Previous Chapter Previous Page Home Next page Next Chapter

SECTION 1

Cryptography

CHAPTER 1

The Data Encryption Standard
*Past and Future**

MILES E. SMID AND DENNIS K. BRANSTAD
National Institute of Standards and Technology

*First appeared in *Proceedings of the IEEE,* vol. 76, no. 5, pp. 550-559, May 1988. U.S. government work not protected by U.S. copyright.

The Data Encryption Standard (DES) is the first, and to the present date, only, publicly available cryptographic algorithm that has been endorsed by the U.S. government. This chapter deals with the past and future of the DES. It discusses the forces leading to the development of the standard during the early 1970s, the controversy regarding the proposed standard during the mid-1970s, the growing acceptance and use of the standard in the 1980s, and some recent developments that could affect the future of the standard.

1 THE BIRTH OF THE DES

1.1 The Development ot Security Standards

In 1972, the National Bureau of Standards (NBS), a part of the U.S. Department of Commerce, initiated a program to develop standards for the protection of computer data. The Institute for Computer Sciences and Technology (ICST), one of the major operating units of the National Bureau of Standards, had been recently established in response to a 1965 federal law known as the Brooks Act (PL89-306) that required new standards for improving utilization of computers by the federal government. Computer security had been identified by an ICST study as one of the high-priority areas requiring standards if computers were to be effectively used. A set of guidelines and standards were defined by the ICST that were to be developed as resources became available in computer security. The guidelines were to include areas such as physical security, risk management, contingency planning, and security auditing. Guidelines were adequate in areas not requiring interoperability among various computers. Standards were required in areas such as encryption, personal authentication, access control, secure data storage, and transmission because they could affect interoperability.

Standards come in different “flavors”: basic, interoperability, interface, and implementation.

1. ***Basic standards*** (also called “standards of good practice”) are used to specify generic functions (services, methods, results) required to achieve a certain set of common goals. Examples include standards for purity of chemicals, contents of food products, and in the computer field, structured programming practices.
2. ***Interoperability standards*** specify functions and formats so that data transmitted from one computer can be properly acted on when received by another computer. The implementation (hardware, firmware, software) or structure (integrated, isolated, interfaced layers) need not be specified in interoperability standards, since there is no intent of replacing one implementation or structure within a system with another.
3. ***Interface standards*** specify not only the function and format of data crossing the interface, but also include physical, electrical, and logical specifications sufficient to replace one implementation (device, program, component) on either side of the interface with another.
4. ***Implementation standards*** not only specify the interfaces, functions, and formats, but also the structure and the method of implementation. These may be necessary to assure that secondary characteristics such as speed, reliability, physical security, etc. also meet certain needs. Such standards are often used to permit component replacement in an overall system.

Each of the above types of standards was considered for the specification of the DES. A basic standard did not achieve telecommunications interoperability if different algorithms were selected by the communicating parties. Although an interface standard was desirable in some applications (e.g., data encryption on a RS-232C interface device) it would not be applicable in other applications (e.g., secure mail systems). An implementation standard was rejected because it would restrict vendors from using new technologies. Therefore, the DES was developed as an interoperability standard, requiring complete specification of basic function and format yet remaining independent of physical implementation.

1.2 Public Perception of Cryptography

Cryptography is a word that has been derived from the Greek words for “secret writing.” It generally implies that information that is secret or sensitive may be converted from an intelligible form to an unintelligible form. The intelligible form of information or data is called plaintext and the unintelligible form is called ciphertext. The process of converting from plaintext to ciphertext is called encryption and the reverse process is called decryption. Most cryptographic algorithms make use of a secret value called the key. Encryption and decryption are easy when the key is known, but decryption should be virtually impossible without the use of the correct key. The process of attempting to find a shortcut method, not envisioned by the designer, for decrypting the ciphertext when the key is unknown is called ***cryptanalysis.***

In the early 1970s, there was little public understanding of cryptography. Most people knew that the military and intelligence organizations used special codes or code equipment to communicate, but few understood the science of cryptography. The International Business Machines Corp. (IBM) initiated a research program in cryptography because of the perceived need to protect electronic information during transmission between terminals and computers and between computers (especially where the transmissions were to authorize the transfer or dispensing of money). Several small companies in the United States made cryptographic equipment for sale, much of it overseas. Several major companies made cryptographic equipment under contract to the U.S. government, but most such equipment was itself classified.

There was an interest in the mathematics of cryptography at several universities, including Stanford and MIT. Cryptographic algorithms were frequently based on mathematics or statistics and hence were often of interest to mathematicians. Making and breaking cryptographic algorithms was considered an intellectual challenge. However, there was only a limited market for expertise in cryptography outside the military and intelligence circles.

The NBS project in computer security identified a number of areas requiring research and the development of standards. A cryptographic algorithm that could be used in a broad spectrum of applications by many different users to protect computer data during transmission and storage was identified as a needed standard. A standard cryptographic algorithm was considered necessary so that only one algorithm needed to be implemented and maintained, and so that interoperability could be easily achieved. This led to the initiation of the NBS project in data encryption and the first solicitation for candidate algorithms.

1.3 The NBS–NSA–IBM Roles

The National Bureau of Standards initiated development of the DES when it published in the ***Federal Register*** of May 15, 1973, a solicitation for encryption algorithms for computer data protection. Responses to this solicitation demonstrated that there was an interest in developing such a standard, but that little technology in encryption was publicly available. NBS requested assistance from the National Security Agency (NSA) in evaluating encryption algorithms if any were received or in providing an encryption algorithm if none were received.

IBM had initiated a research project in the late 1960s in computer cryptography. The research activity, led by Dr. Horst Feistel, resulted in a system called LUCIFER [l]. In the early 1970s, Dr. W. Tuchman became leader of a development team in cryptographic systems at IBM. This development activity resulted in several publications, patents, cryptographic algorithms, and products. One of the algorithms was to become the Data Encryption Standard.

IBM submitted its cryptographic algorithm to NBS in response to a second solicitation in the ***Federal Register*** of August 27, 1974. NBS requested that the NSA evaluate the algorithm against an informal set of requirements and simultaneously requested that IBM consider granting nonexclusive, royalty-free licenses to make, use, and sell apparatus that implemented the algorithm. A great deal of discussion was conducted by NBS with both organizations in response to these requests.

