INTERNATIONAL STANDARD

ISO/IEC 19772

First edition
2009-02-15

Information technology — Security techniques — Authenticated encryption

Technologies de l'information — Techniques de sécurité — Chiffrage authentifié

Reference number
ISO/IEC 19772:2009(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

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

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

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 19772 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

Introduction

When data is sent from one place to another, it is often necessary to protect it in some way whilst it is in transit, e.g. against eavesdropping or unauthorised modification. Similarly, when data is stored in an environment to which unauthorized parties may have access, it may be necessary to protect it.

If the confidentiality of the data needs to be protected, e.g. against eavesdropping, then one solution is to use encryption, as specified in ISO/IEC 18033 and ISO/IEC 10116. Alternatively, if it is necessary to protect the data against modification, i.e. integrity protection, then Message Authentication Codes (MACs), as specified in ISO/IEC 9797, or digital signatures, as specified in ISO/IEC 9796 and ISO/IEC 14888, can be used. If both confidentiality and integrity protection are required, then one possibility is to use both encryption and a MAC or signature. Whilst these operations can be combined in many ways, not all combinations of such mechanisms provide the same security guarantees. As a result it is desirable to define in detail exactly how integrity and confidentiality mechanisms should be combined to provide the optimum level of security. Moreover, in some cases significant efficiency gains can be obtained by defining a single method of processing the data with the objective of providing both confidentiality and integrity protection.

In this standard, *authenticated encryption mechanisms* are defined. These are methods for processing data to provide both integrity and confidentiality protection. They typically involve either a specified combination of a MAC computation and data encryption, or the use of an encryption algorithm in a special way such that both integrity and confidentiality protection are provided.

The methods specified in this standard have been designed to maximise the level of security and provide efficient processing of data. Some of the techniques defined here have mathematical 'proofs of security', i.e. rigorous arguments supporting their soundness.

Information technology — Security techniques — Authenticated encryption

1 Scope

This International Standard specifies six methods for authenticated encryption, i.e. defined ways of processing a data string with the following security objectives:

— data confidentiality, i.e. protection against unauthorized disclosure of data,

— data integrity, i.e. protection that enables the recipient of data to verify that it has not been modified,

— data origin authentication, i.e. protection that enables the recipient of data to verify the identity of the data originator.

All six methods specified in this International Standard are based on a block cipher algorithm, and require the originator and the recipient of the protected data to share a secret key for this block cipher. Key management is outside the scope of this standard; key management techniques are defined in ISO/IEC 11770.

Four of the mechanisms in this standard, namely mechanisms 1, 3, 4 and 6, allow data to be authenticated which is not encrypted. That is, these mechanisms allow a data string that is to be protected to be divided into two parts, *D*, the data string that is to be encrypted and integrity-protected, and *A* (the additional authenticated data) that is integrity-protected but not encrypted. In all cases, the string *A* may be empty.

NOTE Examples of types of data that may need to be sent in unencrypted form, but whose integrity should be protected, include addresses, port numbers, sequence numbers, protocol version numbers, and other network protocol fields that indicate how the plaintext should be handled, forwarded, or processed.

2 Normative references

The following referenced documents are indispensable for the application 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 9797-1:—[1)], *Information technology — Security techniques — Message Authentication Codes (MACs) — Part 1: Mechanisms using a block cipher*

ISO/IEC 10116, *Information technology — Security techniques — Modes of operation for an n-bit block cipher*

ISO/IEC 18033-3, *Information technology — Security techniques — Encryption algorithms — Part 3: Block ciphers*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

1) To be published. (Revision of ISO/IEC 9797-1:1999)

3.1
authenticated encryption
(reversible) transformation of data by a cryptographic algorithm to produce ciphertext that cannot be altered by an unauthorized entity without detection, i.e. it provides data confidentiality, data integrity, and data origin authentication

3.2
authenticated encryption mechanism
cryptographic technique used to protect the confidentiality and guarantee the origin and integrity of data, and which consists of two component processes: an encryption algorithm and a decryption algorithm

3.3
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 [ISO/IEC 18033-1]

3.4
ciphertext
data which has been transformed to hide its information content [ISO/IEC 10116]

3.5
data integrity
the property that data has not been altered or destroyed in an unauthorized manner [ISO/IEC 9797-1]

3.6
decryption
reversal of a corresponding encryption [ISO/IEC 18033-1]

3.7
encryption
(reversible) transformation of data by a cryptographic algorithm to produce ciphertext, i.e., to hide the information content of the data [ISO/IEC 18033-1]

3.8
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 [ISO/IEC 18033-1]

3.9
key
sequence of symbols that controls the operation of a cryptographic transformation (e.g. encipherment, decipherment) [ISO/IEC 18033-1]

3.10
message authentication code (MAC)
string of bits which is the output of a MAC algorithm [ISO/IEC 9797-1]

3.11
partition
process of dividing a string of bits of arbitrary length into a sequence of blocks, where the length of each block shall be n bits, except for the final block which shall contain r bits, $0 < r \leq n$

