BSI Standards Publication

Information security — Encryption algorithms

Part 1: General

bsi.

National foreword

This British Standard is the UK implementation of ISO/IEC 18033-1:2021. It supersedes BS ISO/IEC 18033-1:2015, which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee IST/33/2, Cryptography and Security Mechanisms.

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

Contractual and legal considerations

This publication has been prepared in good faith, however no representation, warranty, assurance or undertaking (express or implied) is or will be made, and no responsibility or liability is or will be accepted by BSI in relation to the adequacy, accuracy, completeness or reasonableness of this publication. All and any such responsibility and liability is expressly disclaimed to the full extent permitted by the law.

This publication is provided as is, and is to be used at the recipient's own risk.

The recipient is advised to consider seeking professional guidance with respect to its use of this publication.

This publication is not intended to constitute a contract. Users are responsible for its correct application.

Published by BSI Standards Limited 2021

ISBN 978 0 539 03456 1

ICS 35.030

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 October 2021.

Amendments/corrigenda issued since publication

Date	Text affected

INTERNATIONAL **ISO/IEC**

Third edition
2021-09-10

Information security — Encryption algorithms —

Part 1: General

Sécurité de l'information — Algorithmes de chiffrement —

Partie 1: Généralités

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

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

Contents

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.

Introduction

The ISO/IEC 18033 series specifies encryption systems for the purpose of data confidentiality. The inclusion of encryption systems in this document is intended to promote their use as reflecting the current state of the art in encryption systems.

The primary purpose of encryption systems is to protect the confidentiality of stored or transmitted data. An encryption algorithm is applied to data (often called plaintext) 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.

Encryption systems work in association with a key. In a symmetric encryption system, the same key is used in both the encryption and decryption algorithms. In an asymmetric encryption system, different but related keys are used for encryption and decryption. ISO/IEC 18033-2 and ISO/IEC 18033-5 focus on two different classes of asymmetric encryption systems, known as conventional asymmetric encryption systems (or just asymmetric encryption systems), and identity-based encryption systems. ISO/IEC 18033-3 and ISO/IEC 18033-4 focus on two different classes of symmetric encryption systems, known as block ciphers and stream ciphers. ISO/IEC 18033-6 focuses on a specific class of encryption systems called homomorphic.

This page deliberately left blank

Information security — Encryption algorithms —

Part 1: General

1 Scope

This document is general in nature and provides definitions that apply in subsequent parts of the ISO/IEC 18033 series.

It introduces the nature of encryption and describes certain general aspects of its use and properties.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 18033-2, *Information technology — Security techniques — Encryption algorithms — Part 2: Asymmetric ciphers*

ISO/IEC 18033-3, *Information technology — Security techniques — Encryption algorithms — Part 3: Block ciphers*

ISO/IEC 18033-4, *Information technology — Security techniques — Encryption algorithms — Part 4: Stream ciphers*

ISO/IEC 18033-5, *Information technology — Security techniques — Encryption algorithms — Part 5: Identity-based ciphers*

ISO/IEC 18033-6, *IT Security techniques — Encryption algorithms — Part 6: Homomorphic encryption*

ISO/IEC 18033-7, *Information technology — Security techniques — Encryption algorithms — Part 7: Tweakable block ciphers*

3 Terms and definitions

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

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

3.1
asymmetric cryptographic technique
cryptographic technique that uses two related transformations, a public transformation [defined by the *public key* (3.22)] and a private transformation [defined by the *private key* (3.21)]

Note 1 to entry: The two transformations have the property that, given the public transformation, it is computationally infeasible to derive the private transformation. Computational feasibility depends on the specific security requirements and environment.

[SOURCE: ISO/IEC 11770-1:2010, 2.1, modified — The last sentence in note 1 to entry has been added.]