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.]

3.25
secret key
key (3.17) used with *symmetric cryptographic techniques* (3.28) by a specified set of entities

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

3.26
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* (3.17) recovery, a security strength of k bits implies that the workload required to break the *cipher* (3.13) is equivalent to 2^k executions of the cipher. For further information on the application of security strength to selecting cryptographic algorithms for this document, see C.1.4.

3.27
stream cipher
symmetric encryption system (3.29) with the property that the *encryption algorithm* (3.12) involves combining a sequence of *plaintext* (3.20) symbols with a sequence of *keystream* (3.18) 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.

3.28
symmetric cryptographic technique
cryptographic technique for which all transformations use the same *key* (3.17)

3.29
symmetric encryption system
symmetric encipherment system
symmetric cipher
encryption system (3.13) based on *symmetric cryptographic techniques* (3.28)

4 Symbols and abbreviated terms

ECB	electronic code book
k	key length
MAC	message authentication code
n	plaintext/ciphertext block length for a block cipher
P	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

5 Nature of encryption

5.1 Purpose of encryption

The primary purpose of encryption 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 is not concealed by encryption, since the length of the ciphertext is typically the same as, or a little larger than, the length of the corresponding plaintext.

It is important to note that encryption does 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.

5.2 Symmetric and asymmetric encryption systems

Symmetric and asymmetric encryption systems differ in their method of key generation.

— In a symmetric encryption system, the same secret key is used with 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 authorized to access the data which the key is used to encrypt.

— In an asymmetric encryption system, different but related keys are used for encryption and decryption. Hence, keys are generated in matching pairs, where one key of the pair 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. Hence, this key is often referred to as the public key. 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 is able to encrypt data intended for the holder of the corresponding private key, while only the private decryption key holder is able to decrypt it.

5.3 Key management

The use of all types of cryptography relies on the management of cryptographic keys. All encryption systems, 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 encryption systems. For symmetric encryption systems, it is necessary to arrange for secret keys to be generated and shared by pairs (or larger groups) of entities. For asymmetric encryption systems, 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. In an identity-based encryption system, the public key is an arbitrary data string, which is usually chosen from some public information associated with the entity which decrypts ciphertexts.

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. ISO/IEC 11770-3 also specifies techniques for the reliable distribution of public keys for asymmetric cryptographic techniques. Methods to establish shared secret keys using weak secrets are specified in ISO/IEC 11770-4.

6 Use and properties of encryption

6.1 General

The criteria used for submission of encryption systems for possible inclusion in, and for their deletion from, the ISO/IEC 18033 series are defined in Annexes A and B.

6.2 Asymmetric encryption systems

The encryption algorithm for an asymmetric encryption system 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 depends on both the choice of encryption system and the key pair.

For an asymmetric encryption system, the encryption algorithm depends on a public key, whereas decryption depends on a private key. Hence, while the ciphertext block corresponding to a chosen plaintext block can 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 can 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.

Authenticity of public keys is of great importance when using asymmetric encryption algorithms. Assurance in the authenticity of a public key can, for example, be provided using a PKI.

6.3 Block ciphers

6.3.1 General

A block cipher is a symmetric encryption system with the property that the encryption algorithm operates on blocks of plaintext 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.

Block ciphers can be used in a wide variety of ways. Two of the most important applications are the modes of operation described in 6.3.2 (modes that provide confidentiality) and 6.3.3 (modes that provide integrity control), but there are many other uses such as in hash-functions (see ISO/IEC 10118-2) and random-number generators (see ISO/IEC 18031).

The criteria used for submission of encryption systems for possible inclusion in, and for their deletion from, the ISO/IEC 18033 series are defined in Annexes A and B.

6.3.2 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, an encryption mode known as electronic code book (ECB). 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.

6.3.3 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 a MAC computation. Alternatively, techniques for authenticated encryption,

which simultaneously provide confidentiality and integrity protection using only a single secret key, are specified in ISO/IEC 19772.

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 are not required.

6.4 Stream ciphers

A stream cipher is, by definition, based on 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 and the same initialization vector is used more than once to initialize the stream cipher, then the same keystream results. If the same keystream is used to encrypt more than one plaintext, then there is a danger that an interceptor of the resulting ciphertexts can 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.

Unless special plaintext formatting techniques are employed, stream ciphers do not provide integrity protection for the plaintext. In the case where the stream cipher encryption operation involves bit-wise exclusive-or 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.

