INTERNATIONAL STANDARD

ISO/IEC 18033-1

First edition
2005-02-01

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 18033-1:2005(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web 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. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

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.

ISO/IEC 18033-1 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

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*

Introduction

ISO/IEC 18033 is a multi-part International Standard that specifies encryption systems (ciphers) for the purpose of data confidentiality. The inclusion of ciphers in ISO/IEC 18033 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. ISO/IEC 18033-2 is devoted to asymmetric 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 ISO/IEC 18033. 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 ISO/IEC 18033 are defined in Annex A.

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). The two transformations have the property that, given the public transformation, it is computationally infeasible to derive the private transformation [ISO/IEC 11770-1:1996].

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 [ISO/IEC 9798-1:1997].

2.5
asymmetric key pair
pair of related keys where the private key defines the private transformation and the public key defines the public transformation [ISO/IEC 9798-1:1997].

2.6
block
string of bits of a defined length.

2.7
block cipher
symmetric encryption 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.

2.8
cipher
alternative term for encipherment system.

2.9
ciphertext
data which has been transformed to hide its information content [ISO/IEC 10116:1997].

2.10
cleartext
alternative term for plaintext.

2.11
decipherment
alternative term for decryption.

2.12
decipherment algorithm
alternative term for decryption algorithm.

2.13
decryption
reversal of a corresponding encipherment [ISO/IEC 11770-1:1996].

2.14
decryption algorithm
process which transforms ciphertext into plaintext.

2.15
encipherment
alternative term for encryption.

2.16
encipherment algorithm
alternative term for encryption algorithm.

2.17
encipherment system
alternative term for encryption system.

2.18
encryption
(reversible) transformation of data by a cryptographic algorithm to produce ciphertext, i.e., to hide the information content of the data [ISO/IEC 9797-1].

2.19
encryption algorithm
process which transforms plaintext into ciphertext.

2.20
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.

2.21
key
sequence of symbols that controls the operation of a cryptographic transformation (e.g. encipherment, decipherment) [ISO/IEC 11770-1:1996].

2.22
keystream
pseudorandom sequence of symbols, intended to be secret, used by the encryption and decryption algorithms of a stream cipher. 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.

2.23
***n*-bit block cipher**
block cipher with the property that plaintext blocks and ciphertext blocks are *n* bits in length [ISO/IEC 10116:1997].

2.24
plaintext
unencrypted information [ISO/IEC 10116:1997].

2.25
private key
that key of an entity's asymmetric key pair which should only be used by that entity [ISO/IEC 11770-1:1996].

NOTE A private key should not normally be disclosed.

2.26
public key
that key of an entity's asymmetric key pair which can be made public [ISO/IEC 11770-1:1996].

2.27
secret key
key used with symmetric cryptographic techniques by a specified set of entities [ISO/IEC 11770-3:1999].

2.28
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.

2.29
synchronous stream cipher
stream cipher with the property that the keystream symbols are generated as a function of a secret key, and are independent of the plaintext and ciphertext.

2.30
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. 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.

2.31
symmetric cipher
alternative term for symmetric encryption system.

2.32
symmetric cryptographic technique
cryptographic technique that uses the same secret key for both the originator's and the recipient's transformation. Without knowledge of the secret key, it is computationally infeasible to compute either the originator's or the recipient's transformation.