On March 17, 1975, nearly 2 years following the first solicitation, NBS published two notices in the ***Federal Register.*** First, the proposed “Encryption Algorithm for

Computer Data Protection" was published in its entirety. NBS stated that it satisfied the primary technical requirements for the algorithm of a DES. It also notified readers to be aware that certain U.S. and foreign patents contain claims that may cover implementation and use of this algorithm and that cryptographic devices and technical data relating to them may come under the export control. The second notice contained a statement by IBM that it would grant the requested nonexclusive, royalty-free licenses provided that the Department of Commerce established the DES by September 1, 1976.

On August 1, 1975, NBS published in the ***Federal Register*** the fourth notice of a proposed Federal Information Processing Data Encryption Standard. Comments were requested from federal agencies and the public regarding the proposed standard. On October 22, 1975, Dr. M. Hellman sent his criticism of the proposed standard. His letter began, "Whit Diffie and I have become concerned that the proposed data encryption standard, while probably secure against commercial assault, may be extremely vulnerable to attack by an intelligence organization." He then outlined a "brute force" attack on the proposed algorithm, using a special-purpose "parallel computer using one million chips to try one million keys each" per second. He estimated the financial requirements to build such a machine to be twenty million dollars [2].

Because of the concern for adequate protection to be provided by the DES, NBS continued to evaluate the algorithm, the requirements for security in the private and public sectors, and the alternatives to issuing the standard. Finally, NBS recommended that the standard be issued and it was published on January 15, 1977. The standard included provisions for a review by NBS every 5 years.

2 THE DES CONTROVERSY

2.1 How Long Is Long Enough?

The DES security controversy forced consideration of basic security questions about how good is good enough and how long is long enough. Every practical security system must be evaluated with respect to security, costs (initial, operational, maintenance), and user "friendliness." These factors were studied in great depth during the evaluation of the proposed standard.

The effective key length of the DES is 56 binary digits (bits) and the straightforward "work factor" of the algorithm is 2^{56} (i.e., the number of keys that would have to be tried is 2^{56} or approximately $7.6 \mathbf{x} 10^{16}$). Hellman and Diffie argued that, in certain situations, a symmetric characteristic of the algorithm would cut this number in half and that on the average, only half of these would have to be tried to find the correct key. They also noted that increasing the key length by 8 bits would "appear to outstrip even the intelligence agencies' budgets" but that "decreasing the key size by 8 bits would decrease the cost, . . . making the system vulnerable to attack by almost any reasonable sized organization." It was thus argued that the length of the key was critical to the maximum security provided by the proposed standard.

2.2 S-Boxes and Trapdoors

The second criticism of the proposed standard was that of the fundamental design of the algorithm which is based on a set of eight fixed substitution tables, or S-boxes, that are used in the encryption and decryption processes. It was argued that, since the design criteria of the tables were not publicly available, the entries could have been selected in such a manner as to hide a “trapdoor.” The argument was that the people or organizations who selected the tables might be able to cryptanalyze the algorithm while everyone else could not.

2.3 Resolution

NBS, NSA, and IBM were the principals in the development of the Data Encryption Standard as noted above. Since NBS had initiated the development of the DES, NBS was responsible for assuring that the proposed standard met all of the requirements, and that it was acceptable to many potential users with a large number of applications. NBS continued to assess the requirements for the standard, analyze the security concerns regarding the proposed standard, and evaluate the costs and benefits of modifying or replacing the proposed standard. The principals involved in developing the proposed standard decided, after 2 years of evaluation, to rely on a public peer review process in order to make a final decision. Two workshops were organized by NBS; one on the mathematics of the algorithm to analyze the “trapdoor” concern [3], and one on the economic trade-offs of modifying the algorithm to increase its key length [4]. The designers, evaluators, implementors, vendors, and potential users of the algorithm, along with the vocal critics of the proposed standard, were invited to both workshops. A number of mathematicians were also invited to the mathematics workshop.

The workshops were extremely lively. The critics were given an opportunity to state their concerns to the audience. The designers stated that some of the design criteria were classified, but outlined many of the criteria used in the design. The evaluators stated the results of their evaluations. The implementors stated they needed a standard in order to justify implementation costs, and the users stated they wanted a resolution of the issue so that they could obtain effective cryptographic protection of their data.

The decision to publish the proposed standard without modification was made immediately following the workshop. There were no “trapdoors” identified in the algorithm. The potential users and vendors of the algorithm agreed that while the key could have been longer at little additional cost, it was considered adequate for their needs for l0-15 years. There was also concern that any change in the key length would make implementations of the algorithm unexportable to all potential markets. It was therefore recommended that the standard be reviewed every few years to evaluate its continued adequacy for meeting all of its intended applications and meeting all of its requirements. This recommendation has been fulfilled by NBS in 1983 and again in 1988.

3 ACCEPTANCE BY GOVERNMENT AND COMMERCIAL SECTORS

3.1 No Attack Demonstrated

Despite the controversy over the security of the Data Encryption Standard, it is the most widely accepted, publicly available, cryptoalgorithm today. And with the exception of the Rivest-Shamir-Adleman (RSA) public key algorithm, no other algorithm is even a significant contender. The DES has been accepted for two main reasons.

First, despite all the claims of discovered or imagined flaws, no one has demonstrated a fundamental weakness of the DES algorithm. In fact, the only seriously proposed attacks involve exhaustively testing keys until the correct key is found. This method is precisely what designers of cryptoalgorithms hope their adversaries will be forced to attempt. If the number of possible keys is sufficiently large to dissuade the attacker from attempting exhaustively testing keys, and no easier attack on the algorithm can be found, then the designer of the algorithm has succeeded in providing adequate security. Today, most security applications can be subverted for much less than the tens of millions of dollars required to break the DES.

Second, the DES has been accepted because of its endorsement by the federal government. No other publicly available algorithm has ever been endorsed by the U.S. government. Federal agencies are required to use DES for the protection of unclassified data, but the private sector has adopted DES as well because government endorsement implies an approved degree of security. Thus, the DES has become the most widely accepted mechanism for the cryptographic protection of unclassified data.