6.5 Identity-based encryption systems

An identity-based encryption system is an asymmetric encryption mechanism that allows an arbitrary string to be used as a public key. By using an easily identifiable string (e.g. an e-mail address) as a public key, an entity which encrypts plaintexts can reliably obtain it without the need to access and verify a public-key certificate. In some circumstances, it can be possible to arrange for a public key to have a short lifetime, e.g. by including a date or timestamp in the public key along with an identifier for the holder. In such a case, an explicit revocation mechanism for public keys may not be required, unlike the case when using public-key certificates (see ISO/IEC 11770-3).

The use of identity-based encryption involves a special trusted third party known as a private key generator. This entity is responsible for generating the private keys of individual users. This third party therefore has the means to decrypt all messages intended for its clients. This property may not always be desirable, in which case a certificate based asymmetric encryption system, as standardized in ISO/IEC 18033-2, should be used instead.

6.6 Homomorphic encryption systems

Homomorphic encryption is a type of symmetric or asymmetric encryption that allows third parties (i.e. parties that are neither the encryptor nor the decryptor) to perform operations on plaintext data while keeping the data in encrypted form. The primary purpose of homomorphic encryption is to allow third parties to perform such computations on data while simultaneously ensuring that the confidentiality of the plaintext data is preserved. It is typically the case that homomorphic encryption systems require the plaintext to be represented in the form of elements of a group, rather than strings of bits or bytes as is the case with most conventional methods of encryption.

7 Object identifiers

Subsequent parts of the ISO/IEC 18033 series specify a unique name (an OSI object identifier) for each specified algorithm. In applications in which object identifiers are used, the object identifiers specified in subsequent parts of the ISO/IEC 18033 series shall be used in preference to any other object identifiers that can exist for the algorithms concerned.

Annex A
(informative)

Criteria for submission of encryption systems for possible inclusion in the ISO/IEC 18033 series

A.1 Guidelines used for evaluating encryption algorithms

The encryption systems included in subsequent parts of the ISO/IEC 18033 series have been selected from the large variety of such techniques published and in use. The exclusion of particular encryption systems does not imply that these techniques are insecure. The encryption systems specified represent a small set of techniques chosen according to the following criteria (where the order of presentation of the criteria is not of significance).

a) The security of the encryption system, i.e. selected algorithms should be resistant to cryptanalytic attack with reasonable attack models (see Clause A.2). The existence of a proof of security is regarded as a significant argument in favour of an encryption system, depending on the security model and the proof assumptions. The nature of any evaluations is also of great importance, especially those conducted by widely recognized evaluation organizations.

b) The performance of the encryption system on a variety of typical platforms. This includes not only issues such as time and space efficiency, but also whether or not the encryption system has characteristics that give it advantages over other algorithms.

c) The nature of any licensing issues affecting the encryption system.

d) The maturity of the encryption system. The maturity of the encryption system is evaluated in terms of how extensively it is used, how widely any analysis has been published and how much the encryption system has been scrutinized.

e) The degree to which the encryption system is endorsed by a recognized organization (e.g. a standards body, government security agency) or is under investigation and/or analysis for endorsement by such a body.

f) The existing level of market adoption of the encryption system. Unless other considerations override such a decision, encryption systems that are widely adopted in markets should be favoured over less well-used techniques.

g) In general, the number of encryption systems to be standardized in each part of the ISO/IEC 18033 series should be as small as possible. Three exceptions to this principle exist.

   — Where two encryption systems have different characteristics, e.g. *n*-bit block ciphers with different values of *n* or encryption systems with widely differing computational and space implementation requirements, and where these characteristics have practical significance, encryption systems of both types are likely to be standardized.

   — It is generally desirable to have available standardized encryption systems based on different fundamental principles, such that if one encryption system becomes vulnerable to cryptanalytic attack, another encryption system has a good chance of remaining secure.

   — It is generally desirable to have standardized encryption systems based on more than one computationally difficult problem, e.g. integer factorization, or the discrete logarithm problem in a variety of settings, including the multiplicative group of a finite field and the group of points on an elliptic curve over a finite field.

A process for inclusion and deletion of new encryption systems in the ISO/IEC 18033 series is presented in ISO/IEC JTC 1/SC 27/WG 2 Standing Document 5[12].

A.2 Qualification of attacks on encryption algorithms

The effectiveness of known cryptanalytic attacks on an encryption algorithm is of fundamental importance in deciding whether an algorithm can be submitted for consideration for inclusion in subsequent parts of the ISO/IEC 18033 series.

