FIPS PUB 46-2 - Announcing the DATA ENCRYPTION STANDARD (DES)

Federal Information Processing Standards Publication 46-2

1993 December 30

Federal Information Processing Standards Publications (FIPS PUBS) are issued by the National Institute of Standards and Technology after approval by the Secretary of Commerce pursuant to Section 111(d) of the Federal Property and Administrative Services Act of 1949 as amended by the Computer Security Act of 1987, Public Law 100-235.

- 1. Name of Standard. Data Encryption Standard (DES).
- 2. Category of Standard. Computer Security.
- 3. Explanation. The Data Encryption Standard (DES) specifies a FIPS approved cryptographic algorithm as required by FIPS 140-1. 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 called plaintext. The algorithm described in this standard specifies both enciphering and deciphering operations which are based on a binary number called a key.
- A key consists of 64 binary digits ("O"s or "1"s) of which 56 bits are randomly generated and used directly by the algorithm. The other 8 bits, which are not used by the algorithm, are used for error detection. 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. Authorized users of encrypted computer data must have the key that was used to encipher the data in order to decrypt it. 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.
- 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. 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.

4. Approving Authority. Secretary of Commerce.

5. Maintenance Agency. U.S. Department of Commerce, National Institute of Standards and Technology, Computer Systems Laboratory.

6. Applicability. This standard may be used by Federal departments and agencies 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.

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.

Other FIPS approved cryptographic algorithms may be used in addition to, or in lieu of, this standard when implemented in accordance with FIPS 140-1.

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.

7. Applications. Data encryption (cryptography) is utilized in various applications and 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. FIPS 171 provides approved methods for managing the keys used by the algorithm specified in this standard.

8. Implementations. Cryptographic modules which implement this standard

shall conform to the requirements of FIPS 140-1. The algorithm specified in this standard may be implemented in software, firmware, hardware, or any combination thereof. The specific implementation may depend on several factors such as the application, the environment, the technology used, etc. Implementations which may comply with this standard include electronic devices (e.g., VLSI chip packages), micro-processors using Read Only Memory (ROM), Programmable Read Only Memory (PROM), or Electronically Erasable Read Only Memory (EEROM), and mainframe computers using Random Access Memory (RAM). When the algorithm is implemented in software or firmware, the processor on which the algorithm runs must be specified as part of the validation process. Implementations of the algorithm which are tested and validated by NIST will be considered as complying with the standard. Note that FIPS 140-1 places additional requirements on cryptographic modules for Government use. Information about devices that have been validated and procedures for testing and validating equipment for conformance with this standard and FIPS 140-1 are available from the National Institute of Standards and Technology, Computer Systems Laboratory, Gaithersburg, MD 20899. 9. 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 120 through 128. Some exports of cryptographic modules implementing this standard and technical data regarding them must comply with these Federal regulations and be licensed by the U.S. Department of State. Other exports of cryptographic modules implementing this standard and technical data regarding them fall under the licensing authority of the Bureau of Export Administration of the U.S. Department of Commerce. The Department of Commerce is responsible for licensing cryptographic devices used for authentication, access control, proprietary software, automatic teller machines (ATMs), and certain devices used in other equipment and software. For advice concerning which agency has licensing authority for a particular cryptographic device, please contact the respective agencies.

- 10. Patents. Cryptographic 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).
- 11. Alternative Modes of Using the DES. FIPS PUB 81, DES Modes of Operation, describes four different modes for using the algorithm described in this standard. These four modes are called the Electronic Codebook (ECB) mode, the Cipher Block Chaining (CBC) mode, the Cipher Feedback (CFB) mode, and the Output Feedback (OFB) mode. ECB is a direct application of the DES algorithm to encrypt and decrypt data; CBC is an enhanced mode of ECB which chains together blocks of cipher text; CFB uses previously

generated cipher text as input to the DES to generate pseudorandom outputs which are combined with the plaintext to produce cipher, thereby chaining together the resulting cipher; OFB is identical to CFB except that the previous output of the DES is used as input in OFB while the previous cipher is used as input in CFB. OFB does not chain the cipher.

- 12. Implementation of this standard. This standard became effective July 1977. It was reaffirmed in 1983, 1988, and 1993. It applies to all Federal agencies, contractors of Federal agencies, or other organizations that process information (using a computer or telecommunications system) on behalf of the Federal Government to accomplish a Federal function. Each Federal agency or department may issue internal directives for the use of this standard by their operating units based on their data security requirement determinations. FIPS 46-2 which revises the implementation of the Data Encryption Algorithm to include software, firmware, hardware, or any combination thereof, is effective June 30, 1994. This revised standard may be used in the interim period before the effective date.
- NIST provides technical assistance to Federal agencies in implementing data encryption through the issuance of guidelines and through individual reimbursable projects. The National Security Agency assists Federal departments and agencies in communications security for classified applications and in determining specific security requirements. Instructions and regulations for procuring data processing equipment utilizing this standard are included in the Federal Information Resources Management Regulation (FIRMR) Subpart 201-8.111-1.
- 13. Specifications. Federal Information Processing Standard (FIPS) 46-2, Data Encryption Standard (DES) (affixed).
- 14. Cross Index. a. Federal Information Resources Management Regulations (FIRMR) subpart 201.20.303, Standards, and subpart 201.39.1002, Federal Standards. b. FIPS PUB 31, Guidelines to ADP Physical Security and Risk Management. c. FIPS PUB 41, Computer Security Guidelines for Implementing the Privacy Act of 1974. d. FIPS PUB 65, Guideline for Automatic Data Processing Risk Analysis. e. FIPS PUB 73, Guidelines for Security of Computer Applications. f. FIPS PUB 74, Guidelines for Implementing and Using the NBS Data Encryption Standard. g. FIPS PUB 81, DES Modes of Operation. h. FIPS PUB 87, Guidelines for ADP Contingency Planning. i. FIPS PUB 112, Password Usage. j. FIPS PUB 113, Computer Data Authentication. k. FIPS PUB 140-1, Security Requirements for Cryptographic Modules. l. FIPS PUB 171, Key Management Using ANSI X9.17. m. Other FIPS and Federal Standards are applicable to the implementation and use of this standard. In particular, the Code for Information Interchange, Its Representations, Subsets, and Extensions (FIPS PUB 1-2) and other related data storage media or data communications standards should be used in conjunction with this standard. A list of currently approved FIPS may be obtained from the National Institute of Standards and Technology, Computer Systems Laboratory, Gaithersburg, MD 20899.
- 15. Qualifications. The cryptographic algorithm specified in this standard

