Appendix C
The Data Encryption Standard

Background on Encryption

The algorithms currently in use to encrypt (or encipher) messages and data are based on sophisticated mathematics and are usually implemented using computers or dedicated microprocessors. Nevertheless, their underlying objective is quite simple and can be traced back to antiquity:[1] to transform a message (or data) into a form that cannot be understood by anyone who does not possess special knowledge—the "key' '-that unlocks the cipher and reveals the message.

Encryption takes a plaintext message and transforms it into a ciphertext (or encrypted) message using an encryption procedure and an encryption key. Thus, if P is the plaintext, E is the encryption procedure, and K. is the encryption key, then the ciphertext, C, can be expressed mathematically as:

$$C = E(K., P).$$

The inverse process, decryption, given by D, transforms the ciphertext back into plaintext using the decryption key, K_d:

$$P = D(K_d, C).$$

In many encryption algorithms, the encryption and decryption keys are identical (Kd = KJ and can be represented simply by K.[2] The algorithm that is used in the Data Encryption Standard (DES) uses one key, K, which is called a "private key" because the key is kept secret to ensure that outsiders cannot use it to read enciphered messages.[3]

The strength of an encryption algorithm (or cipher) can be measured by its "work factor' '–the amount of effort (number of steps and time) required to "break" the cipher and read any encrypted message without the key. An algorithm's strength can be described in terms of the kinds of "attacks" (attempts to break the cipher) it can withstand. The most difficult type of attack to withstand is called the "chosen plaintext attack. In this type of attack, an adversary is able to submit any amount of plaintext to the encryption algorithm and obtain the corresponding ciphertext. The (P,C) pairs can then be used to try to determine the secret key and break the cipher.

An encryption scheme that is used as a standard should be able to withstand chosen plaintext attacks, especially if the algorithms E and D are published as part of the standard. The strength of an encryption scheme is determined by the algorithm itself and by the complexity of the secret information (in the case of modern encryption schemes, by the length of the key). In general, longer keys (i.e., more digits or binary bits) correspond to a stronger cipher, but this is not necessarily the case: for a given algorithm, a shorter key weakens the cipher, but for different algorithms, one using a shorter key may be stronger overall than one using a longer key length.

The strength of any encryption scheme rests fundamentally on the integrity of the key(s) used. Therefore, proper key management is fundamental to the security provided by any encryption scheme or cipher.[4]

Evolution of the Data Encryption Standard

The Solicitation for a Standard

No single event or act of Congress led the Federal Government to adopt a published encryption standard for Federal agencies to protect their unclassified computer data and communications. Instead, a number of developments and concerns came together in the 1960s and 1970s that caused many people in and out of Government to conclude that a common means of protecting the Government's electronic information was needed.

One of these developments was the Brooks Act of 1965 (Public Law 89-306), which authorizes the National Bureau of Standards (NBS) to develop standards governing the purchase and use of computers by the Federal Government, to do research supporting the development of these standards, and to assist Federal agencies in implementing them. At the same time there was an increasing interest in ensuring the confidentiality and security of the Federal Government's computer files containing data on individual citizens.[5] Addition-

[1] See, for example, David Kahn: *The Codebreakers: The Story of Secret Writing* (New York, NY: The MacMillan Co., 1967).

[2] These are called symmetric encryption algorithms. Asymmetric ciphers also exist, such as the "public-key" algorithms. (See the discussions in ch. 4 and app. I).)

[3] See R.C. Summers, "An overview of Computer Security," *IBM Systems Journal,* vol. 23, No. 4, 1984, pp. 309-325.

[4] See the discussion of kev management in ch. 4.

[5] These concerns were addressed in the privacy Act of 1974, ‘or example. For more background on DES, see: U.S. Senate Select Committee on Intelligence. "Unclassified Summary: Involvement of NSA in the Development of the Data Encryption Standard" (Staff Report), 98th Cong., 2d sess., April 1978.

ally, electronic transactions, such as fund transfers, were beginning to proliferate both within the Federal Government and in the private sector.

