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)

© ISO/IEC 2006

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS

Not for Resale

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/IEC 2006

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

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

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Contents

Page

Foreword . . . vii

1 Scope . . . 1

2 Normative references . . . 1

3 Terms and definitions . . . 2

4 Symbols (and abbreviated terms) . . . 3

5 Requirements . . . 5

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

7 Cipher Block Chaining (CBC) mode . . . 6
7.1 Preliminaries . . . 6
7.2 Encryption . . . 7
7.3 Decryption . . . 7

8 Cipher Feedback (CFB) mode . . . 8
8.1 Preliminaries . . . 8
8.2 Encryption . . . 8
8.3 Decryption . . . 9

9 Output Feedback (OFB) mode . . . 10
9.1 Preliminaries . . . 10
9.2 Encryption . . . 10
9.3 Decryption . . . 11

10 Counter (CTR) mode . . . 11
10.1 Preliminaries . . . 11
10.2 Encryption . . . 12
10.3 Decryption . . . 12

Annex A (normative) Object identifiers . . . 14

Annex B (informative) Properties of the modes of operation . . . 16
B.1 Properties of the Electronic Codebook (ECB) mode of operation . . . 16
B.2 Properties of the Cipher Block Chaining (CBC) mode of operation . . . 17
B.3 Properties of the Cipher Feedback (CFB) mode of operation . . . 18
B.4 Properties of the Output Feedback (OFB) mode of operation . . . 20
B.5 Properties of the Counter (CTR) mode of operation . . . 21

Annex C (informative) Figures describing the modes of operation . . . 23

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale