BS ISO/IEC 18033-1:2015

BSI Standards Publication

Information technology — Security techniques — Encryption algorithms

Part 1: General

bsi.

...making excellence a habit.™

Document Sharing Hub

Full document details: BS ISO/IEC 18033-1:2015

National foreword

This British Standard is the UK implementation of ISO/IEC 18033-1:2015. It supersedes BS ISO/IEC 18033-1:2005+A1:2011 which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee IST/33, IT - Security techniques.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© The British Standards Institution 2015. Published by BSI Standards Limited 2015

ISBN 978 0 580 76059 4

ICS 35.040

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 July 2015.

Amendments issued since publication

Date	Text affected

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 18033-1:2015

INTERNATIONAL STANDARD

ISO/IEC 18033-1

Second edition
2015-08-01

Information technology — Security techniques — Encryption algorithms —

Part 1: General

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

Partie 1: Généralités

Reference number
ISO/IEC 18033-1:2015(E)

Documents
Document Sharing Hub
© ISO/IEC 2015

Full document details: BS ISO/IEC 18033-1:2015

COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2015, Published in Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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

© ISO/IEC 2015 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 18033-1:2015

Contents

Page

Foreword ... **iv**

Introduction ... **v**

1 Scope ... **1**

2 Terms and definitions ... **1**

3 Symbols and abbreviated terms ... **5**
3.1 Symbols ... 5
3.2 Abbreviated terms ... 5

4 The nature of encryption ... **5**
4.1 The purpose of encryption ... 5
4.2 Symmetric and asymmetric ciphers ... 6
4.3 Key management ... 6

5 The use and properties of encryption ... **6**
5.1 Asymmetric ciphers ... 6
5.2 Block ciphers ... 7
5.2.1 General ... 7
5.2.2 Modes of operation ... 7
5.2.3 Message Authentication Codes (MACs) ... 7
5.3 Stream ciphers ... 7
5.4 Identity-based mechanisms ... 8

6 Object identifiers ... **8**

Annex A (normative) **Criteria for submission of ciphers for possible inclusion in this International Standard** ... **9**

Annex B (normative) **Criteria for the deletion of ciphers from this International Standard** ... **13**

Annex C (informative) **Attacks on encryption algorithms** ... **14**

Bibliography ... **16**

© ISO/IEC 2015 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 18033-1:2015

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 meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword - Supplementary information

The committee responsible for this document is ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Security techniques*.

This second edition cancels and replaces the first edition (ISO/IEC 18033-1:2005), which has been technically revised.

It also incorporates the Amendment, ISO/IEC 18033-1:2005/Amd.1:2011.

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*

— *Part 5: Identity-based ciphers*

© ISO/IEC 2015 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 18033-1:2015

Introduction

This multi-part International Standard specifies encryption systems (ciphers) for the purpose of data confidentiality. The inclusion of ciphers in this International Standard is intended to promote their use as reflecting the current "state of the art" in encryption techniques.

The primary purpose of encryption (or encipherment) techniques is to protect the confidentiality of stored or transmitted data. An encryption algorithm is applied to data (often called plaintext or cleartext) to yield encrypted data (or ciphertext); this process is known as encryption. The encryption algorithm should be designed so that the ciphertext yields no information about the plaintext except, perhaps, its length. Associated with every encryption algorithm is a corresponding decryption algorithm, which transforms ciphertext back into its original plaintext.

Ciphers work in association with a key. In a symmetric cipher, the same key is used in both the encryption and decryption algorithms. In an asymmetric cipher, different but related keys are used for encryption and decryption. In this multi-part International Standard, ISO/IEC 18033-2 and ISO/IEC 18033-5 are devoted to two different classes of asymmetric ciphers, known as conventional asymmetric ciphers (or just asymmetric ciphers), and identity-based ciphers. ISO/IEC 18033-3 and ISO/IEC 18033-4 are devoted to two different classes of symmetric ciphers, known as block ciphers and stream ciphers.

© ISO/IEC 2015 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 18033-1:2015

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 18033-1:2015

INTERNATIONAL STANDARD ISO/IEC 18033-1:2015(E)

Information technology — Security techniques — Encryption algorithms —

Part 1: General

1 Scope

This part of ISO/IEC 18033 is general in nature, and provides definitions that apply in subsequent parts of this International Standard. The nature of encryption is introduced, and certain general aspects of its use and properties are described. The criteria used to select the algorithms specified in subsequent parts of this International Standard are defined in Annexes A and B.

2 Terms and definitions

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

2.1
asymmetric cipher
alternative term for asymmetric encryption system

2.2
asymmetric cryptographic technique
cryptographic technique that uses two related transformations, a public transformation (defined by the public key) and a private transformation (defined by the private key)

Note1 to entry: The two transformations have the property that, given the public transformation, it is computationally infeasible to derive the private transformation

[SOURCE: ISO/IEC 11770-1:2010, 2.1]

2.3
asymmetric encipherment system
alternative term for asymmetric encryption system

2.4
asymmetric encryption system
system based on asymmetric cryptographic techniques whose public transformation is used for encryption and whose private transformation is used for decryption

[SOURCE: ISO/IEC 9798-1:2010, 3.2]

2.5
asymmetric key pair
pair of related keys for an asymmetric cryptographic technique where the private key defines the private transformation and the public key defines the public transformation

2.6
attack
algorithm that performs computations and makes queries to the encryption algorithm for the encryption and/or decryption of adaptively chosen texts under a single secret key, with the purpose of recovering either the unknown plaintext for a given ciphertext, which may be adaptively chosen but for which a decryption query is not issued, or a secret key

© ISO/IEC 2015 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 18033-1:2015