DATA ENCRYPTION STANDARD FACT SHEET

Introduction

The National Institute of Standards and Technology (NIST) of the Department of Commerce has recently received many inquiries regarding various aspects of the Data Encryption Standard (DES). This document addresses those frequently asked questions and provides interested individuals with sources of additional information. The document is not designed to issue new policy; rather it summarizes and clarifies existing policies. Additional guidance concerning the use of National Security Agency (NSA) developed Type II and Low-cost Encryption Authentication Devices (LEAD) is planned to be issued in 1990.

Background

Issued as Federal Information Processing Standard Publication (FIPS PUB) 46 in 1977, the DES was promulgated by NIST (then the National Bureau of Standards) to provide a system for the protection of the confidentiality and integrity of the federal government's sensitive unclassified computer information. FIPS PUB 46 is based upon work by the International Business Machines Corporation and has been approved as American National Standard X3.92-1981/R1987. The DES has been reaffirmed twice, most recently in 1988. The current standard, which was issued as FIPS PUB 46-1, reaffirms the standard until 1993.

Technical Overview

The Data Encryption Standard specifies a cryptographic algorithm that converts plaintext to ciphertext using a key, a process called encryption. The same algorithm is used with the same key to convert ciphertext back to plaintext, a process called decryption. The DES consists of 16 "rounds" of operations that mix the data and key together is a prescribed manner using the fundamental operations of permutation and substitution. The goal is to completely scramble the data and key so that every bit of the ciphertext depends on every bit of the data and every bit of the key (a 56-bit quantity for the DES). After sufficient "rounds" with a good algorithm, there should be no correlation between the ciphertext and either the original data or key.

The DES uses 16 rounds for several reasons. First, a minimum of 12 rounds were needed to sufficiently scramble the key and data together; the others provided a margin of safety. Second, the operation of 16 rounds would return the key back to its original position in an electronic device for the next use when

used in accordance with the published algorithm. Third, numerous "rounds" were needed to keep an analyst or adversary from working simultaneously forward and backward and "meeting in the middle" with a solution.

Security Provided by DES

The security provided by the DES depends on several factors: mathematical soundness, length of key, key management, input data formatting, mode of operation, implementation, application and threat. The DES was developed to protect unclassified computer data in federal computer systems against a number of passive and active attacks in communications and storage systems. It was assumed that a knowledgeable person might seek to comprise the security system with resources commensurate to the value of the information to be obtained. Applications included Electronic Funds Transfer, privacy protection of personal information, personal authentication, password protection, access control, etc.

The DES has been evaluated by several organizations and has been determined to be mathematically sound. The effective length of the data key (56-bits) was challenged by several people as being too short for high security applications. Several people have analyzed the algorithm and have concluded that the algorithm is sound but would not be "if only this simple change was made." The most recent charge was that "if the DES has only 6 or 8 rounds instead of 16, then it could be broken on a personal computer in 0.3 seconds and 3 minutes respectively.

The two algorithms that were "broken on a personal computer" in 0.3 seconds and 3 minutes respectively WERE NOT THE DES. There is only one DES and any change to it results in an algorithm that IS NOT THE DES. Cryptographically, any algorithm that is obtained by any change to the DES may be significantly different in the security it provides. Thus, while the DES is sound, many algorithms that are similar to, but different from, the DES are not sound.

NIST has determined that at least until 1993, the DES will continue to provide more than adequate security for its intended applications. It is currently the only cryptographic method to be used in the federal government to protect unclassified computer data (except that information described in 10 U.S.C. Section 2315). However, NIST does plan to augment the DES with other cryptographic algorithms in a family of standards that will provide other types of protection in special applications (e.g., digital signatures, key exchange, exportable security). NIST will continue to support the use of DES in government security applications for the foreseeable future.

Applicability

Subject to agency waivers as discussed below, use of DES is mandatory for all federal agencies, including defense agencies, for the protection of sensitive unclassified data communications (except information covered by 10 U.S.C. Section 2315, as described below) when the agency or department determines that cryptographic protection is required. Note that the term unclassified information as used in this document excludes information covered by 10 U.S.C. 2315. Use of DES is currently applicable only to the protection of data communications.