3.2 DES Validations

Since publishing the Data Encryption Standard, NBS has validated 45 (as of May 7, 1991) hardware and firmware implementations. Approximately three implementations are validated each year. The list of companies with validated chips is quite varied. It contains very small companies as well as many of the large U.S. electronics corporations. The implementations range from firmware programmable read-only memories (PROMs), which implement only the basic DES algorithm, to electronic chips that provide several different modes of operation running at speeds up to 45 million bits per second. The motivations of the companies vary as well. Some sell their implementations to other companies that embody the devices into cryptographic equipments; some of the companies embody the DES devices into equipment that they sell directly; and still others use their devices for their own internal security purposes with no intentions of offering security products for sale. Hardware implementations of the DES are widely available in the United States at prices under $100; DES encryption boards that can encrypt stored and transmitted data in a personal computer are available for under $1000; and stand-alone encryption units may be purchased for under $3000. No other public encryption algorithm can claim such availability.

The Data Encryption Standard requires that the DES algorithm be implemented in hardware (or firmware) for federal applications, but many individuals and corporations have programmed it in software. The number of software implementations is unknown. Reported maximum encryption speeds vary from 100,000 bit/sec on a VAX 780 to 20,000 bit/sec on a personal computer. In many applications, however, low cost is more important than maximum speed. Some vendors offer assembled versions of the DES free of charge, and NBS has provided Fortran and C language DES source listings for testing purposes. The cost of a software implementation depends mostly on the supporting software that is desired along with the algorithm.

3.3 DES Standards-Making Organizations

The widespread acceptance of the Data Encryption Standard is evident from the organizations that have produced DES-based standards. The belief that future communications and data storage systems will require cryptographic protection, and the additional belief that standards are necessary to establish common levels of security and interoperability, led five standards-making organizations to participate in the development of DES-based cryptographic standards. These organizations produce standards in many diverse fields, including security.

1. ***The*** American Bankers ***Association (ABA):*** The ABA develops voluntary standards related to financial matters for their own members. DES cryptography has had applications in both retail and wholesale banking. Generally speaking, retail banking involves transactions between private individuals and a financial institution, while wholesale banking involves transactions among financial institutions and corporate customers. Automatic teller machines and point-of-sale terminals identify customers by means of personal identification numbers (PINs) submitted by the customers at the time of the transaction, The DES is widely used to protect these numbers from disclosure and the information contained in the transactions from alteration. Wholesale electronic fund transfers of 2 million dollars are quite common. U.S. banks collectively transfer more than 400 billion dollars daily. The Clearing House Interbank Payments System (CHIPS) which processes 560,000 messages a week with a total dollar value of 1.5 trillion dollars, uses the DES to protect the messages from unauthorized modification.

The ABA has published a standard recommending the use of the DES whenever encryption is needed to protect sensitive financial data [5]. It has also published a standard for the management of cryptographic keys [6].

2. The American National Standards Institute (ANSI): The American National Standards Institute produces voluntary standards in many technical areas. Two committees within ANSI have been involved in developing DES-based cryptographic standards: Accredited Standards Committee (ASC) X3 deals with information processing systems and Accredited Standards Committee (ASC) X9 is responsible for financial services. The Computer and Business Equipment Manufacturers Association (CBEMA) is the secretariat for ASC X3 and the American Bankers Association is the secretariat for ASC X9. ASC X3 standards are published and copyrighted by ANSI while ASC X9 standards are published and copyrighted by the ABA.

Under each committee are subcommittees and working groups. The X3Tl (Data Encryption) subcommittee has standardized the DES as the Data Encryption Algorithm (ANSI X3.92) [7] and produced a Data Encryption Algorithm Modes of Operation Standard (ANSI X3.106) [8]. In the field of network security, X3Tl produced a standard for Information Systems-Data Link Encryption (ANSI X3.105) [9] which makes use of the Data Encryption Algorithm. X3Tl has developed draft standards for encryption at the Transport and Presentation layers of networks which conform to the Open Systems Interconnection Reference Model [10]. The further development of these standards is now taking place in the International Organization for Standardization.

The X9A3 (Financial Institution Retail Security) working group developed DES-based standards for the management and security of PINs (ANSI X9.8) [l11, and for the authentication of retail financial messages (ANSI X9.19) [12]. The PIN standard and the use of DES for PIN encryption has been in use for several years. The working group is now developing a key management standard which will provide for the secure distribution of cryptographic keys to the various terminals and host computers used in retail networks (ANSI X9.24) [13].

The X9E9 (Financial Institution Wholesale Security) working group developed DES-based standards for message authentication (ANSI X9.9) [14] and key management (ANSI X9.17) [15]. ANSI X9.17 and its international counterpart are currently the only standards that fully specify automated key distribution protocols. X9E9 is currently in the process of developing DES-based standards for encryption (ANSI X9.23) [161 and for secure personal and node authentication [17].

3. The General Services Administration (GSA): The GSA is responsible for the promulgation of federal procurement regulations. Prior to the passage of the Computer Security Act of 1987 [18], GSA was responsible for the development of federal telecommunications standards. GSA had delegated the responsibility for producing and coordinating telecommunications standards to the National Communications System (NCS). However, under the Computer Security Act of 1987, NBS has recently been given the responsibility for computer and related telecommunications standards.

NCS produced three DES-based standards: “Telecommunications: Interoperability and Security Requirements for Use of the Data Encryption Standard in the Physical and Data Link Layers of Data Communications” (Federal Standard 1026) [19], “Telecommunications: General Security Requirements for Equipment Using the Data Encryption Standard” (Federal Standard 1027) [20], and “Interoperability and Security Requirements for Use of the Data Encryption Standard with CCITT Group 3 Facsimile Equipment” (Federal Standard 1028) [21]. Federal Standard 1027 is the only public standard for securely implementing a cryptoalgorithm in electronic equipment. Until January 1, 1988, the National Security Agency endorsed products as conforming to the standard.

4. The International Organization for Standardization (ISO): IS0 has become increasingly involved in telecommunications security standards. In 1986 IS0 voted to approve the DES as an international standard called the DEA- 1. However, the approval of the DEA-1 led to a rethinking of the role that IS0 should play in the standardization of cryptography. A resolution was passed that IS0 should not standardize any cryptoalgorithms, and the IS0 Council approved a proposal that the DEA-1 should not progress to publication. As an alternative some IS0 members believe that IS0 should maintain a public registry of cryptoalgorithms. At a minimum, the registry would contain an agreed on name for each algorithm, thereby providing an international referencing capability.

