INTERNATIONAL STANDARD

ISO/IEC 18033-1

First edition
2005-02-01

AMENDMENT 1
2011-03-01

Information technology — Security techniques — Encryption algorithms —

Part 1: **General**

AMENDMENT 1

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

Partie 1: Généralités

AMENDEMENT 1

Reference number
ISO/IEC 18033-1:2005/Amd.1:2011(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.

COPYRIGHT PROTECTED DOCUMENT

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

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.

Amendment 1 to ISO/IEC 18033-1:2005 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

ISO/IEC 18033 specifies encryption systems (ciphers) for the purpose of data confidentiality. The inclusion of ciphers in ISO/IEC 18033 is intended to promote their use as reflecting the current ‘state of the art’ in encryption techniques.

ISO/IEC 18033-1:2005 is general in nature, and provides definitions that apply in subsequent parts of ISO/IEC 18033. All documents referenced in ISO/IEC 18033-1:2005 are only cited in an informative manner or merely served as bibliographic or background material in its preparation. ISO/IEC 18033-1:2005 does not contain any normative references.

Revised or new documents are continually being prepared by ISO/IEC JTC 1/SC 27, *IT Security techniques*. Although it is necessary for the technical work to progress speedily, sufficient time is required before the approval stage for discussions, negotiations and resolutions. Thus SC 27 resolved to provide a timely and cost-effective revision for the bibliographic references through Amendment 1 to ISO/IEC 18033-1:2005.

Information technology — Security techniques — Encryption algorithms —

Part 1: **General**

AMENDMENT 1

Page 8, Bibliography

Replace the Bibliography with the following:

Bibliography

[1] ISO/IEC 9796 (all parts), *Information technology — Security techniques — Digital signature schemes giving message recovery*

[2] ISO/IEC 9797 (all parts), *Information technology — Security techniques — Message Authentication Codes (MACs)*

[3] ISO/IEC 9798-1:1997 [1], *Information technology — Security techniques — Entity authentication — Part 1: General*

[4] ISO/IEC 10116, *Information technology — Security techniques — Modes of operation for an n-bit block cipher*

[5] ISO/IEC 10118-2, *Information technology — Security techniques — Hash-functions — Part 2: Hash-functions using an n-bit block cipher*

[6] ISO/IEC 11770 (all parts), *Information technology — Security techniques — Key management*

[7] ISO/IEC 14888 (all parts), *Information technology — Security techniques — Digital signatures with appendix*

[8] ISO/IEC 15946-2, *Information technology — Security techniques — Cryptographic techniques based on elliptic curves — Part 2: Digital signatures*[2]

[9] ISO/IEC 15946-4, *Information technology — Security techniques — Cryptographic techniques based on elliptic curves — Part 4: Digital signatures giving message recovery*[3]

[10] ISO/IEC 19772, *Information technology — Security techniques — Authenticated encryption*

[1] ISO/IEC 9798-1:1997 has been cancelled and replaced by ISO/IEC 9798-1:2010.

[2] Withdrawn. Relevant content from ISO/IEC 15946-2 can now be found in ISO/IEC 14888 [7].

[3] Withdrawn. Relevant content from ISO/IEC 15946-4 can now be found in ISO/IEC 9796 [1].

ICS 35.040

Price based on 1 page