These trends gave impetus to growing concerns for the security of Federal electronic information and transactions. A consensus developed among computer security researchers at NBS and the National Security Agency (NSA) that a technical means should be developed for safeguarding them against accidental error as well as from assaults by organized crime. At the time, they anticipated that the useful lifetime of this safeguard technology would be about 30 years—until the late 1990s.[6]

NBS initiated a study in 1968 to evaluate the Federal Government's computer security needs. As a result, NBS decided in 1972 to develop a governmentwide standard for encrypting unclassified Government data using an encryption algorithm to be published as a public standard. NBS initiated a computer security program within its Institute for Computer Sciences and Technology (ICST) in mid-1972. In early 1973, NBS and NSA staff met to discuss the encryption project. Throughout the development of the standard, NBS made use of NSA's recognized expertise, including the evaluation of algorithms proposed for the standard. Also, some technical personnel left NSA and joined NBS during the early 1970s to staff the latter's new computer security program. A chronology of DES development, provided by NBS, is shown in table 15,

On May 15, 1973, NBS issued a solicitation through the *Federal Register* for interested parties to submit algorithms for possible consideration as a data encryption standard. There were few responses; none were considered suitable. A second solicitation was issued on August 27, 1974. IBM responded to the second solicitation; its algorithm eventually became the Data Encryption Standard (DES).

IBM had already done considerable work developing encryption algorithms. Prior to the solicitation for DES, IBM had developed and patented a 64-bit Cash Issuing Algorithm for safeguarding financial transactions and a 128-bit encryption algorithm called Lucifer.[7] As part of the patenting process, IBM's algorithms were submitted to NSA for review to determine whether or not the algorithms should be classified. NSA chose not to classify the algorithms and suggested to IBM that one of them, with some modification, should be submitted to NBS.

This step in the process has given rise to a great deal of controversy over the years. Although the algorithm that IBM submitted to NBS was exactly that which was published later as the Data Encryption Standard, this algorithm differed from the original IBM algorithm in a couple of fundamental ways. These changes were made by IBM on the advice of NSA, which later led to questions as to whether NSA had "tampered' with the algorithm or weakened it in some way, perhaps creating a "trapdoor" that NSA could spring. First, the key length was shortened to 56 bits. Second, changes

"I), Branstad.NBSICST. Private communication with OTA staff, Aug. 6, 1986.

'For a discussion of Lucifer and a description of the algorithm. see: Horst Feistel, "Cryptography and Computer Privacy," *Scientific American, vol.* 228, No.5, May 1973, pp. 15-23.

Table 15.—Chronology of DES Development (major Federal agency events)

Event	Date
. NBS identifies need for computer security standards,	August 1971
• NBS initiates program in computer security	July 1972
• NBS meets with NSA on encryption project	February 1973
Ž NBS publishes request for encryption algorithms	May 1973
. NSA reports no suitable algorithms were submitted	December 1973
. NBS publishes second request for algorithms	August 1974
• NSA reports one submitted algorithm is acceptable	October 1974
• NSA approves publication of proposed algorithm	January 1975
• DOJ approves publication of proposed algorithm	February 1975
. NBS publishes proposed algorithm for comment	March 1975
. NBS publishes proposed DES for comment	August 1975
Ž NBS briefs DOJ on competition issues	February 1976
. NBS holds workshop on technology concerning DES.	August 1976
. NBS holds workshop on mathematical foundation of DES	September 1976
Ž DOC approves DES as a FIPS	November 1976
• NBS publishes DES as FIPS PUB 46	January 1977

SOURCE National Bureau of Standards, circa 1978 were made in the internal structure of the substitution functions—often referred to as the “S-boxes’ —contained within the algorithm.[8]

In response to these concerns, NSA publicly stated that the reduced key size was sufficient for use in unclassified applications and, furthermore, that the IBM algorithm proposed for the data encryption standard was “to the best of their knowledge, free of any statistical or mathematical weakness. “g However, it was difficult for individuals outside of NBS, NSA, or IBM to independently substantiate (or refute) these statements. At the request of NSA, IBM had not disclosed all of the design criteria used in the creation of the candidate algorithm-in particular, those resulting from NSA’s testing and evaluation of the original algorithm and the criteria that had been used to select the modified S-boxes and shorter key length. Thus, although the proposed DES was published for comment, not all of the evaluative criteria that has been used in developing the algorithm were made public.

Comments on the Proposed Standard

Comments on the proposed standard were solicited in the Federal *Register* on March 17 and August 1, 1975, and in an August 1, 1975 letter sent to all Federal Information Processing Standards points of contact in Federal agencies. ’” NBS prepared an analysis of the comments from the three solicitations.[11] According to NBS, “all responses have been carefully considered and changes made to the standard where appropriate. However, no changes have been made to the algorithm itself and no substantive changes have been made to the standard which would warrant further solicitation for comments. ”[12] (See box F.)