ISO/TC-68/SC-2/WG-2 (International Wholesale Financial Standards) has produced a message authentication standard [22] and key management [23] standard. Both standards, which permit the use of the DES as well as other cryptoalgorithms, are highly compatible with the corresponding ANSI wholesale authentication and key management standards.

Currently, several IS0 groups are involved in developing standards that use cryptography as a mechanism for network security. The standards will provide for data confidentiality, data integrity, peer entity authentication, access control, key distribution, and digital signatures. It is expected that these standards will be compatible with a variety of cryptoalgorithms and applicable to open systems conforming to the Open Systems Interconnection (OSI) standards.

5. The National Bureau of Standards (NBS): Under the provisions of Public Law 89-306 and the Computer Security Act of 1987, the Secretary of Commerce is authorized to establish uniform federal automatic data processing standards. Within the

Department of Commerce, standards for computer security (and the protection of unclassified automatic data processing [ADP] data by various means, including the application of cryptography) are the responsibility of the Institute for Computer Sciences and Technology (ICST) of the National Bureau of Standards. The Computer Security Act of 1987 affirms and enhances NBS's responsibility for computer security standards and guidance.

NBS has published the Data Encryption Standard (Federal Information Processing Standard [FIPS] 46) [24], Guidelines for Implementing and Using the DES (FIPS 74) [25], DES Modes of Operation (FIPS 81) [26], and Computer Data Authentication (FIPS 113) [27]. These standards have been used as the basis of standards by other standards-making organizations. Additionally, NBS hosts the Workshop for OSI Implementors and chairs its Special Interest Group on Security. This group is selecting which security options in the OSI architecture will be initially implemented.

3.4 Validation and Certification

While cryptographic standards are most useful in defining accepted security methods, often there are no means for determining whether a particular product or implementation does, in fact, conform to a given standard. To satisfy a need for such means, the Department of Treasury, the National Security Agency, and the National Bureau of Standards have developed interrelated validation programs for certain cryptographic systems.

When the Data Encryption Standard was published, NBS felt that it must establish a program for validating hardware implementations. A set of tests were devised so that any device passing all tests was very likely to correctly implement the standard. The success of the program has been previously discussed in this chapter.

Federal Standard 1027 placed additional requirements on equipments beyond the basic DES algorithm. The DES had to be securely embodied into an enclosure with physical access controls including locks and alarms, and the equipment had to be frequently tested for proper operation so that failures would not cause the compromise of sensitive data. The National Security Agency has endorsed at least 32 vendor equipments as properly implementing FS 1027.

In 1984, the U.S. Department of Treasury wrote a policy directive requiring that the Department's electronic funds transfer (EFT) messages be properly authenticated in all new systems immediately and in all systems by 1988 [28]. This policy was affirmed by Treasury Secretary James Baker III on October 2, 1986 [29]. The Treasury also decided to certify vendor authentication devices and wrote the criteria that such devices must meet [30]. Such equipments must implement the DES and conform to FS 1027. NBS and the NSA have assisted Treasury with its certification program.

As a part of this cooperative effort, NBS agreed to develop a validation system which would test conformance of systems to the FIPS 113 and ANSI X9.9 authentication standards. The tests are automated so that a product vendor can call a remote bulletin board system at NBS and validate the product over the telephone. To date, 29 remote validations, including two transatlantic validations, have been performed (as of May 7, 1991). A subsequent security examination is required for Treasury certification, but passing the NBS validation gives the vendor a strong indication that the product functions in accordance with commercial and federal standards. NBS is now developing a key management validation program which will test vendor products for conformance to the DES-based ANSI wholesale key management standards (ANSI X9.17). The Department of Treasury will use the results of the NBS validation program when certifying the key management capabilities of products intended for Treasury applications.

Since the Data Encryption Standard is a federal standard, the federal government has established validation and certification programs to ensure product conformance. No other publicly available algorithm has been validated to this extent.

3.5 Increased Public Knowledge of Cryptography

After the publication of the Data Encryption Standard in 1977 it quickly became clear that there was much more to the implementation of a secure cryptographic system than a high-quality cryptographic algorithm. It can be argued that the development of a secure cryptoalgorithm is an essential tool, but only one building block, of a secure data system. The above mentioned organizations have developed data security standards for security applications. Their goal was to achieve a common level of security and interoperability. While this goal was not always attained, great strides have been achieved as a result of their efforts.

The efforts of the standards-making organizations have also served a purpose far beyond the actual standards that were developed. Standardization, validation, and certification programs greatly increased the public's interest in cryptography and raised the level of confidence that it could be a cost-effective solution to practical security problems. There is still much to decide about the best use of cryptography, but there is now no doubt that it will be used far beyond its original military applications.

4 APPLICATIONS

The DES is a basic building block for data protection. The algorithm provides the user with a set of functions each of which transforms a 64-bit input to a 64-bit output. The user selects which one of over 70 quadrillion transformation functions is to be used by selecting a particular 56-bit key. Anyone knowing the key can calculate both the function and its inverse, but without the key it is infeasible to determine which function was used, even when several inputs and outputs are provided. Since an independent set of 70 quadrillion functions would be impossible to support, the DES provides a simple means of simulating the family of functions.

4.1 General Applications

The basic DES algorithm can be used for both data encryption and data authentication.

1. ***Data Encryption:*** It is easy to see how the DES may be used to encrypt a 64-bit plaintext input to a 64-bit ciphertext output, but data are seldom limited to 64 bits. In order to use DES in a variety of cryptographic applications, four modes of operation were developed: electronic codebook (ECB); cipher feedback (CFB); cipher block chaining (CBC); and output feedback (OFB) [26] (Figs. l-4). Each mode has its advantages and disadvantages. ECB is excellent for encrypting keys; CFB is typically used for encrypting individual characters; and OFB is often used for encrypting satellite communications. Both CBC and CFB can be used to authenticate data. These modes of

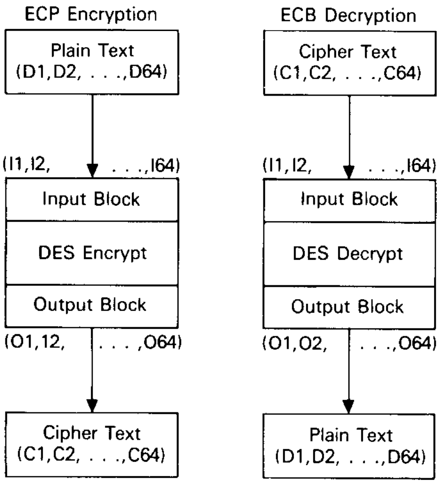

Figure 1 Electronic codebook (ECB) mode.