The National Security Agency (NSA) of the U.S. Department of Defense develops and promulgates requirements for those telecommunications and automated information systems operated by the U.S. Government, its contractors, or agents, that contain classified information or, as delineated in 10 U.S.C. Section 2315, the function, operation, or use of which:

- · involves intelligence activities;
- · involves cryptologic activities related to national security;
- · involves the direct command and control of military forces;
- · involves equipment which is an integral part of a weapon or weapon systems; or
- · is critical to the direct fulfillment of a military or intelligence mission.

DES may be used by private-sector individuals or organizations at their discretion.

Waivers for the Mandatory Use of DES

The head of a federal department or agency may waive the use of DES for the protection of unclassified information as discussed below.

Waivers to the mandatory use of DES are required if:

- · cryptographic devices perform an algorithm other than DES and are used by federal departments or agencies for cryptographic protection of information;
- · DES is implemented in a software-based system (See specific exclusions below.); or
- · the agency or department wishes to use Type II (i.e, for unclassified applications) cryptographic devices certified by NSA (except for current voice only applications).
- [Note: Type I products have been approved by NSA for the protection of classified information while Type II products have been approved for the protection of unclassified information.]

Waivers to the mandatory use of DES are not required if:

- · the agency or department wishes to use Type I (i.e., for classified

applications) cryptographic equipment;
- DES is implemented in software for testing or evaluation purposes; or
- DES is implemented in software for a limited special purpose (e.g., encrypting password files).

Additionally, no waivers are currently required for use of Type II products for voice only applications.

Waiver Procedures

As mentioned above, the heads of federal departments or agencies may waive the mandatory use of DES. This authority may be redelegated only to a senior official designated pursuant to 44 U.S.C. section 3506(b). Waivers shall be granted only when:

- compliance with the standard would adversely affect the accomplishment of the mission of an operator of a federal computer system; or
- compliance would cause a major adverse financial impact on the operator which is not offset by Governmentwide savings.

In addition, when a waiver is being considered to allow for the use of Type II products, the agency must document that such devices offer equivalent cost/performance features when compared to devices conforming to the DES standard.

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 such decision, with procurement-sensitive or classified portions clearly identified, shall be sent to:

National Institute of Standards and Technology
Attention: FIPS Waiver Decisions
Technology Building, Room B-154
Gaithersburg, MD 20899

In addition, notice of each waiver granted and each delegation of authority shall be sent promptly to the Committee on Government Operations of the House of Representatives and the Committee on Governmental 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 supporting or accompanying documents, with such deletions as the agency is authorized and decides to make under 5 U.S.C. Section 552(b), shall be part of the procurement documentation and retained by the agency.

Endorsement of DES Products

DES products for use in telecommunications equipment and systems are no longer being endorsed for conformance to FIPS PUB 140 (formerly Federal Standard 1027) by NSA. NIST has notified the heads of federal departments that they may wish to consider waiving the requirements of FIPS PUB 140 in order to buy equipment which may not meet all of the criteria in the standard. This action will enable agencies to procure cost-effective equipment that meets their needs, but has not been endorsed by NSA.

FIPS PUB 140 is currently under revision to be reissued as FIPS PUB 140-1. All issues contained within the scope of the document are being readdressed. Additionally, NIST is examining various methods for conducting conformance testing against the requirements of FIPS PUB 140-1. Until the NIST FIPS 140-1 program is established, federal agencies may accept written affirmation of conformance to FIPS PUB 140 from vendors as sufficient indication of conformance.

DES Cryptographic Keys

U.S. government users of NSA-endorsed products may obtain DES cryptographic keys for these products from NSA upon request at no cost. Contact your responsible Communications Security (COMSEC) officer for further information.