For the purposes of this annex, comparing the attack cost for the particular cryptanalytic attack to the best generic attack for the given model and goal should be used to determine whether or not the attack is classified as a break of the encryption algorithm. If the attack cost is greater than or equal to the attack cost of the corresponding best generic attack, the cryptanalytic attack should not be deemed to be a break of the encryption algorithm. If the attack cost is less than the attack cost of the corresponding best generic attack for the model and goal, then the cryptanalytic attack should be deemed to be a break of the encryption algorithm. For further information on cryptanalytic attacks, see Annex C.

The same approach can be applied to other attack cost metrics and properties, such as memory and data complexity.

For the purposes of this annex, implementation-specific attacks should not be considered.

A.3 Minimum qualification criteria for the submission of new encryption systems

A.3.1 General

The criteria set out in this clause are meant for the submission of encryption systems not already included in subsequent parts of the ISO/IEC 18033 series. In order for an encryption system to be considered for inclusion in subsequent parts of the ISO/IEC 18033 series, the encryption system should comply with the following recommendations.

A.3.2 Basic recommendations

The following basic recommendations apply.

a) Minimum key length: The encryption algorithm should provide a minimum security strength of 128 bits. Depending on the application, this security strength should be achieved in the classical or quantum model, or both. For symmetric and asymmetric algorithms, the key length should be chosen to offer a security strength of 128 bits as a minimum.

NOTE 1 For more information on the equivalent key length of symmetric and asymmetric encryption systems, see ISO/IEC JTC 1/SC 27 Standing Document 12[15].

NOTE 2 Clause C.2 provides more details on the quantum threat.

b) Known cryptanalysis results: There should be no known cryptanalytic attacks that break the encryption algorithm for the claimed model and goal.

NOTE 3 A general methodology for evaluation of a cryptanalytic attack is described in C.1.4.

EXAMPLE Suppose a symmetric encryption system with a key length of 256 bits is submitted for possible inclusion in the ISO/IEC 18033 series. Suppose also that there is a cryptanalytic attack against the encryption system that can find the key with a complexity of 2^{250} calls to the encryption algorithm, a success probability of 1, and that is faster than the best generic attack in the same model and with the same goal. Then, the encryption system passes criterion a) but fails criterion b), and therefore cannot be accepted for possible inclusion.

c) Public domain: The encryption system description should have been published for a minimum period of 3 years in the public domain. Acceptable venues publications include but are not limited to the following:

   1) IACR conferences, workshops and symposia:

      i) Asiacrypt, Crypto, Eurocrypt;

      ii) International workshop on Fast Software Encryption (FSE);

      iii) International workshop on Cryptographic Hardware and Embedded Systems (CHES);

      iv) Conference on Practice and Theory in Public Key Cryptography (PKC);

      v) Theory of Cryptography Conference (TCC);

      vi) Real World Crypto Symposium (RWC);

   2) conferences, workshops and symposia in cooperation with IACR:

      i) International Conference on Post-Quantum Cryptography (PQCrypto);

      ii) International Conference on Cryptography (Africacrypt);

      iii) Code-based cryptography workshop (CBC);

      iv) Current trends in cryptology workshop (CTCrypt);

      v) Financial Cryptography and Data Security (FC);

      vi) Selected Areas in Cryptography (SAC);

      vii) Conference on Security and Cryptography for Networks (SCN);

      viii) International Conference on Cryptology in India (Indocrypt);

      ix) Conference on Security Standards Research (SSR);

      x) International Workshop on Lightweight Cryptography for Security and Privacy (LightSec);

      xi) Worshop on Fault Diagnosis and Tolerance in Cryptography (FDTC);

   3) IEEE annual conferences:

      i) Symposium on Security and Privacy;

      ii) Symposium on the Foundations of Computer Science (FOCS);

   4) ACM annual conferences:

      i) Symposium on Theory of Computing (ACM-STOC);

      ii) Computer and Communication Security (ACM-CCS);

   5) well-known international conferences which have a history of more than 15 years with available proceedings:

      i) USENIX Security;

      ii) European Symposium on Research in Computer Security (ESORICS);

      iii) Australasian Conference on Information Security and Privacy (ACISP);

iv) International Conference on Information Security and Cryptography (ICISC);

6) well-known journals [at least DataBase systems and Logic Programming (DBLP) cited]:

i) ACM:

— Journal of the ACM;

— Communications of the ACM;

ii) Elsevier:

— Computer Communications;

— Information and Computation;

— Journal of Computer and System Sciences (JCSS);

— Journal of Discrete Algorithms;

iii) IEEE:

— IEEE Transactions on Information Theory;

— IEEE Transactions on Computers;

— IEEE Security and Privacy;

iv) IEICE:

— IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences;

— IEICE Transactions on Information and Systems;

v) SIAM: SIAM Journal on Computing;

vi) Springer:

— Combinatorica;

— Cryptography and Communications;

— Designs, Codes and Cryptography;

— Journal of Cryptology;

— International Journal of Information Security;

vii) IACR: Transactions on Symmetric Cryptography;

NOTE 4 More generally, an acceptable venue for publication would involve peer review, electronic availability, publication in English, and at least three years of publishing history.

