INTERNATIONAL STANDARD

ISO/IEC 18033-1

Third edition
2021-09

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
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

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.

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.]

3.2
asymmetric encryption system
asymmetric cipher
asymmetric encipherment system
system based on *asymmetric cryptographic techniques* (3.1) whose public transformation is used for *encryption* (3.11) and whose private transformation is used for *decryption* (3.9)

Note 1 to entry: A method for *key* (3.17) pair generation is assumed.

[SOURCE: ISO/IEC 9798-1:2010, 3.2, modified — The admitted terms "asymmetric cipher" and "asymmetric encipherment system" and note 1 to entry have been added.]

3.3
attack
algorithm that performs computations and that can request the *encryption* (3.11) and/or *decryption* (3.9) of adaptively chosen texts under a single *secret key* (3.25)/*private key* (3.21), with the purpose of recovering either the unknown *plaintext* (3.20) for a given *ciphertext* (3.7), which may be adaptively chosen but for which a request to decrypt the ciphertext is not issued, or a secret key/private key

Note 1 to entry: Attacks are discussed in detail in Annex C.

3.4
attack cost
ratio of the average workload of the *attack* (3.3) to an equivalent number of calls to the *encryption algorithm* (3.12) under attack multiplied by the success probability of the attack

Note 1 to entry: Using the notation defined in Clause 4, the attack cost is equal to the ratio W/P.

Note 2 to entry: Other attack cost metrics and properties, such as memory complexity, data complexity, the ability to be accelerated by specialized hardware or parallelizability may also be important in judging the impact of a cryptographic attack.

3.5
block
string of bits of a defined length

3.6
block cipher
symmetric encryption system (3.29) with the property that the *encryption algorithm* (3.12) operates on a *block* (3.5) of *plaintext* (3.20) to yield a block of *ciphertext* (3.7)

Note 1 to entry: The block ciphers standardized in ISO/IEC 18033-3 have the property that plaintext and ciphertext blocks are of the same length.

3.7
ciphertext
data which has been transformed to hide its information content

3.8
cryptanalytic attack
attack (3.3) against a *cipher* (3.13) that makes use of properties of the cipher

Note 1 to entry: Every cryptanalytic attack has its own attack model, some of which may or may not be applicable to specific implementations. Since the application of a cipher is generally unknown to the cipher designer, all possible models in the single *key* (3.17) setting need to be considered when assessing the security of an algorithm. Several existing application examples also show the need to consider multi-key settings.

Note 2 to entry: Cryptanalytic attacks do not include implementation-specific attacks, e.g. involving side channel analysis.

3.9
decryption
decipherment
reversal of a corresponding *encryption* (3.11)

[SOURCE: ISO/IEC 11770-1:2010, 2.6, modified — The admitted term "decipherment" has been added; note 1 to entry has been removed.]

3.10
decryption algorithm
decipherment algorithm
process which transforms *ciphertext* (3.7) into *plaintext* (3.20)

3.11
encryption
encipherment
(reversible) transformation of data by an *encryption algorithm* (3.12) to produce *ciphertext* (3.7), i.e. to hide the information content of the data

3.12
encryption algorithm
encipherment algorithm
process which transforms *plaintext* (3.20) into *ciphertext* (3.7)

3.13
encryption system
encipherment system
cipher
cryptographic technique used to protect the confidentiality of data, and which consists of three component processes: an *encryption algorithm* (3.12), a *decryption algorithm* (3.10), and a method for generating *keys* (3.17)

3.14
generic attack
attack (3.3) against an *encryption system* (3.13) which does not rely on the encryption system design and can be used to recover a *secret key* (3.25)/*private key* (3.21) or *plaintext* (3.20)

Note 1 to entry: Generic attacks depend on models and goals, see Clause A.2 for details.

3.15
homomorphic encryption system
homomorphic cipher
homomorphic encipherment system
encryption system (3.13) with the property that if certain computations are performed on the *ciphertext* (3.7), the *plaintext* (3.20) obtained after *decryption* (3.9) will have had the same computations applied to it

3.16
identity-based encryption system
identity-based cipher
asymmetric encryption system (3.2) in which the *encryption algorithm* (3.12) takes an arbitrary string as a *public key* (3.22)

[SOURCE: ISO/IEC 18033-5:2015, 3.6, modified — The preferred term has been changed to "identity-based encryption system"; "identity-based cipher" has been changed to an admitted term; "asymmetric cipher" has been changed to "asymmetric encryption system".]

3.17
key
sequence of symbols that controls the operation of a cryptographic transformation [e.g. *encryption* (3.11), *decryption* (3.9)]

[SOURCE: ISO/IEC 11770-1:2010, 2.12, modified — The list of cryptographic mechanisms has been removed.]

3.18
keystream
pseudorandom sequence of symbols, intended to be secret, used by the *encryption* (3.11) and *decryption algorithms* (3.10) of a *stream cipher* (3.27)

Note 1 to entry: If a portion of the keystream is known by an attacker, then it shall be computationally infeasible for the attacker to deduce more than a negligible amount of information about the remainder of the keystream. Computational feasibility depends on the specific security requirements and environment.

3.19
***n*-bit block cipher**
block cipher (3.6) with the property that *plaintext* (3.20) *blocks* (3.5) and *ciphertext* (3.7) blocks are *n* bits in length

3.20
plaintext
cleartext
unencrypted information

3.21
private key
key (3.17) of an entity's key pair which is known only by that entity

[SOURCE: ISO/IEC 9594-8:2020, 3.5.50, modified — The parenthesis "(In a public-key cryptosystem)", "That" at the beginning of the definition and the period at the end have been deleted.]

3.22
public key
key (3.17) of an entity's key pair which is publicly known

[SOURCE: ISO/IEC 9594-8:2020, 3.5.57, modified — "That" at the beginning of the definition and the period at the end have been deleted.]

3.23
public-key certificate
public key (3.22) of an entity, together with some other information, rendered unforgeable by digital signature with the *private key* (3.21) of the certification authority that issued it

[SOURCE: ISO/IEC 9594-8:2020, 3.5.58, modified — "The" at the beginning of the definition, the parenthesis "(CA)" and the period at the end have been deleted.]

3.24
public-key infrastructure
PKI
infrastructure able to support the management of *public keys* (3.22) able to support authentication, *encryption* (3.11), integrity or non-repudiation services

[SOURCE: ISO/IEC 9594-8:2020, 3.5.60, modified — "The" at the beginning of the definition and the period at the end have been deleted.]