Alternatively, users of the DES, including federal organizations, may generate their own cryptographic keys. DES keys must be properly generated and managed in order to assure a high level of protection to computer data. Electronic Key Management includes generation, distribution, storage, and destruction of cryptographic keys using automated processes. Information on this subject may be obtained from FIPS 74, FIPS 140-1 (future), ANSI X9.17, and the Secure Data Network System (SDNS) documents available from NIST. The specifics of electronic key generation are outside the scope of this document.

The keys used to protect electronic funds transfers must be able to be changed and should be changed aperiodically, but at least annually. Very large electronic

funds transfers should be protected individually with separate keys and the input data must be properly formatted to assure high security.

Exportability of DES Devices and Software Products

Hardware- and software- based implementations of DES are subject to federal export controls as specified in Title 22, Code of Federal Regulations (CFR), Parts 120 - 130, the International Traffic in Arms Regulations (ITAR). Specific information regarding export applications, application procedures, types of licenses, and necessary forms may be found in the CFR. Responsibility for granting export licenses (except for those DES implementations noted below) rests with:

- Office of Munitions Control
- Bureau of Politico-Military Affairs
- U.S. Department of State
- Washington, DC, 20250
- Telephone: (202) 875-6650

The Office of Munitions Control, U.S. Department of State issues either individual or distribution licenses. Under a distribution license, annual reports must be submitted by the distributor describing to whom the licensed products have been sold. License requests for products to be shipped to certain prohibited countries (see Section 126.1 of the ITAR) are denied for foreign policy reasons by the Department of State.

Licenses are normally granted if the end users are either financial institutions or American subsidiaries abroad. In general, either individual or distribution licenses may be used for financial institutions while only individual licenses may be used for subsidiaries of U.S. corporations.

Specific Cryptographic Implementations under Jurisdiction of the Department of Commerce

The Bureau of Export Administration, U.S. Department of Commerce is responsible for the granting of export licenses for the following categories of cryptographic products (including DES):

- · Authentication. Software or hardware which calculates a Message Authentication Code (MAC) or similar result to assure no alteration of text has taken place, or to authenticate users, but does not allow for encryption of data, text or other media other than that needed for the authentication.
- · Access Control. Software or hardware which protect passwords or Personal Identification Numbers (PIN) or similar data to prevent unauthorized access to

computing facilities, but does not allow for encryption of files or text, except as directly related to password or PIN protection.

- Proprietary Software Protection. Decryption-only routines for encrypted proprietary software, fonts, or other computer-related proprietary information for the purpose of maintaining vendor control over said information when such decryption routines are not accessible to users of said software, font or other information, and cannot be used for any other purpose.
- Automatic Teller Devices. Devices limited to the issuance of cash or travellers checks, acceptance of deposits, or account balance reporting.

Vendors of products in the above four categories should contact the following for a product classification determination:

Bureau of Export Administration
U.S. Department of Commerce
P.O. Box 273
Washington, DC 20044
Telephone: (202) 377-0708

Following this determination, the vendor will be informed whether an export license from the U.S. Department of Commerce is necessary. The Bureau of Export Administration will provide vendors with license procedures and further information as appropriate.

Please note that vendors whose products do not fall clearly into the above categories should follow procedures set forth in the ITAR, 22 CFR 120-130.

Validation of Devices for Compliance with FIPS PUBS 46 and 113

NIST performs validations of products for compliance with FIPS PUBS 46 and 113. For further information about submitting products for validation or to obtain a list of devices validated under either standard, please contact:

Manager, Security Technology Group
Computer Security Division
National Computer Systems Laboratory
Building 225, Room A266
National Institute of Standards and Technology
Gaithersburg, MD 20899
Telephone (301) 975-2920

Reference Documents

NIST Documents

NIST has issued FIPS PUBS and special publications regarding DES, its implementation, and modes of operation.

FIPS PUB 46-1, Data Encrtyption Sandard

This standard provides the technical specifications for the DES algorithm.

FIPS PUB 74, Guidelines for Implementation and Using the NBS Data Encryption Standard

This guideline on DES discusses how and when data encryption should be used, various encryption methods, the reduction of security threats, implementation of the DES algorithm, and key management.

