of substantial harm, embarrassment, inconvenience, or unfairness to the individual to whom the information pertains. [8]

The question of what are reasonable safeguards depends on two factors: standard of care and state of the art. The standard of care as applied by the courts would be the so-called standard of reasonable care—the care that reasonable persons, similarly situated, would take under similar circumstances. In the case of *The T. J. Hooper* [9], a federal court declared

> In most cases, reasonable prudence is in fact common prudence; but strictly it is never its measure; a whole calling may have unduly lagged in the adoption of new and available devices. It never may set its own test, however persuasive be its usages. Courts must in the end say what is required; there are precautions so imperative that even their universal disregard will not excuse their omission.

How then will the courts decide what is required? Reasonable care depends on the probability and gravity of the harm balanced against the burden and cost of taking sufficient precautions to prevent the harm. A common sense cost/benefit analysis is thus one method of determining what is reasonable.

State of the art concerns itself with whether a certain technological device or process is technically feasible and commercially available. While to a scientist the question of technology may be a relatively objective one, to a court it may necessarily involve policy considerations. A court might well consider the question of technological feasibility along with economic and public interest considerations. What, then, can be said with regard to cryptography?

Although its cost may still be significant, cryptography currently is the only known practical method to achieve communication security. It represents the only mechanism that can meet the state of the art requirement in

Previous Chapter Previous Page Home Next page Next Chapter

providing such protection. Moreover, for some federal agencies and private organizations, cryptography may be the only practical way to satisfy the requirements of existing or proposed privacy legislation. With a strong encryption procedure available to the general public, and with cryptographic systems also publicly available, cryptographic protection of data has become both technically feasible and commercially achievable.

Further incentive for the implementation of cryptography as a means of protecting assets or data that represent assets may also come from the Foreign Corrupt Practices Act of 1977 [10]. This amendment to the Securities and Exchange Act of 1934 requires every issuer of stock listed on a national exchange to make and keep books, records, and accounts which, in reasonable detail, accurately and fairly reflect the transaction and disposition of corporate assets. The act obliges the corporation and its management to devise and maintain a system of internal accounting controls to provide reasonable assurance that "access to assets is permitted only in accordance with management's . . . authorization" [11].

These provisions apply to all corporate transactions, whether or not they are "foreign" or "corrupt." In addition to corporate fines, criminal penalties of fines and/or imprisonment may be imposed on officers and directors for violations. Assuring that access to assets or data that represent assets is permitted only with management's authorization may require, in certain applications, the use of protective measures that cryptography can offer.

Since laws and regulations are constantly updated, specific applications and security measures should be reviewed with one's own legal counsel. For additional reading material and references dealing with privacy legislation, see Lance J. Hoffman's *Modern Methods for Computer Security and Privacy* [12].

THE DATA ENCRYPTION STANDARD

Martin [1] has stated, "If cryptography is worth using at all, it should be used well." In other words, high-quality cryptography must be the objective of the algorithm designer. Less secure approaches, although attractive for economic or performance reasons, can lead to a false sense of security. And cryptography that is scarcely more than a nuisance to the opponent is therefore worse than no cryptography at all. Thus high-quality cryptography is the best way to ensure effective cryptographic protection of data, even though skilled and determined opponents will always present a threat.

Recognizing the need to adopt a standard algorithm[5] for the encryption of computer data, the National Bureau of Standards (NBS) published a notice in the Federal Register on May 15, 1973, in which it solicited proposals for

[5] An *algorithm* is a procedure for calculating the value of some quantity or for finding the solution to some mathematical problem that frequently involves repetition. (See also Cryptographic Algorithms, Chapter 2.) Note that references outside a chapter are designated by the heading and chapter number, whereas references within a chapter are designated only by the heading.

"cryptographic algorithms for [the] protection of computer data during transmission and dormant storage" [13]. In part, the notice read:

