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)

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

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.

NOTE Examples of symmetric cryptographic techniques include symmetric ciphers and Message Authentication Codes (MACs). In a symmetric cipher, the same secret key is used to encrypt and decrypt data. In a MAC scheme, the same secret key is used to generate and verify MACs.

2.33
symmetric encipherment system
alternative term for symmetric encryption system.

2.34
symmetric encryption system
encryption system based on symmetric cryptographic techniques that uses the same secret key for both the encryption and decryption algorithms.

3 The nature of encryption

3.1 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 decryption key is also known. However, the length of the plaintext will generally 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 15946-2, ISO/IEC 15946-4 and in the future International Standard ISO/IEC 19772.

3.2 Symmetric and asymmetric ciphers

Ciphers work in association with a key.

- In a *symmetric cipher*, the same *secret key* is used in both the encryption and decryption algorithms. Knowledge of this key is required to perform both encryption and decryption, and knowledge of the secret key therefore needs to be restricted to those parties authorised to access the data which the key is used to encrypt.

- In an *asymmetric cipher*, different but related keys are used for encryption and decryption. Hence keys are generated in matching *key pairs*, where one key is the encryption key and the other is the decryption key. Even with knowledge of the encryption key it is assumed to be computationally infeasible to find any information about the content of a plaintext from its corresponding ciphertext. In many situations it is possible to make the encryption key public, and hence this key is often referred to as the *public key*, whilst the corresponding decryption key typically has only one owner and remains confidential (hence it is referred to as the *private key*). Anyone who knows the public encryption key will be able to encrypt data intended for the holder of the corresponding private key, whilst only the private decryption key holder will be able to decrypt it.

NOTE The traditional notion of an asymmetric cipher involves much more computationally complex operations than for a symmetric cipher, and typically such ciphers were not used for encrypting large volumes of data; instead they were typically used only for encrypting secret session keys (that were then used with symmetric ciphers). However, some of the asymmetric ciphers specified in ISO/IEC 18033-2 are designed in a way that makes them suitable for encrypting large volumes of data.

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.

3.3 Key management

The use of all types of cryptography relies on the management of cryptographic keys. All ciphers, both symmetric and asymmetric, require all the parties using the cipher to have access to the necessary keys. This gives rise to the need for *key management*, involving the generation, distribution, and ongoing management of keys. An overall framework for key management is given in ISO/IEC 11770-1.

The problem of key management is rather different depending on whether the keys are for symmetric or asymmetric ciphers. For symmetric ciphers it is necessary to arrange for secret keys to be generated and shared by pairs (or larger groups) of entities. For asymmetric ciphers it is necessary for key pairs to be generated and for public keys to be distributed in such a way that their authenticity is guaranteed.

Methods to establish shared secret keys using symmetric cryptographic techniques are specified in ISO/IEC 11770-2. Methods to establish shared secret keys using asymmetric cryptographic techniques are specified in ISO/IEC 11770-3; this latter International Standard also specifies techniques for the reliable distribution of public keys for asymmetric cryptographic techniques.

4 The use and properties of encryption

4.1 Asymmetric ciphers

The encryption algorithm for an asymmetric cipher defines a mapping from the set of permissible plaintext messages (typically a set of bit strings) to the set of ciphertext messages (typically also a set of bit-strings). The set of permissible messages and the set of ciphertexts will depend upon both the choice of cipher and the key pair.

For an asymmetric cipher the encryption algorithm depends on a public key, whereas decryption depends on a private key. Hence, whilst the ciphertext block corresponding to a chosen plaintext block may be readily computed, it shall be infeasible for anyone, other than the holder of the private key, to deduce the plaintext block corresponding to a chosen ciphertext block. However, if an interceptor of ciphertext knows the public key used to produce it, and also knows that the plaintext has been chosen from a small set of possibilities, it may become possible to deduce the plaintext by an exhaustive search through all possible plaintexts.

As a result, and in order to achieve a satisfactory level of security, it is necessary to incorporate random data in the encryption process so that the ciphertext block corresponding to a given plaintext block cannot be predicted. Detailed techniques for incorporating random data are described in ISO/IEC 18033-2.

4.2 Block ciphers

A block cipher is a symmetric cipher with the property that the encryption algorithm operates on blocks of plaintext, i.e. strings of bits of a defined length, to yield ciphertext blocks. Each key for a block cipher defines a particular invertible mapping of plaintext blocks to ciphertext blocks (and a corresponding inverse mapping used for decryption). If, as is typically the case, the plaintext blocks and ciphertext blocks are all blocks of n binary digits, then each key simply defines a permutation on the set of all n-bit blocks.

4.2.1 Modes of operation

There are many ways in which an n-bit block cipher can be used to encipher plaintext; such methods are known as *modes of operation* for block ciphers. Modes of operation are defined in ISO/IEC 10116. If the number of bits in the plaintext happens to be n, then encryption can be achieved by simply applying the encryption process to this block. However, for arbitrary length plaintext, it is necessary to employ a more sophisticated approach. For this and other reasons it is often necessary to use one of the other modes of operation defined in ISO/IEC 10116.

4.2.2 Message Authentication Codes (MACs)

Although encryption does not provide data integrity, it is possible to use a block cipher in a specially defined way to provide a data integrity protection function. In particular, it is possible to use a block cipher to compute a Message Authentication Code (MAC) for a string of bits. Such a MAC can be used to provide integrity and origin protection for the string of bits. Ways to achieve this are specified in ISO/IEC 9797-1. Note that it is sometimes desirable to use a block cipher to both encrypt and compute a MAC on plaintext. In such an event it is generally necessary to use two different secret keys, one for encryption and one for MAC computation.

NOTE – If a particular combination of the MAC and encryption specifically allows for the use of the same secret key, then two different secret keys will not be required.

4.3 Stream ciphers

A stream cipher is always based upon a keystream generator, i.e. a function which, when given a secret key (and possibly also previous ciphertext) as input, outputs a sequence of symbols known as the keystream. This sequence is used to encrypt plaintext by combining it with the sequence of plaintext symbols one symbol at a time using an invertible function (e.g. the bit-wise exclusive-or operation).

Typically, if the same key is used more than once to initialise the keystream generator, then the same keystream will result. If the same keystream is used to encrypt more than one plaintext, then there is a danger that an interceptor of the resulting ciphertexts will be able to deduce information about both plaintexts. As a result it is necessary to provide means for a different keystream to be used to encrypt every plaintext. Such keying issues are discussed further in ISO/IEC 18033-4.

Stream ciphers do not always provide integrity protection for the plaintext. In the case where the stream cipher encryption operation involves bitwise modulo 2 addition of the plaintext to the keystream, a single bit change in the ciphertext results in a single bit change to the recovered plaintext. Also, such stream ciphers always reveal the exact length of the plaintext.

5 Object identifiers

ISO/IEC 18033 specifies a unique name (an OSI object identifier) for each specified algorithm. In applications in which object identifiers are used, the object identifiers specified in ISO/IEC 18033 are to be used in preference to any other object identifiers that may exist for the algorithms concerned.