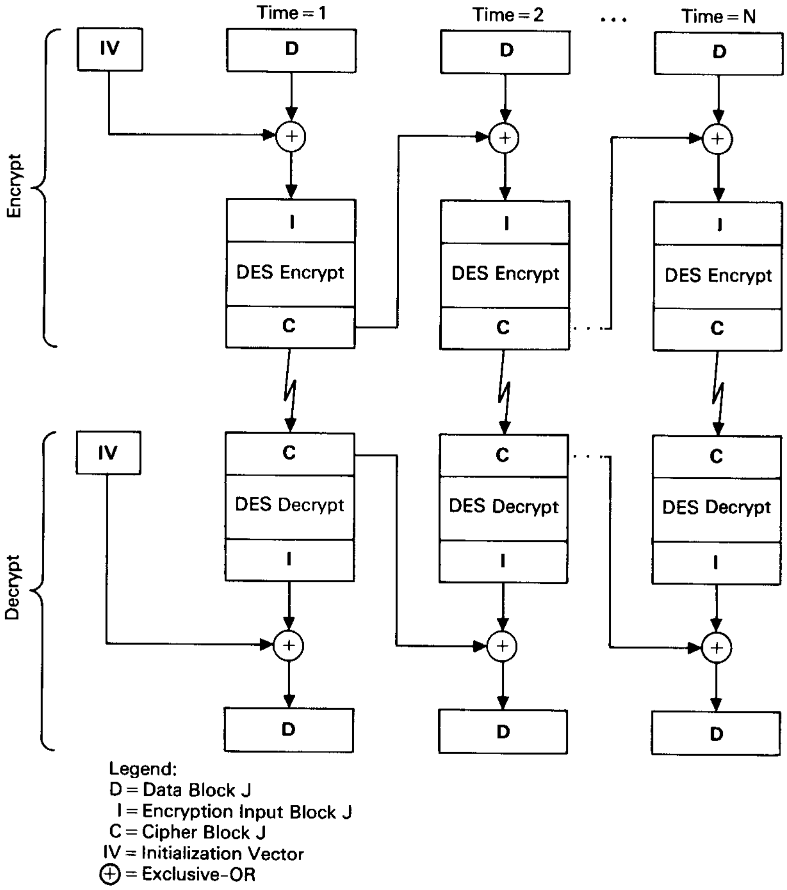

Figure 2 Cipher block chaining (CBC) mode.

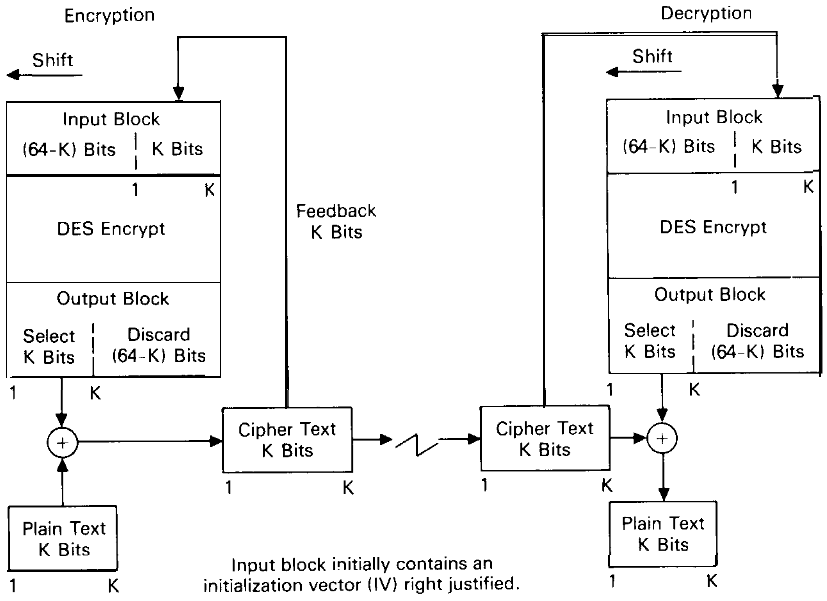

Figure 3 k-bit cipher feedback (CFB) mode.

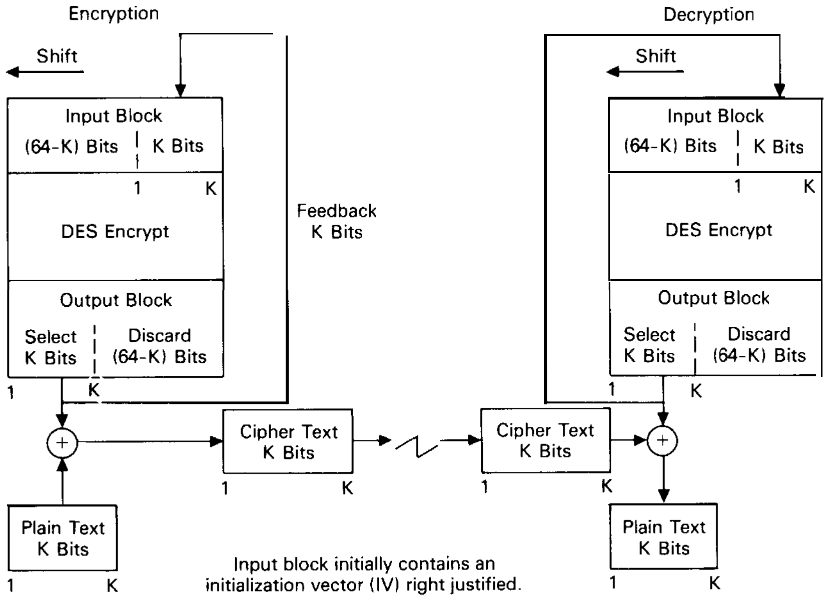

Figure 4 k-bit output feedback (OFB) mode.

operation permit the use of DES for interactive terminal to host encryption, cryptographic key encryption for automated key management applications, file encryption, mail encryption, satellite data encryption, and other applications. In fact, it is extremely difficult, if not impossible, to find a cryptographic application where the DES cannot be applied.

