AS ISO/IEC 10116:2019

Australian STANDARD

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

STANDARDS Australia

AS ISO/IEC 10116:2019

This Australian Standard® was prepared by IT-005, Financial Transaction Systems. It was approved on behalf of the Council of Standards Australia on 5 August 2019.

This Standard was published on 28 August 2019.

The following are represented on Committee IT-005:

Australian Payments Network
EFTPOS Payments Australia
New Payments Platform Australia

Additional Interests

American Express
ANZ Banking Group
Coles Group
Commonwealth Bank of Australia
Diebold Nixdorf
Eracom Technologies Australia
FIS Global
Gemalto
Mag-Tek
National Australia Bank
Pacific Research
SWIFT
Thales eSecurity
Triton Systems of Delaware LLC
UL Transaction Security
Westpac Banking Corporation
Woolworths Group

This Standard was issued in draft form for comment as DR AS ISO/IEC 10116:2019.

Keeping Standards up-to-date

Ensure you have the latest versions of our publications and keep up-to-date about Amendments, Rulings, Withdrawals, and new projects by visiting:
www.standards.org.au

ISBN 978 1 76072 559 4

AS ISO/IEC 10116:2019
ISO/IEC 10116:2017

Australian STANDARD

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

Originated as part of AS 2805.5—1985.
Revised and redesignated as AS 2805.5.2—1992.
Previous edition 2009.
Revised and redesignated as AS ISO/IEC 10116:2019.

COPYRIGHT

© ISO/IEC 2019 — All rights reserved
© Standards Australia Limited 2019

All rights are reserved. No part of this work may be reproduced or copied in any form or by any means, electronic or mechanical, including photocopying, without the written permission of the publisher, unless otherwise permitted under the Copyright Act 1968 (Cth).

Preface

This Standard was prepared by the Standards Australia Committee IT-005, Financial Transaction Systems, to supersede AS ISO 2805.5.2—2009, *Electronic funds transfer — Requirements for interfaces, Part 5.2: Ciphers — Modes of operation for an n-bit block cipher.*

The objective of this Standard is to establish 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.

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

This Standard is identical with, and has been reproduced from, ISO/IEC 10116:2017, *Information technology — Security techniques — Modes of operation for an n-bit block cipher.*

As this document has been reproduced from an International Standard, a full point substitutes for a comma when referring to a decimal marker.

Australian or Australian/New Zealand Standards that are identical adoptions of international normative references may be used interchangeably. Refer to the online catalogue for information on specific Standards.

The terms “normative” and “informative” are used in Standards to define the application of the appendices or annexes to which they apply. A “normative” appendix or annex is an integral part of a Standard, whereas an “informative” appendix or annex is only for information and guidance.

© Standards Australia Limited 2019

Contents

Preface ii

Foreword iv

Introduction v

1 Scope 1

2 Normative references 1

3 Terms and definitions 1

4 Symbols, abbreviated terms and notation 3
4.1 Symbols and abbreviated terms 3
4.2 Notation 4

5 Requirements 4

6 Electronic Codebook (ECB) mode 5
6.1 Preliminaries 5
6.2 Encryption 5
6.3 Decryption 5

7 Cipher Block Chaining (CBC) mode 6
7.1 Preliminaries 6
7.2 Encryption 6
7.3 Decryption 6
7.4 Avoiding ciphertext expansion 7
7.4.1 General 7
7.4.2 Three ciphertext stealing variants of CBC 7

8 Cipher Feedback (CFB) mode 8
8.1 Preliminaries 8
8.2 Encryption 9
8.3 Decryption 10
8.4 Avoiding ciphertext expansion 10

9 Output Feedback (OFB) mode 11
9.1 Preliminaries 11
9.2 Encryption 11
9.3 Decryption 12
9.4 Avoiding ciphertext expansion 12

10 Counter (CTR) mode 13
10.1 Preliminaries 13
10.2 Encryption 13
10.3 Decryption 14
10.4 Avoiding ciphertext expansion 14

Annex A (normative) **Object identifiers** 15

Annex B (informative) **Properties of the modes of operation and important security guidance** 17

Annex C (informative) **Figures describing the modes of operation** 22

Annex D (informative) **Numerical examples for the modes of operation** 27

Bibliography 38

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.

© Standards Australia Limited 2019

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.

© Standards Australia Limited 2019

Australian Standard®

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*.

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— IEC Electropedia: available at http://www.electropedia.org/

— ISO Online browsing platform: available at http://www.iso.org/obp

3.1
block cipher
symmetric encipherment system with the property that the encryption algorithm operates on a block of plaintext, i.e. a string of bits of a defined length, to yield a block of ciphertext

[SOURCE: ISO/IEC 18033-1:2015, 2.9]

3.2
ciphertext
data which has been transformed to hide its information content

[SOURCE: ISO/IEC 18033-1:2015, 2.11]

© Standards Australia Limited 2019