

Information technology — Security techniques — Modes of operation for an n -bit block cipher

ICS 35.040

NO COPYING WITHOUT BSI PERMISSION EXCEPT AS PERMITTED BY COPYRIGHT LAW

BSI
Documents

AVA

Document Sharing Hub

National foreword

This British Standard reproduces verbatim ISO/IEC 10116:1997 and implements it as the UK national standard. It supersedes BS ISO/IEC 10116:1991 which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee IST/33, Information technology — Security techniques, which has the responsibility to:

- aid enquirers to understand the text;
- present to the responsible international/European committee any enquiries on the interpretation, or proposals for change, and keep the UK interests informed;
- monitor related international and European developments and promulgate them in the UK.

A list of organizations represented on this committee can be obtained on request to its secretary.

Cross-references

The British Standards which implement international or European publications referred to in this document may be found in the BSI Standards Catalogue under the section entitled “International Standards Correspondence Index”, or by using the “Find” facility of the BSI Standards Electronic Catalogue.

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 and ii, the ISO/IEC title page, pages ii to iv, pages 1 to 12, 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.

Amendments issued since publication

Amd. No.	Date	Comments

This British Standard, having been prepared under the direction of the DISC Board, was published under the authority of the Standards Committee and comes into effect on 15 December 1998

© BSI 06-1999

ISBN 0 580 30925 8

Contents

	Page
National foreword	Inside front cover
Foreword	iii
Text of ISO/IEC 10116	1

INTERNATIONAL
STANDARD

**ISO/IEC
10116**

Second edition
1997-04-15

**Information technology — Security
techniques — Modes of operation for an
n-bit block cipher**

*Technologies de l'information — Techniques de sécurité — Modes
opératoires d'un chiffrement par blocs de *n*-bits*



Reference number
ISO/IEC 10116:1997(E)



Documents

Document Sharing Hub

Contents

	Page
Foreword	iii
1 Scope	1
2 Definitions	1
3 Notation	1
4 Requirements	2
5 Electronic Codebook (ECB) Mode	2
6 Cipher Block Chaining (CBC) Mode	2
7 Cipher Feedback (CFB) Mode	2
8 Output Feedback (OFB) Mode	4
Annex A (informative) Properties of the modes of operation	7
Annex B (informative) Information about patents	10
Annex C (informative) Examples for the modes of operation	10
Annex D (informative) Bibliography	Inside back cover
Figure 1 — The cipher block chaining (CBC) mode of operation	5
Figure 2 — The cipher feedback (CFB) mode of operation	5
Figure 3 — The output feedback (OFB) mode of operation	6
Table C.1 — ECB mode, encipherment	10
Table C.2 — ECB mode, decipherment	11
Table C.3 — CBC mode, encipherment	11
Table C.4 — CBC mode, decipherment	11
Table C.5 — CFB mode, encipherment	11
Table C.6 — CFB mode, decipherment	11
Table C.7 — OFB mode, encipherment	11
Table C.8 — OFB mode, decipherment	12

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

International Standard ISO/IEC 10116 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

This second edition cancels and replaces the first edition (ISO/IEC 10116:1991), which has been technically revised.

Annex A to Annex D of this International Standard are for information only.

Descriptors: Data processing, information interchange, protection of information, security techniques, coded representation, algorithms.