One of the specific recommendations contained in the comments was that only hardware implementations should be considered. In response, NBS stated that “hardware is the only recommended implementation.[13] Nevertheless, several software implementations of DES have been developed by vendors for use by the private sector;

Box F.–Data Encryption Standard Summary of General Concerns

The following is a summary of the substantive general concerns about the proposed Data Encryption Standard stated in the comments received by NBS:

1. Computer equipment and related data processing equipment not based on a 64-bit architecture will be placed at a competitive disadvantage (A2, A3, A4, A5, A9, A10, B2, B5, B7, B10),
2. Certain types of communication systems may be degraded to a significant degree (Al, A2, A3, A4, A5, A10, All, B2, B4, B5, B9).
3. The proposed algorithm is too complex, especially when implemented in software (Al, A3, A4, A8, A10, All, B4, B9).
4. Applicability of the algorithm, including when and where to use it, is not specified (All, B2, C2, C6).
5. The proposed standard does not contain information on electrical, mechanical and functional interfaces to devices implementing the standard (A2, A7, A9, B2, B5, B7, C2, C6).
6. Administrative procedures for validation, procurement and testing have not been described (Al, A4, A7, B2, C2, C6).
7. Policy for exporting devices implementing the proposed DES has not been made (B2).
8. The algorithm does not provide an adequate level of security (A2, A3, A4, A6, A8, B7, B9, B10).

SOURCE: “Analysis of Comments on the Data Encryption Standard, ” unpublished data available for public review at NBS.

[8] These were some of a set of allegations to the effect that NSA was improperly involved in the development of DES and was attempting to exert undue influence on university and private-sector cryptological research. The Senate Select Comrnittee on Intelligence conducted a classified investigation of these allegations. Among its findings was that: “NSA did not tamper with the design of the algorithm in any way. IBM invented and designed the algorithm, made all pertinent decisions regarding it, and concurred that the agreed upon key size was more than adequate for all commercial applications for which the DES was intended. ” U.S. Senate, Select Committee on Intelligence, “Unclassified Summary: Involvement of NSA in the Development of the Data Encryption Standard” (Staff Report), 95th Cong., 2d sess., April 1978, p. 4.

Others contend that the modifications that were made to the S-boxes improved them and also were, at least in part, intended to minimize their logic to permit a smaller chip size when DES was implemented in hardware.

[9] U.S. Senate Select Committee on Intelligence, April 1978, op. cit.

[10] The Department of Commerce/NBS published the proposed Data Encryption Algorithm in the *Federal Register* on Mar. 17, 1975 (vol. 40, No, 52, p. 12134 et, seq.) and solicited comments to be submitted to NBS by May 16, 1975.

[11] “Analysis of Comments on the Data Encryption Standard, ” NBS/ICST (n.d., circa 1978). In total, 18 industry, 10 Federal, and 1 congressional source responded. Copies of all comments received by NBS and NBS' responses are available for public review at NBS.

[12] Ibid.

[13] Ibid,

the first software simulation of DES (by Computation Planning, Inc.) was announced in November 1975.

The previously mentioned controversy and debate concerning the strength of the proposed standard and NSA's role in its development continued through the 1970s. To address some of these concerns, NBS sponsored two workshops on DES and also briefed the Department of Justice concerning possible competition issues involving the proposed standard. The first workshop, held in August 1976, addressed the technical and economic feasibility of constructing a special-purpose computer to attack DES through computational brute force, The second workshop, held in September 1977, addressed the mathematical foundations of the DES algorithm. Although the outcome of these workshops was to allay most fears that DES was not sound or could be inexpensively broken by brute force before the 1990s, participants expressed concerns that it had not been possible to assess all of the design characteristics of DES because some had not been made public. *[4]

Also, in late 1975, Congressman Jack Brooks (D-Tex.), writing in response to the solicitation for comments, asked whether NSA had put undue influence on NBS in setting the security level of DES and what the NBS role had been in DES development and key generation. Prompted by Brooks' inquiry, the Senate Select Committee on Intelligence staff ultimately responded, after a classified inquiry, that there had been no undue NSA influence. [15]At the time, NBS stated that, although it would provide guidance and good techniques for individual Federal agencies to generate their own DES keys in accordance with Federal Information Processing Standards (FIPS), no Government agency should generate keys for other agencies or for the private sector.

