N

FIPS PUB 46

FEDERAL INFORMATION
PROCESSING STANDARDS PUBLICATION
1977 JANUARY 15

U.S. DEPARTMENT OF COMMERCE / National Bureau of Standards

DATA ENCRYPTION STANDARD

CATEGORY: ADP OPERATIONS
SUBCATEGORY: COMPUTER SECURITY

U.S. DEPARTMENT OF COMMERCE • Elliot L. Richardson, *Secretary*

Edward O. Vetter, *Under Secretary*

Dr. Betsy Ancker-Johnson, *Assistant Secretary for Science and Technology*

NATIONAL BUREAU OF STANDARDS • Ernest Ambler, *Acting Director*

Foreword

The Federal Information Processing Standards Publication Series of the National Bureau of Standards is the official publication relating to standards adopted and promulgated under the provisions of Public Law 89-306 (Brooks Bill) and under Part 6 of Title 15, Code of Federal Regulations. These legislative and executive mandates have given the Secretary of Commerce important responsibilities for improving the utilization and management of computers and automatic data processing systems in the Federal Government. To carry out the Secretary's responsibilities, the NBS, through its Institute for Computer Sciences and Technology, provides leadership, technical guidance, and coordination of government efforts in the development of technical guidelines and standards in these areas.

The series is used to announce Federal Information Processing Standards, and to provide standards information of general interest and an index of relevant standards publications and specifications. Publications that announce adoption of standards provide the necessary policy, administrative, and guidance information for effective standards implementation and use. The technical specifications of the standard are usually attached to the publication, otherwise a reference source is cited.

Comments covering Federal Information Processing Standards and Publications are welcomed, and should be addressed to the Associate Director for ADP Standards, Institute for Computer Sciences and Technology, National Bureau of Standards, Washington, D.C. 20234. Such comments will be either considered by NBS or forwarded to the responsible activity as appropriate.

ERNEST AMBLER, *Acting Director*

Abstract

The selective application of technological and related procedural safeguards is an important responsibility of every Federal organization in providing adequate security to its ADP systems. This publication provides a standard to be used by Federal organizations when these organizations specify that cryptographic protection is to be used for sensitive or valuable computer data. Protection of computer data during transmission between electronic components or while in storage may be necessary to maintain the confidentiality and integrity of the information represented by that data. The standard specifies an encryption algorithm which is to be implemented in an electronic device for use in Federal ADP systems and networks. The algorithm uniquely defines the mathematical steps required to transform computer data into a cryptographic cipher. It also specifies the steps required to transform the cipher back to its original form. A device performing this algorithm may be used in many applications areas where cryptographic data protection is needed. Within the context of a total security program comprising physical security procedures, good information management practices and computer system/network access controls, the Data Encryption Standard is being made available for use by Federal agencies.

Key Words: ADP security; computer security; encryption; Federal Information Processing Standard.

Nat. Bur. Stand. (U.S.), Fed. Info. Process. Stand. Publ. (FIPS PUB) 46, 17 pages (1977)
CODEN: FIPPAT

For sale by the National Technical Information Service, U.S. Department of Commerce, Springfield, Virginia 22161

Federal Information Processing Standards Publication 46

1977 January 15

ANNOUNCING THE

DATA ENCRYPTION STANDARD

Federal Information Processing Standards are issued by the National Bureau of Standards pursuant to the Federal Property and Administrative Services Act of 1949, as amended, Public Law 89-306 (79 Stat 1127), Executive Order 11717 (38 FR 12315, dated May 11, 1973), and Part 6 of Title 15 Code of Federal Regulations (CFR).

Name of Standard: Data Encryption Standard (DES).

Category of Standard: Operations, Computer Security.