> Over the last decade, there has been an accelerating increase in the accumulations and communication of digital data by government, industry and by other organizations in the private sector. The contents of these communicated and stored data often have very significant value and/or sensitivity. It is now common to find data transmissions which constitute funds transfers of several million dollars, purchase or sale of securities, warrants for arrests or arrest and conviction records being communicated between law enforcement agencies, airline reservations and ticketing representing investment and value both to the airline and passengers, and health and patient care records transmitted among physicians and treatment centers.
>
> The increasing volume, value and confidentiality of these records regularly transmitted and stored by commercial and government agencies has led to heightened recognition and concern over their exposure to unauthorized access and use. This misuse can be in the form of theft or defalcations of data records representing money, malicious modification of business inventories or the interception and misuse of confidential information about people. The need for protection is then apparent and urgent.
>
> It is recognized that encryption (otherwise known as scrambling, enciphering or privacy transformation) represents the only means of protecting such data during transmission and a useful means of protecting the content of data stored on various media, providing encryption of adequate strength can be devised and validated and is inherently integrable into system architecture. The National Bureau of Standards solicits proposed techniques and algorithms for computer data encryption. The Bureau also solicits recommended techniques for implementing the cryptographic function; for generating, evaluating, and protecting cryptographic keys; for maintaining files encoded under expiring keys; for making partial updates to encrypted files; and mixed clear and encrypted data to permit labeling, polling, routing, etc. The Bureau in its role for establishing standards and aiding government and industry in assessing technology, will arrange for the evaluation of protection methods in order to prepare guidelines.

In a second notice on August 27, 1974, the NBS again solicited cryptographic algorithms. Basically, the two notices stated that the NBS recognized the "apparent and urgent" need for data protection within government and the private sector, and that encryption is the "only means" for protecting communicated data, and a "useful means" for protecting stored data. The NBS therefore solicited "proposals for algorithms for the encryption of computer data" and agreed to "arrange for the evaluation" of these algorithms in order to "select those algorithms suitable for commercial and non-defense goverment use."

The requirements that NBS imposed for acceptable encryption algorithms included the following.

1. They must be completely specified and unambiguous.
2. They must provide a known level of protection, normally expressed in length of time or number of operations required to recover the key in terms of the perceived threat.

3. They must have methods of protection based only on the secrecy of the keys.
4. They must not discriminate against any user or supplier.

On August 6, 1974, International Business Machines Corporation (IBM) submitted a candidate algorithm that had been jointly developed by personnel at the company's research laboratory in Yorktown Heights, New York and at its Kingston, New York development laboratory.

According to the NBS, only one algorithm (the one submitted by IBM) was found acceptable. (Because cryptographic expertise within the government is almost totally resident within the National Security Agency (NSA), and NSA is the national communications security authority, NBS requested and obtained assistance from NSA in assessing the strength of candidate algorithms [14]). This algorithm formed the basis for the proposed Data Encryption Standard (DES). On March 17, 1975, the NBS published the algorithm stating its intent to have it considered as a Federal Information Processing Standard and requesting comments on the algorithm and its submission as a standard. On July 15, 1977, the proposed DES became a federal standard.

DES applies only to federal departments and agencies for the cryptographic protection of computer data not classified according to the National Security Act of 1974, as amended, or the Atomic Energy Act of 1954, as amended [15].[6] However, since the standard may be adopted and used by organizations outside the federal government, the NBS has provided the private sector with a cryptographic algorithm that has been found, after intensive analysis,[7] to be free from any known shortcut solution. DES has also been adopted by the American National Standards Institute (ANSI), on the recommendation of the Committee on Computers and Information Processing (X3), as the standard industry algorithm ("Data Encryption Algorithm," X3.92).

Incorporation of DES in computers and related peripheral devices can eliminate cryptographic algorithm incompatability between different manufacturers' equipment. Moreover, costs associated with the development and validation of comparable cryptographic algorithms can be avoided.

For a more detailed history of DES, see Ruth M. Davis' "The Data Encryption Standard in Perspective" [16].

DEMONSTRATING EFFECTIVE CRYPTOGRAPHIC SECURITY

Developing a strong cryptographic algorithm involves two endeavors: design and validation. Algorithm design consists of specifying criteria and inventing

[6] Supplemental interpretation of the standard has allowed its use in selected classified areas [17].

[7] Seventeen man-years of effort were expended by IBM personnel to design and validate DES. Several consultants were employed by IBM to provide additional assistance and analysis. Subsequently, an independent validation of the algorithm was initiated by the NBS and performed by the NSA.

a candidate algorithm that satisfies those criteria. Algorithm validation consists of subjecting the candidate algorithm to a thorough, intensive, and rigorous analysis (cryptanalysis).