Promulgation of the Standard

The Department of Commerce approved DES as a standard in November 1976. NBS published it as FIPS PUB 46 in January 1977, with the provision that DES would be reviewed for continued suitability at 5-year intervals and would be recertified (or not) every 5 years by NSA. DES was last recertified in 1982.

The administrative and technical workloads associated with the development and promulgation of DES were substantial-for NBS; other Federal agencies; the private sector (including vendors, the banking community, university researchers, and others); and for Congress, its staff, and support agencies. According to NBS, DES consumed some 3 man-years of effort for DES-related interactions alone by 1978, exclusive of IBM technical development of the algorithm. Although exact statistics were not compiled, these interactions included a conference at NBS and some 2,000 technical and policy meetings, telephone discussions, and mail contacts. A 3-year projection of continued interactions more than tripled the man-year estimates,

Developing the standards to support DES–for use in communications, data storage, message authentication, user/terminal authentication, physical security, magnetic stripe encryption, and key management—consumed an estimated 6½ man-years at NBS and another 34 man-years elsewhere between 1977 and 1980.[16]

One estimate of the total (administrative, technical, test, and validation) DES-related costs through 1977 amounted to about $515,000 for NBS, some $6 to $10 million for IBM, about $460,000 for NSA, and around $1.5 million for other users and vendors. The estimated NBS support cost for DES during the period 1978-80 was more than $800,000.

As of January 1987, about 20 industry vendors had produced one or more versions of hardware or firmware devices (chips) implementing the DES algorithm, for use in their own products or for sale to other manufacturers, And, as of that date, NBS had validated 28 implementations of the DES algorithm in hardware or firmware, produced by 11 vendors.

NBS, which takes the position that software implementations of DES would not comply with the Federal standard, only validates electronic devices (hardware or firmware) implementing the DES algorithm. The rationale is that hardware implementations are faster than software and that they are thought to be more reliable and harder for an adversary to modify "behind the user's back.[17]; Software implementations of DES are being marketed, but are not validated or certified for Government use. Also, some vendors choose not to sub-

[14] 'Computer Encryption and the National Security Agency Connecion," Science, vol. 197, July 29, 1977, pp. 438-440.

[1] "U.S. Senate Select Committee on Intelligence, April 1978, op. cit.

[16] Source: Unpublished estimates developed at NBS in the late 1970s.

[17] At the same time, it is worth noting that software *implementations* of high-quality encryption are much more difficult to control in terms of their dissemination and exportability. Because the DES algorithm is published, almost anyone with the requisite technical skills can produce soft ware versions of it, producing microprocessor-based implementations is more difficult, The new NSA secret algorithms are easier to control because thev are not published.

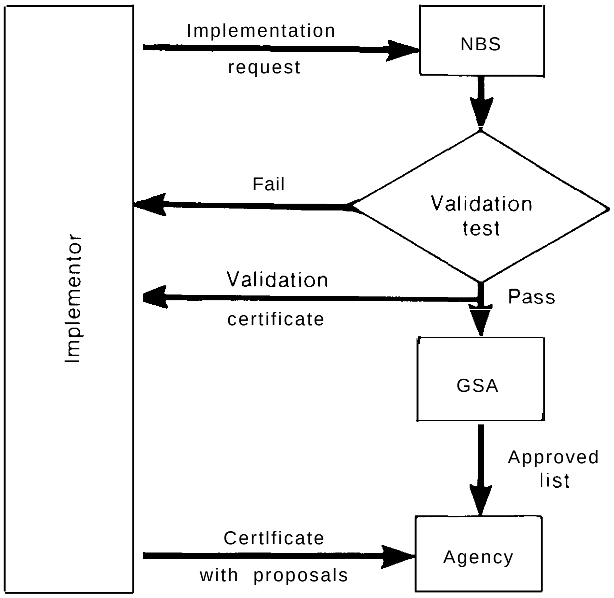
mit their hardware or firmware DES products for validation or certification for Government use. According to NBS staff, the Department of Defense is one of the largest single Federal customers for DES-based devices.

Figure 22 shows the roles of NBS and GSA in DES-based product validation and procurement.

Description of DES

A short technical summary of the encryption algorithm used in DES is given in figure 13 and box B of chapter 4. Complete technical descriptions of the four DES modes of operation, including initialization and error propagation properties and use for message authentication, may be found in FIPS Publications 74, 81, and 113, issued by NBS.[18] Diagrams of DES modes of operation, taken from NBS publications, are given in figure 23.

