INTERNATIONAL
STANDARD

ISO/IEC 10116

Fourth edition
2017-07

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 10116:2017(E)

COPYRIGHT PROTECTED DOCUMENT

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Contents

Page

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.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

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 identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see the following URL: www.iso.org/iso/foreword.html.

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

This fourth edition cancels and replaces the third edition (ISO/IEC 10116:2006) and ISO/IEC 10116:2006/Cor1:2008, which have been technically revised.

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

a) the inclusion of padding within the normative scope of ISO/IEC 10116;

b) the inclusion of methods for avoiding ciphertext expansion for CBC, CFB, OFB and CTR modes.

Introduction

This document specifies modes of operation for an *n*-bit block cipher. These modes provide methods for encrypting and decrypting data using a block cipher.

This fourth 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);

e) Counter (CTR).

NOTE Annex C presents figures describing the modes of operation. Annex D provides numerical examples of the modes of operation.

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

1 Scope

This document establishes five modes of operation for applications of an *n*-bit block cipher (e.g. protection of data during transmission or in storage). The defined modes only provide protection of data confidentiality. Protection of data integrity is not within the scope of this document. Also, most modes do not protect the confidentiality of message length information.

NOTE 1 Methods for protecting the integrity of data using a block cipher are provided in ISO/IEC 9797-1.

NOTE 2 Methods for simultaneously protecting the confidentiality and integrity of data are provided in ISO/IEC 19772.

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

NOTE 3 The modes of operation specified in this document 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 can exist for the mode concerned.

NOTE 4 Annex B contains comments on the properties of each mode and important security guidance.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements 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*.

ISO/IEC 29192-2, *Information technology — Security techniques — Lightweight cryptography — Part 2: Block ciphers*.