DRAFT INTERNATIONAL STANDARD

ISO/IEC DIS 18033-1

ISO/IEC JTC **1**/SC **27**

Secretariat: **DIN**

Voting begins on:
2020-11-27

Voting terminates on:
2021-02-19

Information security — Encryption algorithms —

Part 1:
General

Partie 1: Généralités

ICS: 35.030

This document is circulated as received from the committee secretariat.

Reference number
ISO/IEC DIS 18033-1:2020(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) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

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 ISO documents 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 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 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.

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 to the previous edition are as follows:

— Refining terminology;

— Refining criteria for submission of ciphers for possible inclusion in the ISO/IEC 18033 series; and

— Clarification of the use and security properties of encryption algorithms.

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.

Introduction

This ISO/IEC 18033 series specifies encryption systems (ciphers) for the purpose of data confidentiality. The inclusion of ciphers in this document 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 ISO/IEC 18033 series, 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 18033-6 is devoted to a specific class of encryption algorithms 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. The nature of encryption is introduced, and certain general aspects of its use and properties are described.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

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

ISO and IEC maintain terminological 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) and a private transformation (defined by the private key)

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]]

3.2
asymmetric encryption system
asymmetric cipher
asymmetric encipherment system
system based on asymmetric cryptographic techniques whose public transformation is used for encryption and whose private transformation is used for decryption

Note 1 to entry: A method for key pair generation is assumed.

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

3.3
attack
algorithm that performs computations and that can request the encryption and/or decryption of adaptively chosen texts under a single secret/private key, with the purpose of recovering either the unknown plaintext for a given ciphertext, which may be adaptively chosen but for which a request to decrypt the ciphertext is not issued, or a secret/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 to an equivalent number of calls to the encryption algorithm under attack multiplied by the success probability of the attack

Note 1 to entry: Using the notation defined in 4.1, 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 encipherment system with the property that the encryption algorithm operates on a block of plaintext to yield a block of ciphertext

Note 1 to entry: The block ciphers standardised 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 against a cipher 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 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

[SOURCE: ISO/IEC 11770-1:2010, 2.6]

3.10
decryption algorithm
decipherment algorithm
process which transforms ciphertext into plaintext

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

[SOURCE: ISO/IEC 9797-1:2011, 3.6, modified – editorial change]

3.12
encryption algorithm
encipherment algorithm
process which transforms plaintext into ciphertext

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, a decryption algorithm, and a method for generating keys

3.14
generic attack
attack against a cipher which does not rely on the cipher design and can be used to recover a secret/ private key or plaintext

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

3.15
identity-based encryption system
identity-based cipher
asymmetric cipher in which the encryption algorithm takes an arbitrary string as a public key

[SOURCE: ISO/IEC 18033-5:2015, 3.6]

3.16
key
sequence of symbols that controls the operation of a cryptographic transformation (e.g., encipherment, decipherment)

[SOURCE: ISO/IEC 11770-1:2010, 2.12, modified – the list of cryptographic mechanisms is removed]

3.17
keystream
pseudorandom sequence of symbols, intended to be secret, used by the encryption and decryption algorithms of a stream cipher

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.

3.18
***n*-bit block cipher**
block cipher with the property that plaintext blocks and ciphertext blocks are *n* bits in length

3.19
plaintext
cleartext
unencrypted information

3.20
private key
key of an entity's asymmetric key pair which should only be used by that entity

Note 1 to entry: A private key should not normally be disclosed.

[SOURCE: ISO/IEC 11770-1:2010, 2.35, modified – editorial change, new text of a note]

3.21
public key
key of an entity's asymmetric key pair which can usually be made public without compromising security

[SOURCE: ISO/IEC 11770-1:2010, 2.36]

3.22
public key certificate
public key information of an entity signed by the certification authority and thereby rendered unforgeable

[SOURCE: ISO/IEC 11770-3:2015, 3.34]

3.23
public key infrastructure
PKI
infrastructure able to support the management of public keys able to support authentication, encryption, integrity or non-repudiation services

[SOURCE: ISO/IEC 9594-8:2017, 3.5.59]

3.24
secret key
key used with symmetric cryptographic techniques by a specified set of entities

[SOURCE: ISO/IEC 11770-3:2015, 3.36]

3.25
security strength
number associated with the amount of work (e.g. the number of operations) that is required to break a cryptographic algorithm

Note 1 to entry: For key recovery, a security strength of k bits implies that the workload required to break the encryption system is equivalent to 2^k executions of the encryption system. For further information on the application of security strength to selecting cryptographic algorithms for this document, see C.1.4.

3.26
stream cipher
symmetric encryption system with the property that the encryption algorithm involves combining a sequence of plaintext symbols with a sequence of keystream symbols one symbol at a time, using an invertible function

Note 1 to entry: Two types of stream cipher can be identified: synchronous stream ciphers and self-synchronous stream ciphers, distinguished by the method used to obtain the keystream.

3.27
symmetric cryptographic technique
cryptographic technique for which all transformations use the same key

3.28
symmetric encryption system
symmetric encipherment system
symmetric cipher
encryption system based on symmetric cryptographic techniques

3.29
homomorphic cipher
homomorphic encryption system
homomorphic encipherment system
encryption system with the property that if certain computations are performed on the ciphertext, the plaintext obtained after decryption will have had the same computations applied to it

4 Symbols and abbreviated terms

4.1 Symbols

For the purposes of this document, the following symbols apply.

n	Plaintext/ciphertext block length for a block cipher
k	Key length
P	The probability that a cryptanalytic attack will succeed
W	Workload or complexity of an attack, measured in terms of the number of calls to the cryptographic algorithm

4.2 Abbreviated terms

For the purposes of this document, the following abbreviated terms apply.

ECB	Electronic Code Book
MAC	Message authentication code
SC	Subcommittee
SD	Standing document
WG	Working group

5 The nature of encryption

5.1 The purpose of encryption

The primary purpose of encryption (or encipherment) systems is to protect the confidentiality of stored or transmitted data. Encryption algorithms achieve this by transforming plaintext into ciphertext, from which it is computationally infeasible to find any information about the content of the plaintext unless the secret/private key is also known. However, in many cases the length of the ciphertext will not be concealed by encryption, since the length of the ciphertext will typically be the same as, or a little larger than, the length of the corresponding plaintext.

It is important to note that encryption may not always, by itself, protect the integrity or the origin of data. In many cases it is possible, without knowledge of the key, to modify encrypted text with predictable effects on the recovered plaintext. In order to ensure integrity and origin of data it is often necessary to use additional techniques, such as those described in ISO/IEC 9796 (all parts), ISO/IEC 9797 (all parts), ISO/IEC 14888 (all parts), ISO/IEC 19772, ISO/IEC 29192-2, ISO/IEC 29192-3 and ISO/IEC 29192-4.