Explanation: The Data Encryption Standard (DES) specifies an algorithm to be implemented in electronic hardware devices and used for the cryptographic protection of computer data. This publication provides a complete description of a mathematical algorithm for encrypting (enciphering) and decrypting (deciphering) binary coded information. Encrypting data converts it to an unintelligible form called cipher. Decrypting cipher converts the data back to its original form. The algorithm described in this standard specifies both enciphering and deciphering operations which are based on a binary number called a key. The key consists of 64 binary digits ("0"s or "1"s) of which 56 bits are used directly by the algorithm and 8 bits are used for error detection.

Binary coded data may be cryptographically protected using the DES algorithm in conjunction with a key. The key is generated in such a way that each of the 56 bits used directly by the algorithm are random and the 8 error detecting bits are set to make the parity of each 8-bit byte of the key odd, i.e., there is an odd number of "1"s in each 8-bit byte. Each member of a group of authorized users of encrypted computer data must have the key that was used to encipher the data in order to use it. This key, held by each member in common, is used to decipher the data received in cipher form from other members of the group. The encryption algorithm specified in this standard is commonly known among those using the standard. The unique key chosen for use in a particular application makes the results of encrypting data using the algorithm unique. Selection of a different key causes the cipher that is produced for any given set of inputs to be different. The cryptographic security of the data depends on the security provided for the key used to encipher and decipher the data.

Data can be recovered from cipher only by using exactly the same key used to encipher it. Unauthorized recipients of the cipher who know the algorithm but do not have the correct key cannot derive the original data algorithmically. However, anyone who does have the key and the algorithm can easily decipher the cipher and obtain the original data. A standard algorithm based on a secure key thus provides a basis for exchanging encrypted computer data by issuing the key used to encipher it to those authorized to have the data. Additional FIPS guidelines for implementing and using the DES are being developed and will be published by NBS.

Approving Authority: Secretary of Commerce.

Maintenance Agency: Institute for Computer Sciences and Technology, National Bureau of Standards.

Applicability: This standard will be used by Federal departments and agencies for the cryptographic protection of computer data when the following conditions apply:

1. An authorized official or manager responsible for data security or the security of any computer system decides that cryptographic protection is required; and

2. The data is not classified according to the National Security Act of 1947, as amended, or the Atomic Energy Act of 1954, as amended.

However, Federal agencies or departments which use cryptographic devices for protecting data classified according to either of these acts can use those devices for protecting unclassified data in lieu of the standard.

In addition, this standard may be adopted and used by non-Federal Government organizations. Such use is encouraged when it provides the desired security for commercial and private organizations.

Data that is considered sensitive by the responsible authority, data that has a high value, or data that represents a high value should be cryptographically protected if it is vulnerable to unauthorized disclosure or undetected modification during transmission or while in storage. A risk analysis should be performed under the direction of a responsible authority to determine potential threats. FIPS PUB 31 (Guidelines for Automatic Data Processing Physical Security and Risk Management) and FIPS PUB 41 (Computer Security Guidelines for Implementing the Privacy Act of 1974) provide guidance for making such an analysis. The costs of providing cryptographic protection using this standard as well as alternative methods of providing this protection and their respective costs should be projected. A responsible authority then should make a decision, based on these analyses, whether or not to use cryptographic protection and this standard.

Applications: Data encryption (cryptography) may be utilized in various applications and in various environments. The specific utilization of encryption and the implementation of the DES will be based on many factors particular to the computer system and its associated components. In general, cryptography is used to protect data while it is being communicated between two points or while it is stored in a medium vulnerable to physical theft. Communication security provides protection to data by enciphering it at the transmitting point and deciphering it at the receiving point. File security provides protection to data by enciphering it when it is recorded on a storage medium and deciphering it when it is read back from the storage medium. In the first case, the key must be available at the transmitter and receiver simultaneously during communication. In the second case, the key must be maintained and accessible for the duration of the storage period.