2. Data Authentication: Originally the Data Encryption Standard was intended for the encryption and decryption of computer data. However, its application has been extended to data authentication as well. In automated data processing systems it is often not possible for humans to scan data to determine if the data have been modified. Examination may be too time consuming for the vast quantities of data involved in modern data processing, or the data may have insufficient redundancy for error detection. Even if human scanning were possible, the data could have been modified in such a manner that it would be very difficult for the human to detect the modification. For example, “do” may have been changed to “do not” or “$1900” may have been changed to “$9100”. Without additional information the human scanner could easily accept the altered data as authentic. These threats may still exist even when data encryption is used. It is therefore desirable to have an automated means of detecting both intentional and unintentional modifications to data. Ordinary error detecting codes are not adequate because, if the algorithm for generating the code is known, an adversary can generate the correct code after modifying the data. Intentional modification is undetectable with such codes. However, DES can be used to produce a cryptographic checksum that can protect against both accidental and intentional, but unauthorized, data modification. NBS Standard for Computer Data Authentication (FIPS 113) [27] describes the process. Essentially the data are encrypted using either the cipher feedback or the cipher block chaining mode which yields a final cipher block that is a function of all the plaintext bits. The plaintext message may then be transmitted with the computed final cipher block used as the cryptographic checksum.

3. Data Encryption and Authentication: The same data may be protected by both encryption and authentication. The data are protected from disclosure by encryption and modification is detected by authentication. The authentication algorithm may be applied to either the plaintext or the cipher. In most financial applications where both encryption and authentication are implemented, authentication is applied to the plaintext.

4.2 Specific Applications

1. ***Data Storage and Mail Systems:*** Encryption and authentication may be used to protect data stored in computers. Many computer systems encrypt passwords in a one-way fashion for storage in the computer memory. When a user signs on the computer and enters the password, it is encrypted and compared with the stored value. If the two encryptions are equal the user is permitted access to the computer; otherwise access is denied. The encrypted password is often created by using DES; setting the key equal to the password and the plaintext equal to the user’s identity. A Fortran program for implementing this function is given in the NBS Standard for Password Usage (FIPS 112) [31].

The DES can also be used to encrypt computer files for storage. NBS Special Publication 500-54 [32] describes a key notarization system which may be integrated into computer systems to protect files from undetected modification and disclosure, and to provide a digital signature capability using the DES. Users have the capability of exercising a set of commands for key management as well as for data encryption and authentication functions. The facilities perform notarization which, on encryption, seals a key or password with the identities of the transmitter and intended receiver. Thus, in order to decrypt a message, the receiver must be authenticated and must supply the correct identity of the transmitter. This notarization technique is used in ANSI standard X9.17 to protect against key substitutions which could lead to the compromise of sensitive data.

The key notarization system that incorporates the DES may also be used in conjunction with a mail system to provide for secure mail. A cryptographic header that contains the information necessary to decrypt and authenticate a mail file is automatically appended to the file that is transmitted to the receiver. The receiver may then decrypt and authenticate the file in a near transparent manner.

2. Electronic Funds Transfers (Retail and Wholesale): Perhaps the most significant use of the DES is for the protection of retail and wholesale electronic funds transfer messages. The retail and wholesale financial communities have developed standards for the authentication of EFT messages (ANSI X9.9 and ANSI X9.19), and these efforts have led to encryption (ANSI X9.23 Draft) and key management (ANSI X9.17 and ANSI X9.24 Draft) standards. DES is used in automatic teller machines, point of sale terminals, workstations, and host computers. The data that it protects range from a $50 charge to a multi-million-dollar transfer. The flexibility of the basic DES algorithm permits its use in a wide variety of EFT applications. The standards that have been developed for U.S. EFT applications are now being developed into international standards in the IS0 community. Therefore, these authentication, encryption, and key management techniques will be used worldwide.

The U.S. government is responsible for transferring billions of dollars daily. In order that these transfers be secure, the Department of Treasury initiated its (previously cited) policy on the authentication of EFT messages. The Federal Reserve Bank is cooperating with the Treasury to insure that this policy is successful. One system, which the Treasury is considering, makes use of hand-held tokens that contain DES keys that are generated for a particular individual. The token is used to supply a key that authenticates an EFT message containing the individual’s identity. This authenticated message, containing the individual’s identity, is the electronic substitute for a signed paper document.

3. Electronic Business Data Interchange: Large corporations are now in the process of automating their business transactions to reduce costs and increase efficiency. Business transactions will be accomplished via electronic means rather than by traditional paper-based systems, and ANSI Accredited Standards Committee Xl2 (Electronic Business Data Interchange) is now in the process of developing the formats that will be used for these communications. Electronic transmissions among buyer, seller, and banker will have to be protected from modification and eavesdropping. In most cases cryptography provides the only effective mechanism for providing such protection.

Electronic business data interchange will incorporate several DES-based standards [33-34]. ANSI X9.9 will provide protection against unauthorized modification and replay; the methods of draft ANSI Standard X9.23 will prevent unauthorized disclosure; and the secure generation, distribution, and storage of DES keys will be accomplished using the techniques specified in ANSI Standard X9.17. Currently General Motors and seven associated banks are using the method specified in these standards to protect their business transactions.

5 NEW ALGORITHMS

5.1 Forces for New Algorithms

From its initial specification, the Data Encryption Standard was intended to be a publicly known algorithm. Previously, most cryptographic algorithms fell into one of three categories: outdated algorithms developed during the Second World War, proprietary algorithms known only to the vendors who designed them, and classified government algorithms. Therefore, commercial and nonclassified government users did not have confidence that the algorithms available to them offered a reasonable level of security. NBS developed the DES to provide a high-quality, modern cryptoalgorithm that could be used to protect unclassified sensitive data.

In addition, the DES was intended to be widely available. DES has been published, dissected, and analyzed in the open literature. It can be built and used without a clearance or license (in the United States). It can be implemented in hardware, firmware, or software by anyone from a large corporation to a private individual.

