

Guide to

Modes of operation for a 64-bit block cipher algorithm

Committees responsible for this British Standard

The preparation of this British Standard was entrusted by the Information Systems Technology Standards Policy Committee (IST/-) to Technical Committee IST/33, upon which the following bodies were represented:

- Association for Payment Clearing Services
- Association of Cryptographic and Security Equipment Manufacturers
- British Computer Society
- British Telecommunications plc
- Business Equipment and Information Technology Association
- Communications-electronics Security Group (CESG CCTA)
- Computing Services Association
- Department of Trade and Industry (National Physical Laboratory)
- EEA (The Association of Electronics, Telecommunications and Business Equipment Industries)
- Government Communications Headquarters
- HM Treasury (Central Computer and Telecommunications Agency)
- Institute of Data Processing Management
- Ministry of Defence
- National Computer Users Forum
- National Computing Centre Ltd.
- Telecommunication Engineering and Manufacturing Association (TEMA)
- Coopted member

This British Standard, having been prepared under the direction of the Information Systems Technology Standards Policy Committee, was published under the authority of the Standards Board and comes into effect on 30 April 1991

© BSI 02-2000

The following BSI references relate to the work on this standard:
Committee reference IST 33
Draft for comment 83 61953 DC

ISBN 0 580 17786 6

Amendments issued since publication

Amd. No.	Date	Comments

Contents

	Page
Committees responsible	Inside front cover
National foreword	ii
1 Scope and field of application	1
2 Reference	1
3 Definitions	1
4 Notation	1
5 Electronic Codebook (ECB) mode	2
6 Cipher Block Chaining (CBC) mode	2
7 Cipher Feedback (CFB) mode	3
8 Output Feedback (OFB) mode	5
Annex A Properties of the modes of operation	7
Figure 1 — Cipher Block Chaining (CBC) mode of operation	3
Figure 2 — Cipher Feedback (CFB) mode of operation	4
Figure 3 — Output Feedback (OFB) mode of operation	6
Publication(s) referred to	Inside back cover

National foreword

This British Standard has been prepared under the direction of the Information Systems Technology Standards Policy Committee (IST/-). It is the UK implementation of, and is identical to, ISO 8372:1987 “*Information processing — Modes of operation for a 64-bit block cipher algorithm*”, published by the International Organization for Standardization (ISO), except that the title of the British Standard differs in order to more accurately reflect the actual contents of the text.

This standard implements the international text without change for the reasons given (see “Reasons for implementation”).

The UK actively participated in the development of the International Standard through BSI Technical Committee IST/33 and fully approved publication of the International Standard.

There are no plans at present to supplement this British Standard with any additional guidance, and any comments or enquiries on the International Standard or its application should be addressed to the Secretary to IST/33 at the BSI London address.

Reasons for implementation

- a) Because information technology equipment, services and systems tend to be, and generally need to be, designed, purchased and used in a world-wide context IST/- policy is to agree, wherever possible, standards at international level and not to prepare unique national standards. At the time of its approval, the text of the International Standard was considered to be the best that could be achieved, taking into account both the needs of the “market place” and the “state of the art” in this subject area, and the international standardization process.
- b) Further development of the international text at international level has been accorded relatively low priority in relation to other projects in the same international committee.
- c) Publication of British Standards corresponding to the International Standards in which IST/- resources were invested will ensure that the BSI Catalogue becomes, and then remains, a comprehensive first source of information for UK users of Information Technology equipment and services about the availability of International Standards on Information Technology subjects. In turn, this will facilitate UK use of, and access to, those standards.

Cross-reference

The Technical Committee has reviewed the provisions of ANSI X3.92:1981 “Data Encryption Algorithm” to which reference is made in the text, and has decided that it is acceptable for use in conjunction with this British Standard.

Publications of the American National Standards Institute (ANSI) can be obtained from *the BSI Sales Department, Linford Wood, Milton Keynes, MK14 6LE*.

Information on the availability of interim ISO documents, as well as up-to-date information on existing and projected British Standards publications in the general area of Information Technology, is included in the “BASIC LIST” and regular Newsletter published as part of the BSI Information Technology Services (BITS) initiative.

For details, contact:

*Marketing Department
BSI
Linford Wood
Milton Keynes
MK14 6LE*

A British Standard does not purport to include all the necessary provisions of a contract. Users of British Standards are responsible for their correct application.

Compliance with a British Standard does not of itself confer immunity from legal obligations.

Summary of pages

This document comprises a front cover, an inside front cover, pages i to iv, pages 1 to 8, an inside back cover and a back cover.

This standard has been updated (see copyright date) and may have had amendments incorporated. This will be indicated in the amendment table on the inside front cover.