transforms a 64-bit binary value into a unique 64-bit binary value based on a 56-bit variable. If the complete 64-bit input is used (i.e., none of the input bits should be predetermined from block to block) and if the 56-bit variable is randomly chosen, no technique other than trying all possible keys using known input and output for the DES will guarantee finding the chosen key. As there are over 70,000,000,000,000,000 (seventy quadrillion) possible keys of 56 bits, the feasibility of deriving a particular key in this way is extremely unlikely in typical threat environments. Moreover, if the key is changed frequently, the risk of this event is greatly diminished. However, users should be aware that it is theoretically possible to derive the key in fewer trials (with a correspondingly lower probability of success depending on the number of keys tried) and should be cautioned to change the key as often as practical. Users must change the key and provide it a high level of protection in order to minimize the potential risks of its unauthorized computation or acquisition. The feasibility of computing the correct key may change with advances in technology.

- A more complete description of the strength of this algorithm against various threats is contained in FIPS PUB 74, Guidelines for Implementing and Using the NBS Data Encryption Standard.
- When correctly implemented and properly used, this standard will provide a high level of cryptographic protection to computer data. NIST, supported by the technical assistance of Government agencies responsible for communication security, has determined that the algorithm specified in this standard will provide a high level of protection for a time period beyond the normal life cycle of its associated equipment. The protection provided by this algorithm against potential new threats will be reviewed within 5 years to assess its adequacy (See Special Information Section). In addition, both the standard and possible threats reducing the security provided through the use of this standard will undergo continual review by NIST and other cognizant Federal organizations. The new technology available at that time will be evaluated to determine its impact on the standard. In addition, the awareness of any breakthrough in technology or any mathematical weakness of the algorithm will cause NIST to reevaluate this standard and provide necessary revisions.
- At the next review (1998), the algorithm specified in this standard will be over twenty years old. NIST will consider alternatives which offer a higher level of security. One of these alternatives may be proposed as a replacement standard at the 1998 review.
- 16. Comments. Comments and suggestions regarding this standard and its use are welcomed and should be addressed to the National Institute of Standards and Technology, Attn: Director, Computer Systems Laboratory, Gaithersburg, MD 20899.
- 17. Waiver Procedure. Under certain exceptional circumstances, the heads of Federal departments and agencies may approve waivers to Federal Information Processing Standards (FIPS). The head of such agency may redelegate such authority only to a senior official designated pursuant to section 3506(b) of Title 44, United States Code. Waiver shall be granted only when:

- a. Compliance with a standard would adversely affect the accomplishment of the mission of an operator of a Federal computer system; or
- b. Compliance with a standard would cause a major adverse financial impact on the operator which is not offset by Government-wide savings.

Agency heads may act upon a written waiver request containing the information detailed above. Agency heads may also act without a written waiver request when they determine that conditions for meeting the standard cannot be met. Agency heads may approve waivers only by a written decision which explains the basis on which the agency head made the required finding(s). A copy of each decision, with procurement sensitive or classified portions clearly identified, shall be sent to: National Institute of Standards and Technology; ATTN: FIPS Waiver Decisions, Technology Building, Room B-154, Gaithersburg, MD 20899.

In addition, notice of each waiver granted and each delegation of authority to approve waivers shall be sent promptly to the Committee on Government Operations of the House of Representatives and the Committee on Government Affairs of the Senate and shall be published promptly in the Federal Register.

When the determination on a waiver applies to the procurement of equipment and/or services, a notice of the waiver determination must be published in the Commerce Business Daily as a part of the notice of solicitation for offers of an acquisition or, if the waiver determination is made after that notice is published, by amendment to such notice.

A copy of the waiver, any supporting documents, the document approving the waiver and any accompanying documents, with such deletions as the agency is authorized and decides to make under 5 United States Code Section 552(b), shall be part of the procurement documentation and retained by the agency.

- 18. Special Information. In accordance with the Qualifications Section of this standard, reviews of this standard have been conducted every 5 years since its adoption in 1977. The standard was reaffirmed during each of those reviews. This revision to the text of the standard contains changes which allow software implementations of the algorithm and which permit the use of other FIPS approved cryptographic algorithms.
- 19. Where to Obtain Copies of the Standard. Copies of this publication are for sale by the National Technical Information Service, U.S. Department of Commerce, Springfield, VA 22161. When ordering, refer to Federal Information Processing Standards Publication 46-2 (FIPS PUB 46-2), and identify the title. When microfiche is desired, this should be specified. Prices are published by NTIS in current catalogs and other issuances. Payment may be made by check, money order, deposit account or charged to a credit card accepted by NTIS.
- --- End Included Message ---