Algorithm validation is performed by an "attack" team playing the role of opponent or antagonist. Attempts are made to uncover weaknesses that might lead to an attack against the algorithm, and to break the algorithm by using all known methods of attack for that type of algorithm. In the absolute sense, *a cryptographic algorithm is attack-proof (perfectly strong) only if there is no procedure or method that can be successfully used to attack (break) it.* Thus, to certify that an algorithm is attack-proof requires the proof of a negative hypothesis: the nonexistence of a procedure for breaking the algorithm. In general, such proofs are impossible.[8]

Since it is impossible to prove that an algorithm is attack-proof, a compromise is necessary. The dilemma must be resolved (to an acceptable point) by performing algorithm validation on a best-effort basis. An algorithm is considered strong (resistant to certain types of attack) if no exploitable weakness can be uncovered during the validation effort. Thus the basis for developing or creating a strong cryptographic algorithm requires an extensive knowledge of how to break cryptographic algorithms. The proper application of this knowledge helps to build a strong algorithm. In turn, the quality of this measure of strength depends on the knowledge and expertise of the attack team, and the scope, intensity, and duration of the investigation. Ideally, the two tasks—design and validation—are performed by two independent, and possibly competitive, groups. In practice, however, the design and validation groups may interact. Such interaction is intended to provide the means to uncover flaws and defects, thereby permitting the algorithm's designers to incorporate any necessary improvements.

A properly validated cryptographic algorithm of demonstrated strength is the foundation upon which more sophisticated encryption-based protection schemes (communication and file security, message authentication, and so forth) can be implemented. With any nonsecret, key-controlled cryptographic algorithm, such as DES, the protection achieved through encryption ultimately depends on how well the secrecy of the cryptographic keys can be maintained. An opponent who obtains the key(s), as well as the encrypted data, does not need to perform a cryptanalysis; since the algorithm is publicly available, the key will directly "unlock" the data. Thus a strong cryptographic algorithm alone does not automatically guarantee protection. Effective security requires both a strong algorithm and secure procedures for generating, distributing, installing, and managing keys.

It is not surprising that the problems encountered in cryptographic algorithm design are also encountered in the design of encryption-based protection schemes. These schemes are designed and validated in the same manner as cryptographic algorithms. A favorable validation leads to a conclu-

[8] Such a proof is possible for the so-called *one-time tape* system (see Designing an Algorithm, Chapter 2). A certifiably unbreakable cipher is obtained if a plaintext is combined bit-by-bit or character-by-character with a truly random sequence of bits or characters using a single, elementary, reversible operation (e.g., modulo 2 addition).

sion that penetration of the system, although not certifiably impossible, is at least demonstrably difficult or unlikely.

THE OUTLOOK FOR CRYPTOGRAPHY

In the late 1960s and early 1970s, data security began to be recognized as a major design concern for data processing (DP) systems. During this period, systems were designed to operate reliably only in environments subjected to "random noise"–power line disturbances, spurious electromagnetic radiation, equipment malfunction, programming errors, and the like. Few, if any, precautions were taken to protect the secrecy of computer data, or to defend it against "intelligent noise"–the deliberate actions of people intent on subversion. As a result, many systems were vulnerable to attack. Transmitted data could be intercepted and data could be modified, deleted, or added to a system. But today data processing system designers are more aware of these threats, and cryptography is recognized as an important factor in the design of secure systems.

Within the computer industry there is a movement toward more secure systems. Cryptography is being used in selected high-risk applications. For example, significant numbers of cash-issuing terminals employ DES to verify the identity of customers. At IBM's Thomas J. Watson Research Center at Yorktown Heights, New York, a DES-based cryptographic system, known as the Information Protection System (IPS), is used to protect stored computer data [18]. International Flavors and Fragrances, Inc., uses DES to protect valuable formulas transmitted via voice-grade public telephone lines [19]. Other designs for new and better cryptographic applications are being developed. Therefore, those responsible for the security of computer operations and data should be prepared to include cryptographic measures in their security system. Although many companies might not feel the need to encrypt their data, and even if they do, they might not use DES, according to a statement in the December 1979 issue of *EDP Analyzer,* "there is a fairly good chance they would be making a mistake on both counts–and particularly the second" [20].

However, to derive the maximum benefits from cryptography, significant planning is required to integrate it into system architectures properly, and standards are necessary to assure cryptographic compatibility within applications and among devices implementing DES. In addition to establishing the standard for computer data encryption [15], the NBS has published a standard on modes of DES operation [21] and is investigating file encryption in order to issue yet another standard for this cryptographic application.

Efforts by the Technical Committee on Encryption (X3.T1) on behalf of the American National Standards Institute (ANSI) have resulted in the adoption of DES as an ANSI standard [22]. In addition, the committee is developing standards for DES modes of operation and DES devices operating at the communications link level. Work is in progress to develop additional cryptographic standards for higher levels of communication protection as well as for removable file media.

ANSI technical committees involved with the finance industry are developing application standards to address the broad subject of electronic funds transfer systems, including methods using DES for consumer-initiated electronic financial transactions as well as transaction data authentication.