FIPS PUB 81, DES Modes of Operation

FIPS PUB 81 defines four modes of operation for DES which may be used in a wide variety of applications. The modes specify how data will be encrypted and decrypted. The four modes are: (1) Electronic Codebook (ECB), (2) the Cipher Block Chaining (CBC), (3) Cipher Feedback (CFB), and (4) Output Feedback (OFB).

FIPS PUP 113, Computer Data Authentication

This standard specifies a Data Authentication Algorithm, based upon DES, which may be used to detect unauthorized modifications, both intentional and accidental, to data. The Message Authentication Code as specified in ANSI X9.9 is computed in the same manner as the Data Authentication Code as specified in this standard.

FIPS PUB 139, Interoperability and Security Requirements for Use of the Data Encryption Standard in the Physical Layer of Data Communications

This standard specifies interoperability and security-related requirements for using encryption at the Physical Layer of the ISO Open Systems Interconnection (OSI) Reference Model in telecommunications systems conveying digital information. FIPS PUB 139 was previously issued by the General Services Administration as Federal Standard 1026.

FIPS PUB 140, General Security Requirements for Equipment Using the Data Encryption Standard

This document establishes the physical and logical security requirements for the design and manufacture of DES equipment. FIPS PUB 140 was previously issued by the General Services Administration as Federal Standard 1027.

FIPS PUB 141, Interoperability and Security Requirements for Use of the Data Encryption Standard With CCITT Group 3 Facsimile Equipment

This document specifies interoperability and security related requirements for use of encryption with the International Telegraph and Telephone Consultative Committee (CCITT), Group 3-type facsimile equipment.

NBS Special Publication 500-61, Maintenance Testing for the Data Encryption Standard

This special publication describes the design of four maintenance tests for the Data Encryption Standard. The tests consist of an iterative procedure that tests the operation of DES devices using a small program and minimal data. The tests are defined as four specific stopping points in a general testing process and satisfy four testing requirements of increasing degree of completeness depending on the thoroughness of testing desired.

NBS Special Publication 500-156, Message Authentication Code (MAC) Validation System: Requirements and Procedures

This special publication describes a Message Authentication Code (MAC) Validation System (MVS) to test message authentication devices for conformance to two data authentication standards:

FIPS PUB 113 and ANSI X9.9-1986, Financial Institution Message Authentication (Wholesale).

The MVS is designed to perform automated testing on message authentication devices which are remote to NIST. This publication provides brief overviews of the two data authentication standards and introduces the basic design and configuration of the MVS. The requirements and administrative procedures to be followed by those seeking formal NIST validation of a message authentication device are presented.

National Technical Information Service

Copies of these publications are for sale by the National Technical Information Service, at:

- National Technical Information Service
- U.S. Department of Commerce
- 5285 Port Royal Road
- Springfield, VA 22161
- Telephone (703) 487-4650, FTS: 737-4650

Other Documents

DES has been incorporated into a number of other standards, including: American National Standard for Financial Institution Message Authentication, ANSI X9.9-1982, 1430 Broadway, New York, NY.

American National Standard for Personal Identification Number (PIN) Management and Security, ANSI X9.8-1982, 1430 Broadway, New York, NY.

Data Encryption Algorithm (DEA), ANSI X3.92-1981, 1430 Broadway, New York, NY.

Key Management Standard, Document 4.3, American Bankers Association, Washington, DC, 1980.

Management and Use of Personal Identification Numbers, Cat. No.

207213, American Bankers Association, Washington, DC, 1979.

Protection of Personal Identification Numbers in Interchange, Document 4.5.6, American Bankers Association, Washington, DC, 1981.

NIST's Computer Security Program

For further information regarding other aspects of NIST's computer security program, including NIST's federal agency assistance program, please contact:

- Computer Security Division
- National Computer Systems Laboratory
- Building 225, Room A216
- National Institute of Standards and Technology
- Gaithersburg, MD 20899
- Telephone (301) 975-2934