Making a cryptographic algorithm publicly known has its disadvantages as well. Even though the DES is designed to be secure as long as the secret key is kept secret, algorithms that are kept secret can make the attacker's task more difficult since the algorithm often has to be deduced before the algorithm can be broken. Also, if a known algorithm becomes popular and is widely used, as is the case with the DES, it becomes a more attractive target for the attacker. Since the potential payoff is greater, the attacker may be willing to put forth an increased effort in breaking the algorithm.

On the other hand, one should not put too much value into the secrecy of the algorithm. First of all, poorly designed secret algorithms can often be deduced by the attacker. Consider, for example, the recent article in which five secret algorithms were easily recovered and broken [35]. Second, algorithms that are themselves secret are usually compromised (i.e., disclosed) sooner or later. For this reason, governments design their classified algorithms assuming the details of the design have been, or will be, compromised.

Since the DES has been publicly known for more than 10 years and since it is becoming very widely used, the National Security Agency (NSA) has decided to develop new algorithms. These algorithms will provide the cryptosecurity for the program discussed in the following section.

5.2 CCEP: The New Way of Doing Business

In 1984, the NSA initiated the Commercial COMSEC Endorsement Program (CCEP) which was intended by NSA to provide cryptographic algorithms that would eventually replace the DES [36]. NSA has stated that in 1988 it would no longer endorse equipments as complying with Federal Standard 1027, and that CCEP would provide government-endorsed cryptographic equipments [37]. Two types of cryptographic equipment are intended by NSA to be produced: type 1 and type 2. Type 1 equipment would protect classified data while type 2 equipment is intended by NSA to replace DES for the protection of unclassified data. The CCEP differs from the Federal Standard 1027 endorsement program in three respects.

1. The cryptoalgorithms would be designed only by NSA.

2. The cryptoalgorithms would not be made public. A protective coating will be used on electronic chip implementations to prevent reverse engineering.
3. The manufacturers of CCEP products and NSA would follow a seven-step process leading to product production: initial contact; program decision (approval); memorandum of understanding and transfer of technology by NSA; memorandum of agreement and product specification; program execution and product development and evaluation; endorsement; and production.

NSA's intent of the CCEP is that less expensive and technologically more sophisticated products will be produced as a result of an increased market base (both government and commercial) and the technical guidance provided by the NSA.

5.3 Unresolved Issues

The CCEP program still has several unresolved issues.

1. Since vendors permitted to enter the program must meet certain criteria, competition is restricted. Restricted competition can lead to higher customer costs.
2. Since the CCEP algorithms are secret and their implementation is restricted to vendors participating in the program, software implementations that do not lend themselves to the physical security provided by the protective coating would defeat the secrecy of the algorithm and therefore would not be permitted.
3. Since CCEP algorithms are secret and their implementation by foreign manufacturers will likely be restricted, end-to-end cryptography for many international security applications will be impossible. Future international networks may require cryptographic gateways between countries where the data are translated from the cryptographic protection of one country to the cryptographic protection of the other. In such networks, end users would have to be satisfied that their data remained secure within these gateways.
4. It is not clear whether the user will be able to select the key or if the user will have to use a key provided by NSA.
5. Since sophisticated cryptography and highly secure implementations often result in increased costs, the number of customers is usually reduced which in turn increases the cost of individual equipments.

It is still too early to determine whether the CCEP will be successful in meeting its goals, especially in unclassified government applications and in the commercial sector.

6 DES: THE NEXT DECADE

6.1 Renewing DES for Another 5 Years

On March 6, 1987, NBS published in the ***Federal Register*** a request for comments on the second Five Year Review of the Data Encryption Standard. Three alternatives were suggested for consideration.

1. Reaffirm the standard for another 5 years. The National Bureau of Standards would continue to validate equipment that implements the standard. The DES would continue to be an approved method for protecting unclassified computer data against unauthorized modification or disclosure.
2. Withdraw the standard. The National Bureau of Standards would no longer continue to support the standard. Organizations could continue to utilize existing equipment that implements the standard, and nongovernment organizations could continue to develop new implementations as desired.
3. Revise the applicability of the standard. The applicability statement of the standard would be changed to specify certain uses, such as using the standard for protecting electronic funds transfers. Proposed technical changes to the algorithm will not be considered during this review.

Thirty-three comments were received; 12 were from federal agencies and the remainder were from the private sector. The federal agency responses were often at the department level, and the private sector responses included comments from industry organizations such as the Computer and Business Equipment Manufacturers Association and the American Bankers Association. Thirty-one comments supported the reaffirmation of the standard for another 5 years. One organization stated that it had no comments but did not oppose reaffirmation, and one organization recommended that the DES be modified to apply only to the protection of financial transactions.

Many of the comments pointed out that the DES is widely available as a commercial product, that it is used extensively by both commercial and government organizations for a variety of applications extending far beyond financial transactions, and that no adequate alternative currently exists. Withdrawal of the standard or the limitation of it to financial transactions would leave many organizations without adequate protection for their information.

NBS reviewed all comments, and made its recommendation to the secretary of commerce. After considering all available information, the secretary of commerce reaffirmed the standard, in its present form, for another 5 years. The standard will be reviewed again beginning on or before January 1992.

Waivers will be considered for devices certified by the National Security Agency as complying with its commercial COMSEC Endorsement Program when such devices offer equivalent cost and performance features as compared to devices conforming with the DES.

6.2 Government Use

The DES is now a basic security mechanism employed by several government organizations. For example, the Department of Energy has more than 30 active networks using DES devices, and the Justice Department is in the process of installing 20,000 DES radio units. It is likely that the DES will continue to provide protection for network communications, stored data, passwords, and access control systems.

6.3 Commercial and Government Financial Applications

Many commercial and certain government applications have already committed to the DES. DES is the basis of the Department of the Treasury's Electronic Funds Transfer program, and the Federal Reserve System uses DES to encrypt connections between depository financial institutions and Federal Reserve banks. In addition, many financial and electronic business data applications already use DES and are unlikely to change for some time.

6.4 Gradual Progression of New Security Devices

In the past, the cryptography industry has not experienced rapid growth. Indications are that the interest and commitment to security by U.S. corporations is increasing and therefore the market for security products will increase as well. It is important that new products be developed that can offer cost, performance, and security advantages. However, it is also important to make use of existing technologies. Since the DES offers a substantial security improvement to the vast majority of government and commercial data security applications, sensitive data should not be left unprotected while waiting for future cryptographic systems.

