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)

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

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. 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*

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.

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

2.7
attack cost
ratio of the average complexity of the attack algorithm measured in terms of the number of calls to the encryption algorithm made by the attack to the probability of success of the attack

Note 1 to entry: Using the notation defined in 3.1, the attack cost is equal to the ratio W/P.

2.8
block
string of bits of a defined length

2.9
block cipher
symmetric encipherment system with the property that the encryption algorithm operates on a block of plaintext, i.e. a string of bits of a defined length, to yield a block of ciphertext

2.10
cipher
alternative term for encipherment system

2.11
ciphertext
data which has been transformed to hide its information content

[SOURCE: ISO/IEC 10116:2006, 3.3]

2.12
cleartext
alternative term for plaintext

2.13
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 are considered when assessing the security of an algorithm.

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

2.14
decipherment
alternative term for decryption

2.15
decipherment algorithm
alternative term for decryption algorithm

2.16
decryption
reversal of a corresponding encipherment

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

2.17
decryption algorithm
process which transforms ciphertext into plaintext

2.18
encipherment
alternative term for encryption

2.19
encipherment algorithm
alternative term for encryption algorithm

2.20
encipherment system
alternative term for encryption system

2.21
encryption
(reversible) transformation of data by a cryptographic algorithm to produce ciphertext, i.e. to hide the information content of the data

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

2.22
encryption algorithm
process which transforms plaintext into ciphertext

2.23
encryption system
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

2.24
generic attack
attack against a cipher which does not rely on the cipher design and can be used to recover an encryption key or plaintext

2.25
identity-based cipher
alternative term for identity-based encryption system

2.26
identity-based encryption system
asymmetric cipher in which the encryption algorithm takes an arbitrary string as a public key

2.27
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]

2.28
keystream
pseudorandom sequence of symbols, intended to be secret, used by the encryption and decryption algorithms of a stream cipher

Note 1 to entry: Note1 to entry: If a portion of the keystream is known by an attacker, then it shall be computationally infeasible for the attacker to deduce any information about the remainder of the keystream.

2.29
***n*-bit block cipher**
block cipher with the property that plaintext blocks and ciphertext blocks are *n* bits in length

[SOURCE: ISO/IEC 10116:2006, 3.10]

2.30
plaintext
unencrypted information

[SOURCE: ISO/IEC 10116:2006, 3.11]

2.31
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]

2.32
public key
key of an entity's asymmetric key pair which can be made public

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

2.33
secret key
key used with symmetric cryptographic techniques by a specified set of entities

[SOURCE: ISO/IEC 11770-3:2008, 3.35]

2.34
security strength
number associated with the amount of work (e.g. the number of operations) that is required to break a cryptographic algorithm or system

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

Note 2 to entry: In ISO/IEC 29192, security strength is specified in bits, e.g. 80, 112, 128, 192, or 256.

2.35
self-synchronous stream cipher
stream cipher with the property that the keystream symbols are generated as a function of a secret key and a fixed number of previous ciphertext bits

2.36
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.

2.37
symmetric cipher
alternative term for symmetric encryption system

2.38
symmetric cryptographic technique
cryptographic technique that uses the same secret key for both the originator's and the recipient's transformation

Note 1 to entry: Without knowledge of the secret key, it is computationally infeasible to compute either the originator's or the recipient's transformation.

2.39
symmetric encipherment system
alternative term for symmetric encryption system

2.40
symmetric encryption system
encryption system based on symmetric cryptographic techniques

2.41
synchronous stream cipher
stream cipher with the property that the keystream symbols are generated as a function of a secret key and, possibly, an initialisation vector, independent of the plaintext and ciphertext

3 Symbols and abbreviated terms

3.1 Symbols

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

n An integer

P The probability of success of an attack on a cryptographic algorithm to succeed

W Workload or complexity of an attack, measured in terms of the number of calls to the cryptographic algorithm

3.2 Abbreviated terms

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

ECB Electronic codebook

MAC Message authentication code

SC Subcommittee

SD Standing document

WG Working group

4 The nature of encryption

4.1 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 from the ciphertext unless the decryption 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, ISO/IEC 9797, ISO/IEC 14888, ISO/IEC 19772, and ISO/IEC 29192.