FIPS PUB 81

FEDERAL INFORMATION
PROCESSING STANDARDS PUBLICATION

1980 December 2

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

DES MODES OF OPERATION

CATEGORY: ADP OPERATIONS
SUBCATEGORY: COMPUTER SECURITY

U.S. DEPARTMENT OF COMMERCE, Philip M. Klutznick, Secretary

Jordan J. Baruch, Assistant Secretary for Productivity,
Technology and Innovation

NATIONAL BUREAU OF STANDARDS, Ernest Ambler, 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 Act) 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 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 guidelines and standards in these areas.

Comments concerning Federal Information Processing Standards Publications are welcomed and should be addressed to the Director, Institute for Computer Sciences and Technology, National Bureau of Standards, Washington, DC 20234.

James H. Burrows, Director
Institute for Computer Sciences
and Technology

Abstract

The Federal Data Encryption Standard (DES) (FIPS 46) specifies a cryptographic algorithm to be used for the cryptographic protection of sensitive, but unclassified, computer data. This FIPS defines four modes of operation for the DES which may be used in a wide variety of applications. The modes specify how data will be encrypted (cryptographically protected) and decrypted (returned to original form). The modes included in this standard are the Electronic Codebook (ECB) mode, the Cipher Block Chaining (CBC) mode, the Cipher Feedback (CFB) mode, and the Output Feedback (OFB) mode.

KEY WORDS: Computer security; cryptography; data security; DES; encryption; Federal Information Processing Standards; modes of operation.

Nat.Bur.Stand. (U.S.), Fed.Info.Process.Stand.Publ.(FIPS PUB) 81, 26 pages.

(1981)
CODEN:FIPPAT

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

Federal Information Processing Standards Publication 81

1980 December 2

ANNOUNCING THE STANDARD FOR

DES MODES OF OPERATION

Federal Information Processing Standards Publications 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).

1. **Name of Standard.** DES Modes of Operation.

2. **Category of Standard.** ADP Operations, computer security.

3. **Explanation.** The Federal Data Encryption Standard (DES) (FIPS 46) specifies a cryptographic algorithm to be used for the cryptographic protection of sensitive, but unclassified, computer data. This FIPS defines four modes of operation for the DES which may be used in a wide variety of applications. The modes specify how data will be encrypted (cryptographically protected) and decrypted (returned to original form). The modes included in this standard are the Electronic Codebook (ECB) mode, the Cipher Block Chaining (CBC) mode, the Cipher Feedback (CFB) mode, and the Output Feedback (OFB) mode.

The body of this standard provides specifications of the recommended modes of operation but does not specify the necessary and sufficient conditions for their secure implementation in a particular application. This standard specifies the numbering of data bits, how the bits are encrypted and decrypted, and the data paths and the data processing necessary for encrypting and decrypting data or messages. This standard is based on (and references) the DES and provides the next level of detail necessary for providing compatibility among DES equipment. This standard anticipates the development of a set of application standards which reference it such as communication security standards, data storage standards, password protection standards and key management standards. Cryptographic system designers or security application designers must select one or more of the possible modes of operation for implementing and using the DES in a cryptographic system or security application. The Appendices to this standard provide tutorial information on the modes of operation and examples for validating their correct implementation. The Appendices are guidelines and are not mandatory requirements of this standard.

4. **Approving Authority.** Secretary of Commerce.

5. **Maintenance Agency.** U.S. Department of Commerce, National Bureau of Standards, Institute for Computer Sciences and Technology.

6. **Related Documents.**

FIPS PUB 46, "Data Encryption Standard," January 15, 1977.

(Proposed) Federal Standard 1026, "Telecommunications: Interoperability Requirements for Use of the Data Encryption Standard," May 20, 1980, draft.

(Proposed) Federal Standard 1027, "Telecommunications: Security Requirements for Use of the Data Encryption Standard," August 5, 1980, draft.

A list of currently approved FIPS may be obtained from the Standards Administration Office, Institute for Computer Sciences and Technology, National Bureau of Standards, Washington, DC 20234.

7. **Applicability.** This standard shall be used by Federal departments and agencies when procuring equipment or services which implement the Data Encryption Standard and which are intended for use in the cryptographic protection of sensitive, but unclassified, computer data. This standard may be used by anyone desiring to implement and use the Data Encryption Standard. The selection of one of the specified modes of operation will depend on the particular application being considered.

8. **Specifications.** Federal Information Processing Standard (FIPS 81) DES Modes of Operation (affixed).

9. **Qualifications.** The DES modes of operation described in this standard are based upon information provided by many sources within the Federal Government and private industry. These modes are presently being implemented in cryptographic equipment containing DES devices. However, a standard of this nature must, of necessity, remain flexible enough to adapt to advancements and innovations in science and technology. As such, this standard should not be construed as being either exhaustive or static. It will be reviewed every five years in order to incorporate new implementations whose technical and economic merit justify the issuance of a revised standard. FIPS 46 requires implementations of the DES algorithm in electronic devices when used by Federal departments and agencies. The DES, itself, must therefore be in hardware or firmware for Federal applications. However, the modes of operation specified in this standard may be implemented in software, hardware, or firmware.

10. **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.

11. **Patents.** Cryptographic equipment implementing this standard may be covered by U.S. and foreign patents.

12. **Implementation Schedule.** This standard becomes effective on June 2, 1981.

13. **Waivers.** Heads of agencies may request that the requirements of this standard be waived in instances where it can be clearly demonstrated that there are appreciable performance or cost advantages to be gained and when the overall interests of the Federal Government are best served by granting the requested waiver. Such waiver requests will be reviewed by and are subject to the approval of the Secretary of Commerce. The waiver request must specify anticipated performance and cost advantages in the justification for the waiver.

Forty-five days should be allowed for review and response by the Secretary of Commerce. Waiver requests shall be submitted to the Secretary of Commerce, Washington, DC 20230, and labeled as a Request for a Waiver to this Federal Information Processing Standard. No agency shall take any action to deviate from this standard prior to the receipt of a waiver approval from the Secretary of Commerce. No agency shall implement or procure equipment using a DES mode of operation not conforming to this standard unless a waiver has been approved.

14. **Where to Obtain Copies.** 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 81 (FIPS PUB 81), and title. When microfiche is desired, this should be specified. Payment may be made by check, money order, or deposit account.

Federal Information Processing Standards Publication 81

1980 December 2

Specifications for

DES MODES OF OPERATION

CONTENTS

FIGURES

TABLES

APPENDICES

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.