This is a preview of "ISO/IEC 18033-3:2010". Click here to purchase the full version from the ANSI store.

INTERNATIONAL ISO/IEC

Second edition
2010-12-15

Information technology — Security techniques — Encryption algorithms —

Part 3: Block ciphers

Technologies de l'information — Techniques de sécurité — Algorithmes de chiffrement

Partie 3: Chiffrement par blocs

Reference number
ISO/IEC 18033-3:2010(E)

© ISO/IEC 2010

This is a preview of "ISO/IEC 18033-3:2010". Click here to purchase the full version from the ANSI store.

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.

COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2010

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

© ISO/IEC 2010 – All rights reserved

This is a preview of "ISO/IEC 18033-3:2010". Click here to purchase the full version from the ANSI store.

Contents

Page

Foreword v

1 Scope 1

2 Terms and definitions 1

3 Symbols 2

4 64-bit block ciphers 3
4.1 Introduction 3
4.2 TDEA 3
4.2.1 The Triple Data Encryption Algorithm 3
4.2.2 TDEA encryption/decryption 3
4.2.3 TDEA keying options 4
4.3 MISTY1 4
4.3.1 The MISTY1 algorithm 4
4.3.2 MISTY1 encryption 4
4.3.3 MISTY1 decryption 5
4.3.4 MISTY1 functions 5
4.3.5 MISTY1 key schedule 10
4.4 CAST-128 11
4.4.1 The CAST-128 algorithm 11
4.4.2 CAST-128 encryption 11
4.4.3 CAST-128 decryption 11
4.4.4 CAST-128 functions 11
4.4.5 CAST-128 key schedule 18
4.5 HIGHT 20
4.5.1 The HIGHT algorithm 20
4.5.2 HIGHT encryption 21
4.5.3 HIGHT decryption 22
4.5.4 HIGHT functions 23
4.5.5 HIGHT key schedule 23

5 128-bit block ciphers 24
5.1 Introduction 24
5.2 AES 24
5.2.1 The AES algorithm 24
5.2.2 AES encryption 24
5.2.3 AES decryption 25
5.2.4 AES transformations 26
5.2.5 AES key schedule 30
5.3 Camellia 32
5.3.1 The Camellia algorithm 32
5.3.2 Camellia encryption 32
5.3.3 Camellia decryption 34
5.3.4 Camellia functions 37
5.3.5 Camellia key schedule 43
5.4 SEED 47
5.4.1 The SEED algorithm 47
5.4.2 SEED encryption 47
5.4.3 SEED decryption 47
5.4.4 SEED functions 48
5.4.5 SEED key schedule 50

Annex A (normative) **Description of DES** 52

© ISO/IEC 2010 — All rights reserved

This is a preview of "ISO/IEC 18033-3:2010". Click here to purchase the full version from the ANSI store.

A.1 Introduction 52
A.2 DES encryption 52
A.3 DES decryption 52
A.4 DES functions 52
A.4.1 Initial permutation *IP* 52
A.4.2 Inverse initial permutation IP^{-1} 54
A.4.3 Function *f* 54
A.4.4 Expansion permutation *E* 55
A.4.5 Permutation *P* 55
A.4.6 S-Boxes 56
A.5 DES key schedule 57

Annex B (normative) **Object identifiers** 60

Annex C (informative) **Algebraic forms of MISTY1 and Camellia S-boxes** 62
C.1 Introduction 62
C.2 MISTY1 S-boxes 62
C.2.1 The S-boxes S_7 and S_9 62
C.2.2 MISTY1 S-box S_7 62
C.2.3 MISTY1 S-box S_9 62
C.3 Camellia S-boxes 63

Annex D (informative) **Test vectors** 64
D.1 Introduction 64
D.2 TDEA test vectors 64
D.2.1 TDEA encryption 64
D.2.2 DES encryption and decryption 65
D.3 MISTY1 test vectors 66
D.4 CAST-128 test vectors 67
D.5 HIGHT test vectors 67
D.6 AES test vectors 67
D.6.1 AES encryption 67
D.6.2 Key expansion example 68
D.6.3 Cipher example 70
D.7 Camellia test vectors 73
D.7.1 Introduction 73
D.7.2 Camellia encryption 73
D.8 SEED test vectors 75

Annex E (informative) **Feature table** 77

Bibliography 78

 © ISO/IEC 2010 — All rights reserved

This is a preview of "ISO/IEC 18033-3:2010". Click here to purchase the full version from the ANSI store.

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 identifying any or all such patent rights.

ISO/IEC 18033-3 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 18033-3:2005), which has been technically revised. It also incorporates the Technical Corrigenda ISO/IEC 18033-3:2005/Cor.1:2006, ISO/IEC 18033-3:2005/Cor.2:2007 and ISO/IEC 18033-3:2005/Cor.3:2008.

ISO/IEC 18033 consists of the following parts, under the general title *Information technology — Security techniques — Encryption algorithms*:

— *Part 1: General*

— *Part 2: Asymmetric ciphers*

— *Part 3: Block ciphers*

— *Part 4: Stream ciphers*

© ISO/IEC 2010 — All rights reserved