7) other standards: Official publication as a standard in English, or an approved translation that has been made publicly available by a recognized standardization organization;

8) an international competition with the sole purpose of choosing a new state of the art encryption algorithm of a particular type (e.g. block cipher, stream cipher, asymmetric encryption system) which is run for a minimum of two years, and where analysis and publications satisfying c) 1) to c) 7) are open to the general public. The unmodified version of the algorithm should have

been in the public domain for at least three years before submission to the ISO/IEC 18033 series can be considered.

d) Cryptanalysis: Prior to inclusion an encryption system should have cryptanalysis papers, supporting requirements stated in b), published in peer reviewed journals or conferences such as those listed in c).

e) Performance: For a pre-determined security strength (e.g. key length), performance measurements can be quantified using a variety of metrics, such as bits/cycle, bits/watt, bits of memory, gates. Robust evidence should be provided that the encryption system offers better performance than existing standard encryption systems with respect to metrics relevant to the intended applications, while offering a level of security at least comparable to the existing standardized encryption systems in the standard. Encryption systems that cannot achieve better performance but provide better security in comparable environments and attack models are good subjects for standardization.

A.3.3 Additional recommendations

Industry adoption: Robust evidence should be provided of commercial applications using the encryption system and possible international deployments of the applications.

Annex B
(informative)

Criteria for the deletion of encryption systems from the ISO/IEC 18033 series

Encryption algorithms already standardized in subsequent parts of ISO/IEC 18033 are subject to deletion from the ISO/IEC 18033 series if the security of the encryption system cannot be ensured against newly developed methods of cryptanalysis, and as a result the practical security of the encryption algorithm can no longer be guaranteed. All parts of the ISO/IEC 18033 series are reviewed regularly to ensure their correctness and applicability. During reviews, newly published cryptanalysis of the encryption algorithms published in the ISO/IEC 18033 series are considered. To assess newly published cryptanalysis techniques, the procedures described in ISO/IEC JTC 1/SC 27/WG 2 Standing Document 5[12] are followed.

Factors that are considered during the assessment of how new cryptanalysis techniques affect encryption algorithms already published in the ISO/IEC 18033 series are:

a) correctness of the cryptanalysis. Novel cryptanalysis techniques are disclosed in a wide variety of fora. Sometimes, published cryptanalysis exaggerate claims in terms of security strength, or in terms of the complexity analysis of a cryptanalytic attack. Furthermore, the proposed model in which a cryptanalytic attack is proposed is an important factor in determining its validity. Before the impact of a new technique on published algorithms is assessed, consensus needs to be reached that the published cryptanalysis is valid;

b) practical feasibility of the cryptanalysis. Some cryptanalytic results are of theoretical interest, but not necessarily applicable to the complete encryption algorithm. It can also happen that cryptanalysis of an encryption system leads to a theoretical attack on an encryption algorithm, but the attack is not practical, either because of the attack model, or because of the attack complexity involved (the cost of the attack is higher than the cost of the generic attack). If an attack is practical, serious implications to users of the encryption algorithm can exist, and deletion of the encryption algorithm from the ISO/IEC 18033 series is considered;

c) impact on products of the encryption algorithm in industry: When considering deletion of an algorithm, a prediction of its impact on industry should be fully taken into account along with the report of weakness in the encryption algorithm, especially if the weakness is not serious from a practical point of view.

Depending on the outcome of the review, an algorithm can be deleted from the ISO/IEC 18033 series if it poses serious practical risks for users of the algorithm. If an algorithm is not deleted, but nevertheless its security is affected by a newly disclosed cryptanalytic technique, then further information about the impact of this technique on the level of security provided by the algorithm is added to ISO/IEC JTC 1/SC 27 Standing Document 12[15].

In order to speed up communication regarding the assessment of the impact of cryptanalytic attacks, ISO/IEC JTC 1/SC 27/WG 2 Standing Document 6[13] can be used.

The procedures for inclusion and removal of cryptographic mechanisms are listed in ISO/IEC JTC 1/SC 27/WG 2 Standing Document 5[12].