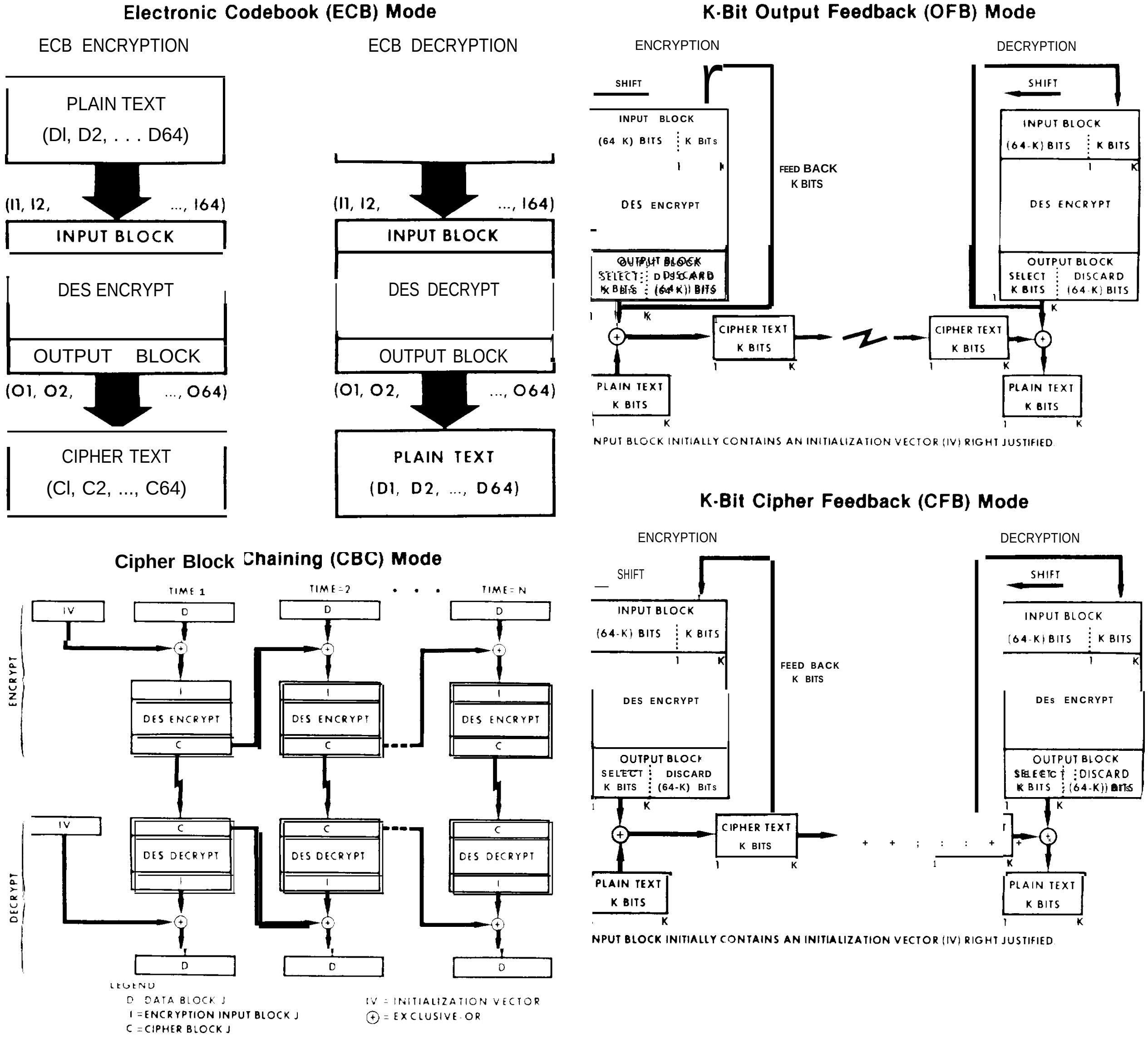
Figure 22.— DES Validation and Procurement



SOURCE National Bureau of Standards/Institute for Computer Sciences and Technology

[1*] U.S. Department of Commerce, National Bureau of Standards: "Guidelines for Implementing and using the NBS Data Encryption Standard, " FIPS PUB 74, Apr. 1, 1981; "DES Modes of Operation, " FIPS PUB 81, Dec. 2, 1980; and "Computer Data Authentication, " FIPS PUB 113, May 30, 1985.

Figure 23.—DES Modes of Operation



SOURCE: National Bureau of Standards, FIPS PUBS 81 and 74, Apr. 1, 1981.