7 CONCLUSIONS

As we move toward a society where automated information resources are increasingly shared, cryptography will continue to increase in importance as a security mechanism. Electronic networks for banking, shopping, inventory control, benefit and service delivery, information storage and retrieval, distributed processing, and government applications will need improved methods for access control and data security. The DES algorithm has been a successful effort in the early development of security mechanisms. It is the most widely analyzed, tested, and used cryptoalgorithm and it will continue to be for some time yet to come. But perhaps the most important contribution of the DES is that it has led us to other security considerations, beyond the algorithm itself, that must be made in order to have secure computer systems and networks.

REFERENCES

[l] H. Feistel, “Cryptography and computer privacy,” ***Sci. Amer., vol. 228,*** no. 5, pp. 15-23, May 1973.

[2] W. Diffie, M. Hellman, “Exhaustive cryptanalysis of the NBS data encryption standard,” ***Computer,*** pp. 74-78, June 1977.

[3] D. Branstad, J. Gait, and S. Katzke, “Report on the workshop on cryptography in support of computer security”, Sept. 21-22, 1976, NBSIR-771291, Sept. 1977.

[4] “Report of the workshop on estimation of significant advances in computer technology,” NBSIR 76-1189, National Bureau of Standards, Dec. 1976.

[5] “Management and use of personal identification numbers,” ABA Bank Card Standard, Aids from ABA, Catalog no. 207213, 1979.

[6] “Key management standard,” Document 4.3, American Bankers Association, Washington, DC, 1980.

[7] “American national standard for data encryption algorithm (DEA)” ANSI X3.92-198 1, American National Standards Institute, New York.

[8] "American national standard for information systems-Data encryption algorithm-Modes of operation," ANSI X3.106-1983, American National Standards Institute, New York.

[9] "American national standard for information systems-Data link encryption," ANSI X3.105-1983, American National Standards Institute, New York.

[10] "Information processing systems--Open systems interconnection-Basic reference model ,' ' IS 7498-1984, International Organization for Standardization, Geneva, Switzerland.

[11] "American national standard for personal identification number (PIN) management and security," ANSI X9.8-1982, American Bankers Association, Washington, DC.

[12] "American national standard for retail message authentication," ANSI X9.19-1985, American Bankers Association, Washington, DC.

[13] "Draft proposed American national standard for retail key management," ANSI X9.24-1988, American Bankers Association, Washington, DC.

[14] "American national standard for financial institution message authentication (wholesale)," ANSI X9.9-1986 (Revised), American Bankers Association, Washington, DC.

[15] "American national standard for financial institution key management (wholesale)," ANSI X9.17-1985 (Revised), American Bankers Association, Washington, DC.

[16] "American national standard for financial institution message encryption," ANSI X9.23-1988, American Bankers Association, Washington, DC.

[17] "American national standard for financial institution sign-on authentication for wholesale financial transactions," ANSI X9.26-1990, American Bankers Association, Washington, DC.

[18] Computer Security Act of 1987, PL 100-235.

[19] "Telecommunications: Interoperability and security requirements for use of the data encryption standard in the physical and data link layers of data communications," Federal Standard 1026, General Services Administration, Washington, DC, Jan. 1983.

[20] "Telecommunications: General security requirements for equipment using the data encryption standard," Federal Standard 1027, General Services Administration, Washington, DC, Apr. 1982.

[21] "Interoperability and security requirements for use of the data encryption standard with CCITT group 3 facsimile equipment," Federal Standard 1028, General Services Administration, Washington, DC, Apr. 1985.

[22] "Banking-Requirements for message authentication (wholesale)," DIS 8730, Association for Payment Clearing Services, London, July 1987.

[23] "Banking-Key management (wholesale)," DIS 8732, Association for Payment Clearing Services, London, Dec. 1987.

[24] "Data encryption standard (DES)," National Bureau of Standards (U.S.), Federal Information Processing Standards Publication 46, National Technical Information Service, Springfield, VA, Apr. 1977.

[25] "Guidelines for implementing and using the NBS data encryption standard," National Bureau of Standards (U.S.), Federal Information Processing Standards Publication 74, National Technical Information Service, Springfield, VA, Apr. 1981.

[26] "DES modes of operation," National Bureau of Standards (U.S.), Federal Information Processing Standards Publication 81, National Technical Information Service, Springfield, VA, Dec. 1980.

[27] "Computer data authentication," National Bureau of Standards (U.S.), Federal Information Processing Standards Publication 113, National Technical Information Service, Springfield, VA, May 1985.

[28] "Electronic funds and securities transfer policy," Department of the Treasury Directives Manual, Chapter TD 81, Section 80, Department of the Treasury, Washington, DC, Aug. 16, 1984.

[29] "Electronic funds and securities transfer policy-Message authentication and enhanced security," Department of the Treasury Order number 106-09, Department of the Treasury, Washington, DC, Oct. 2, 1986.

[30] "Criteria and procedures for testing, evaluating, and certifying message authentication devices for federal E.F.T. use," United States Department of the Treasury, May 1, 1985.

[31] "Password usage," National Bureau of Standards (U.S.), Federal Information Processing Standards Publication 112, National Technical Information Service, Springfield, VA, May 1985.

[32] "A key notarization system for computer networks," National Bureau of Standards (U.S.), Special Publication 500-54, National Technical Information Service, Springfield, VA, Oct. 1979.

[33] "American standards committee Xl2 draft standard for trial use for managing electronic data interchange, cryptographic service, message transaction set (815)," ANSI X12.42-1990, Data Interchange Standards Association, Inc., Alexandria, VA.

[34] "American standards committee Xl2 draft standard for trial use for managing electronic data interchange, security structures," ANSI X12.58-1990, Data Interchange Standards Association, Inc., Alexandria, VA.

[35] M. Kochanski, "A survey of **data** insecurity package," ***Cryptologia,*** pp. 1-15, Jan. 1987.

[36] C. Barker, "An industry perspective of the CCEP," presented at the 2nd Annual AIAA Computer Security Conf. Proceedings, Dec. 1986.

[37] Letter from H. E. Daniels, Jr., NSA Deputy Director for Information Security, to Datapro Research Corporation, Dec. 23, 1985.