
**Information security — Encryption
algorithms —**

**Part 1:
General**

Sécurité de l'information — Algorithmes de chiffrement —

Partie 1: Généralités

ITeH Standards
(<https://standards.iteh.ai>)
Document Preview

[ISO/IEC 18033-1:2021](https://standards.iteh.ai/catalog/standards/iso/3c31efea-3403-4e5c-ae60-301a4befd3fe/iso-iec-18033-1-2021)

<https://standards.iteh.ai/catalog/standards/iso/3c31efea-3403-4e5c-ae60-301a4befd3fe/iso-iec-18033-1-2021>



Reference number
ISO/IEC 18033-1:2021(E)

© ISO/IEC 2021

iTeh Standards
(<https://standards.iteh.ai>)
Document Preview

[ISO/IEC 18033-1:2021](https://standards.iteh.ai/catalog/standards/iso/3c31efea-3403-4e5c-ae60-301a4befd3fe/iso-iec-18033-1-2021)

<https://standards.iteh.ai/catalog/standards/iso/3c31efea-3403-4e5c-ae60-301a4befd3fe/iso-iec-18033-1-2021>



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2021

All rights reserved. Unless otherwise specified, or required in the context of its implementation, 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
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier; Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword	iv
Introduction	v
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Symbols and abbreviated terms	5
5 Nature of encryption	5
5.1 Purpose of encryption	5
5.2 Symmetric and asymmetric encryption systems	6
5.3 Key management	6
6 Use and properties of encryption	6
6.1 General	6
6.2 Asymmetric encryption systems	7
6.3 Block ciphers	7
6.3.1 General	7
6.3.2 Modes of operation	7
6.3.3 Message authentication codes (MACs)	7
6.4 Stream ciphers	8
6.5 Identity-based encryption systems	8
6.6 Homomorphic encryption systems	8
7 Object identifiers	8
Annex A (informative) Criteria for submission of encryption systems for possible inclusion in the ISO/IEC 18033 series	9
Annex B (informative) Criteria for the deletion of encryption systems from the ISO/IEC 18033 series	14
Annex C (informative) Attacks on encryption algorithms	15
Bibliography	18

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.

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 or www.iec.ch/members_experts/refdocs).

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) or the IEC list of patent declarations received (see patents.iec.ch).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of 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 www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

This third edition cancels and replaces the second edition (ISO/IEC 18033-1:2015), which has been technically revised. The main changes compared with the previous edition are as follows:

- [Clause 3](#) has been refined;
- criteria for submission of encryption systems have been refined for possible inclusion in the ISO/IEC 18033 series; and
- the use and security properties of encryption algorithms have been clarified.

A list of all parts in the ISO/IEC 18033 series can be found on the ISO website.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.