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 algorihm

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.

4.2 Symmetric and asymmetric ciphers

Ciphers work in association with a key.

- In a symmetric cipher, 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 cipher, 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, and hence this key is often referred to as the public key, while the corresponding decryption key typically has only one owner and remains confidential and 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, while only the private decryption key holder will be able to decrypt it.

NOTE In many cases an asymmetric cipher involves much more computationally complex operations than a symmetric cipher, and such ciphers are typically not used for encrypting large volumes of data; instead they are typically only used to encrypt secret session keys (that are 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 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.

4.3 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. In an identity-based cipher, the public key is an arbitrary data string, which is usually chosen from some public information associated with the decryptor.

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.

5 The use and properties of encryption

5.1 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, while 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.

5.2 Block ciphers

5.2.1 General

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.

Block ciphers can be used in a wide variety of ways. Two of the most important applications are described in 5.2.2 and 5.2.3, but there are many other uses such as in hash-functions (see ISO/IEC 10118-2) and random-number generators (see ISO/IEC 18031).

5.2.2 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.

5.2.3 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 will not be required.

5.3 Stream ciphers

A stream cipher is by definition 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 and the same initialisation vector 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.

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.

5.4 Identity-based mechanisms

An identity-based encryption technique 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 encryptor can reliably obtain it without the need to access and verify a public key certificate. In some circumstances it may 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). Since public key certificates are not required, and a revocation mechanism may also not be needed, identity-based encryption has the potential to offer significant practical advantages by comparison with certificate-based asymmetric encryption techniques.

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 technique, as standardized in ISO/IEC 18033-2, should be used instead.

6 Object identifiers

This International Standard 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 this International Standard are to be used in preference to any other object identifiers that may exist for the algorithms concerned.

Annex A
(normative)

Criteria for submission of ciphers for possible inclusion in this International Standard

A.1 Guidelines used for evaluating encryption algorithms

The ciphers included in subsequent parts of this International Standard have been selected from the large variety of such techniques published and in use. The exclusion of particular ciphers does not imply that these techniques are insecure. The ciphers 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).

Evaluations are made with respect to the following aspects of the cipher.

a) The *security* of the cipher, i.e. selected algorithms must be resistant to cryptanalytic attack. The existence of a proof of security is regarded as a significant argument in favour of a cipher, 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 organisations.

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

c) The nature of any *licensing issues* affecting the cipher.

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

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

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

g) In general, the *number* of ciphers to be standardized in each part of this International Standard should be as small as possible. Three exceptions to this principle exist.

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

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

   — It is generally desirable to have standardized ciphers 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.

h) A process that SC 27 follows when deciding on the inclusion of new ciphers in this International Standard can be found in WG 2 SD 5.

A.2 Qualification of attacks on encryption algorithms

The effectiveness of the known cryptanalytic attacks on an encryption algorithm is of fundamental importance in deciding whether an algorithm can be submitted for consideration for inclusion into subsequent parts of this International Standard.

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 shall determine whether the attack is classified as a break of the encryption algorithm or not. If the attack cost is greater than or equal to the attack cost of the corresponding best generic attack, the cryptanalytic attack shall 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 shall be deemed to be a break of the encryption algorithm. See 2.6 for a definition of the term attack.

For the purposes of this Annex, implementation-specific attacks shall not be considered.

NOTE See Annex C for background information on attacks.

A.3 Minimum qualification criteria for the submission of new ciphers

The criteria set out in this clause are meant for the submission of ciphers not already included in subsequent parts of this International Standard. In order for a cipher to be considered for inclusion in subsequent parts of this International Standard, the cipher shall comply with the following requirements:

a) Minimum key length: The encryption algorithm shall provide a minimum key length of 128 bits for symmetric encryption algorithms. For asymmetric algorithms, the key length in bits is generally longer, but can be mapped to an equivalent symmetric key length. In such cases, the asymmetric algorithm must offer an equivalent key length of 128-bits as a minimum.

   NOTE For more information on the equivalent key length of symmetric and asymmetric ciphers, refer to JTC 1/SC 27 Standing Document 12 (SC 27 SD 12) at http://www.jtc1sc27.din.de/sbe/SD12.

b) Known cryptanalysis results: There shall be no known cryptanalytic attacks that break the encryption algorithm as described in C.1.4.

   EXAMPLE A symmetric cipher with a key length of 256 bits is submitted. There is a cryptanalytic attack against the cipher. This cryptanalytic attack can find the key with a complexity of 2^{250} and success probability of 1 and is faster than the best generic attack in the same model and goal. The cipher passes criteria a, but fails criteria b and therefore will not be considered for possible inclusion.

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

   1) IACR conferences and workshops:

      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)

   2) IEEE annual conferences:

      i) Symposium on Security and Privacy

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

3) ACM annual conferences:

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

   ii) Computer and Communication Security (ACM-CCS)

4) 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) Financial Cryptography and Data Security (FC)

   v) International Conference on Information Security and Cryptography (ICISC)

   vi) Selected Areas in Cryptography (SAC)

5) 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,

6) Other standards

   - Official publication as a standard in English that has been made publicly available by a recognized standardization organization.

7) 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 cipher) which is run for a minimum of two years, and where analysis and publications 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 this International Standard can be considered.

d) Cryptanalysis: Prior to inclusion a cipher shall have cryptanalysis papers published in peer reviewed journals or conferences such as those listed in c).

e) Industry adoption: Robust evidence shall be provided of commercial applications using the cipher and possible international deployments of the applications.

f) Performance: For a pre-determined security level (e.g. key length), performance measurements can be quantified using a variety of metrics, such as bits/cycle or bits/watt. Robust evidence shall be provided that the cipher offers better performance than existing standard ciphers with respect to metrics relevant to the intended applications, while offering a level of security at least comparable to the existing standardized ciphers in the standard.

Annex B
(normative)

Criteria for the deletion of ciphers from this International Standard

Encryption algorithms already standardized in subsequent parts of ISO/IEC 18033 are subject to deletion from the standard if the security of the cipher 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. Existing standards are reviewed regularly to ensure their correctness and applicability. During reviews, newly published cryptanalysis of the encryption algorithms published in this International Standard are considered. To assess newly published cryptanalysis techniques, the procedures described in SC 27 are followed.

Factors that are considered during the assessment of how new cryptanalysis techniques affect encryption algorithms already published in this International Standard 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 must 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 may also happen that cryptanalysis of a cipher 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. If an attack is practical, serious implications to users of the encryption algorithm may exist, and deletion of the encryption algorithm from this International Standard is considered.

c) Impact on products of the encryption algorithm in industry: When considering deletion of an algorithm, prediction of 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 may be deleted from this International Standard if it poses serious practical risks for the 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 described in SC 27 Standing Document 12 (SC 27 SD 12) which is freely available at http://www.jtc1sc27.din.de/sbe/SD12.