INTERNATIONAL STANDARD

ISO/IEC 10116

Third edition
2006-02-01

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

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

Reference number
ISO/IEC 10116:2006(E)

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Figures

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.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. 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.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identfying any or all such patent rights.

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

This third edition cancels and replaces the second edition (ISO/IEC 10116:1997) which has been revised. Implementations that comply with ISO/IEC 10116:1997 will also comply with this third edition.

The main technical changes between the second edition and this third edition are as follows:

a) CBC mode has been extended to permit interleaving; and

b) a new mode (Counter mode) has been introduced.

Introduction

ISO/IEC 10116 specifies modes of operation for an n-bit block cipher. These modes provide methods for encrypting and decrypting data where the bit length of the data may exceed the size n of the block cipher.

This third edition of ISO/IEC 10116 specifies five modes of operation:

a) Electronic Codebook (ECB);

b) Cipher Block Chaining (CBC);

c) Cipher Feedback (CFB);

d) Output Feedback (OFB); and

e) Counter (CTR).

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

1 Scope

This International Standard establishes five modes of operation for applications of an n-bit block cipher (e.g. protection of data transmission, data storage). The defined modes only provide protection of data confidentiality. Protection of data integrity and requirements for padding the data are not within the scope of this International Standard. Also most modes do not protect the confidentiality of message length information.

This International Standard specifies the modes of operation and gives recommendations for choosing values of parameters (as appropriate).

The modes of operation specified in this International Standard have been assigned object identifiers in accordance with ISO/IEC 9834. The list of assigned object identifiers is given in Annex A. In applications in which object identifiers are used, the object identifiers specified in Annex A are to be used in preference to any other object identifiers that may exist for the mode concerned.

NOTE Annex B (informative) contains comments on the properties of each mode. Block ciphers are specified in ISO/IEC 18033-3.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 18033-3, *Information technology – Security techniques – Encryption algorithms – Part 3: Block ciphers.*