Hardware Implementation: The algorithm specified in this standard is to be implemented in computer or related data communication devices using hardware (not software) technology. The specific implementation may depend on several factors such as the application, the environment, the technology used, etc. Implementations which comply with this standard include Large Scale Integration (LSI) "chips" in individual electronic packages, devices built from Medium Scale Integration (MSI) electronic components, or other electronic devices dedicated to performing the operations of the algorithm. Micro-processors using Read Only Memory (ROM) or micro-programmed devices using microcode for hardware level control instructions are examples of the latter. Hardware implementations of the algorithm which are tested and validated by NBS will be considered as complying with the standard. Procedures for testing and validating equipment for conformance with this standard are available from the Systems and Software Division, National Bureau of Standards, Washington, D.C. 20234. Software implementations in general purpose computers are not in compliance with this standard. Information regarding devices which have been tested and validated will be made available to all FIPS points of contact.

Export Control: Cryptographic devices and technical data regarding them are subject to Federal Government export controls as specified in Title 22, Code of Federal Regulations, Parts 121 through 128. Cryptographic devices implementing this standard and technical data regarding them must comply with these Federal regulations.

Patents: Crytographic devices implementing this standard may be covered by U.S. and foreign patents issued to the International Business Machines Corporation. However, IBM has granted nonexclusive, royalty-free licenses under the patents to make, use and sell apparatus which complies with the standard. The terms, conditions and scope of the licenses are set out in notices published in the May 13, 1975 and August 31, 1976 issues of the Official Gazette of the United States Patent and Trademark Office (934 O. G. 452 and 949 O. G. 1717).

Alternative Modes of Using the DES: The "Guidelines for Implementing and Using the Data Encryption Standard" describe two different modes for using the algorithm described in this standard. Blocks of data containing 64 bits may be directly entered into the device where 64-bit cipher blocks are generated under control of the key. This is called the electronic code book mode. Alternatively, the device may be used as a binary stream generator to produce statistically random binary bits which are then combined with the clear (unencrypted) data (1-64 bits) using an "exclusive-or" logic operation. In order to assure that the enciphering device and the deciphering device are synchronized, their inputs are always set to the previous 64 bits of cipher that were transmitted or received. This second mode of using the encryption algorithm is called the cipher feedback (CFB) mode. The electronic codebook mode generates blocks of 64 cipher bits. The cipher feedback mode generates cipher having the same number of bits as the plain text. Each block of cipher is independent of all others when the electronic codebook mode is used while each byte (group of bits) of cipher depends on the previous 64 cipher bits when the cipher feedback mode is used. The modes of operation briefly described here are further explained in the FIPS "Guidelines for Implementing and Using the Data Encryption Standard."

Implementation of this standard: This standard becomes effective six months after the publication date of this FIPS PUB. It applies to all Federal ADP systems and associated telecommunications networks under development as well as to installed systems when it is determined that cryptographic protection is required. Each Federal department or agency will issue internal directives for the use of this standard by their operating units based on their data security requirement determinations.

NBS will provide assistance to Federal organizations by developing and issuing additional technical guidelines on computer security and by providing technical assistance in using data encryption. A data encryption testbed has been established within NBS for use in providing this technical assistance. The National Security Agency assists Federal departments and agencies in communications security and in determining specific security requirements. Instructions and regulations for procuring data processing equipment utilizing this standard will be provided by the General Services Administration.

Specifications: Federal Information Processing Standard (FIPS 46) Data Encryption Standard (DES) (affixed).

Cross Index:

a. FIPS PUB 31, "Guidelines to ADP Physical Security and Risk Management"

b. FIPS PUB 39, "Glossary for Computer Systems Security"

c. FIPS PUB 41, "Computer Security Guidelines for Implementing the Privacy Act of 1974"

d. FIPS PUB 74—, "Guidelines for Implementing and Using the Data Encryption Standard" (to be published)

e. Other FIPS and Federal Standards are applicable to the implementation and use of this standard. In particular, the American Standard Code for Information Interchange (FIPS PUB 1)

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.