Other government agencies besides the NBS have drafted additional application standards involving DES and DES equipment. Proposed Federal Standard 1026 [23] specifies the interoperability and security requirements for use of DES. Proposed Federal Standard 1027 [24] specifies the minimum physical and electrical security features of devices implementing DES.

The development of cryptographic standards is a lengthy process. Proposed Federal Standard 1026, for example, represents more than three years of work. ANSI adopted DES more than three years after its adoption by the U.S. Federal Government. The time necessary to draft and adopt cryptographic standards is relative to the time necessary to design, test, manufacture, and install cryptographic computer equipment. Thus to meet the challenges and demands in the emerging field of system security, data processing people should begin their cryptographic education, research, and planning now.

REFERENCES

1. Martin, J. T., *Security, Accuracy and Privacy in Computer Systems,* Prentice-Hall, Englewood Cliffs, NJ, 1973.
2. Burnham, D., and Horrock, N. M., "Administration Maps Secret Plan to Fight Telephone Intrusion," *The New York Times,* pp. 1, 34 (July 10, 1977).
3. O'Toole, T., "Fed Is Testing 'Unbreakable' Code System," *Washington Post,* p. A10 (August 13, 1978).
4. Westin, A. F., *Privacy and Freedom,* Atheneum, New York, 1968.
5. Privacy Act of 1974, Public Law 93-579, 5 U.S.C. 552a(e) (10).
6. 5 U.S.C. 552(a), Sec. 3(E) (10).
7. 5 U.S.C. 552(a), Sec. 5(B) (1), (2).
8. *Personal Privacy in an Information Society–The Report of the Privacy Protection Study Commission,* p. 527 (July 1977).
9. *The T. J. Hooper,* 60F. 2d 737 N2d Cir. (1932), cert. den 287 U.S. 662 (1933).
10. Public Law 95-213, Title I S102, 91 Stat. 1494.
11. 15 U.S.C. 78m(b)(2).
12. Hoffman, L. J., *Modern Methods for Computer Security and Privacy,* Prentice-Hall, Englewood Cliffs, NJ, 1977.
13. "Cryptographic Algorithms for Protection of Computer Data During Transmission and Dormant Storage," *Federal Register* **38**, No. 93 (May 15, 1973).
14. *Report of the Workshop on Cryptography in Support of Computer Security,* NBSIR 77-1291, Held at the National Bureau of Standards, September 21–22, 1976, National Bureau of Standards, U.S. Department of Commerce, Washington, D.C. (September 1977).
15. *Data Encryption Standard,* Federal Information Processing Standard (FIPS) Publication 46, National Bureau of Standards, U.S. Department of Commerce, Washington, D.C. (January 1977).
16. Davis, R. M., "The Data Encryption Standard in Perspective," *IEEE Communications Society Magazine* **16**, No. 6, 5–9 (1978).

17. Inman, B. R., "The NSA perspective on Telecommunications Protection in the Non-Governmental Sector," *Signal* **33**, No. 6, 7-13 (1979).

18. Konheim, A. G., Mack, M. H., McNeill, R. K., Tuckerman, B., and Waldbaum, G., "The IPS Cryptographic Programs," *IBM Systems Journal* **19**, No. 2, 253-283 (1980).

19. "With Data Encryption, Scents Are Safe at IFF," DP Dialogue, Data Processing Division, IBM Corporation, printed in *Computerworld* **14**, No. 21, 95 (1980).

20. "Data Encryption: Is It for You?," *EDP Analyzer* **16**, No. 12, 1-13 (1978).

21. *DES Modes of Operation,* Federal Information Processing Standards (FIPS) Publication 81, National Bureau of Standards, U.S. Department of Commerce, Washington, D.C. (1981).

22. ANSI X3.92-1981, *Data Encryption Algorithm,* American National Standards Institute, New York (December 31, 1980).

23. Proposed Federal Standard 1026, *Telecommunications: Interoperability and Security Requirements for Use of the Data Encryption Standard in the Physical and Data Link Layers of Data Communications,* General Services Administration, Washington, D.C., Draft (January 21, 1982).

24. Federal Standard 1027, *Telecommunications: General Security Requirements for Equipment Using the Data Encryption Standard,* General Services Administration, Washington, D.C. (April 14, 1982).

Other Publications of Interest

25. Parker, D. B., *Crime by Computer,* Scribner, New York, 1976.

26. Kahn, D., "Cryptology Goes Public," *Foreign Affairs* **58**, No. 1, 141-159 (1979).