3.12
plaintext
unencrypted information [ISO/IEC 10116]

3.13
secret key
key used with symmetric cryptographic techniques by a specified set of entities [ISO/IEC 18033-1]

3.14
symmetric encryption system
encryption system based on symmetric cryptographic techniques that uses the same secret key for both the encryption and decryption algorithms [ISO/IEC 18033-1]

4 Symbols (and abbreviated terms)

For the purposes of this document, the following symbols and notation apply:

A	Additional authenticated data.
C	Authenticated-encrypted data string.
D	Data string to which an authenticated encryption mechanism is to be applied.
d	Block cipher decryption algorithm; $d_K(Y)$ denotes the result of block cipher decrypting the n-bit block Y using the secret key K.
e	Block cipher encryption algorithm; $e_K(X)$ denotes the result of block cipher encrypting the n-bit block X using the secret key K.
K	Secret block cipher key shared by the originator and recipient of the data to which the authenticated encryption mechanism is to be applied.
m	Number of blocks in the partitioned version of D.
n	Block length (in bits) for a block cipher.
t	Tag length (in bits).
0^i	Block of i zero bits.
1^i	Block of i one bits.
$\oplus$	Bit-wise exclusive-or of strings of bits (of the same bit-length).
$\|\|$	Concatenation of bit strings, i.e. if A and B are blocks of bits, then $A\|\|B$ is the block of bits obtained by concatenating A and B in the order specified.
#	Function converting a number into an a-bit block of bits; if k is an integer ($0 \leq k < 2^a$) then $\#_a(k)$ is the a-bit block which, when regarded as the binary representation of a number with the most significant bit on the left, equals k.
$\#^{-1}$	Function converting a block of bits to a number; if A is a block of bits, then $\#^{-1}(A)$ is the unique non-negative integer whose binary representation is A. Hence, if A has n bits, then $\#_n(\#^{-1}(A)) = A$.
$X]_s$	Left-truncation of the block of bits X: if X has bit-length greater than or equal to s, then $X]_s$ is the s-bit block consisting of the left-most s bits of X.
$X]^s$	Right-truncation of the block of bits X: if X has bit-length greater than or equal to s, then $X]^s$ is the s-bit block consisting of the right-most s bits of X.
X<<1	Left shift of a block of bits X by one position: the rightmost bit of $Y = X$<<1 will always be set to zero.

X>>1 Right shift of a block of bits X by one position: the leftmost bit of $Y = X$>>1 will always be set to zero.

len Function taking a bit-string X as input, and which gives as output the number of bits in X.

mod If a and $b > 0$ are integers, then a mod b denotes the unique integer c such that:

i) $0 \leq c < b$, and

ii) a-c is an integer multiple of b.

5 Requirements

The authenticated encryption mechanisms specified in this document have the following requirements.

The originator and recipient of the data to which the authenticated encryption mechanism is to be applied, must:

a) agree on the use of a particular mechanism from those specified in this document;

b) agree on the use of a particular block cipher to be used with the mechanism (one of the block ciphers standardised in ISO/IEC 18033-3 shall be used);

c) share a secret key K: in all mechanisms except for authenticated encryption mechanism 5, this shall be a key for the selected block cipher, and in mechanism 5 it shall be a key used as input to a key derivation procedure.

In addition, each mechanism has specific requirements listed immediately prior to the mechanism description.

6 Authenticated encryption mechanism 1 (OCB 2.0)

6.1 Introduction

In this clause an authenticated encryption mechanism commonly known as OCB 2.0 (for *Offset Codebook* version 2) is defined.

NOTE OCB 2.0 is due to Krovetz and Rogaway [7]. OCB 2.0 possesses a proof of security on the assumption that the block cipher used possesses certain 'ideal properties'.

6.2 Specific notation

For the purposes of the specification of this mechanism, the following symbols and notation apply:

B Block of bits used in the definition of function J.

$B_1, B_2, \ldots, B_w$ Sequence of blocks of bits (each of n bits, with the possible exception of B_w) used in the definition of function J.

$C_1, C_2, \ldots, C_m$ Sequence of blocks of bits (each of n bits, with the possible exception of C_m) obtained as part of the output of the authenticated encryption process.

$D_1, D_2, \ldots, D_m$ Sequence of blocks of bits (each of n bits, with the possible exception of D_m) obtained by partitioning D.

F n-bit block used in the encryption and decryption processes.

H n-bit block used in the encryption and decryption processes.

J	Function used in the encryption and decryption processes.
k	Variable used in the definition of function J.
m	The number of n-bit blocks in the message to be encrypted (where the final block may contain less than n bits), i.e. the message contains $(m\text{-}1)n+r$ bits.
M_2	Function used in the encryption and decryption processes.
M_3	Function used in the encryption and decryption processes.
P	n-bit block used in the definition of M_2.
r	The number ($0 < r \leq n$) of bits in the final block of the message to be encrypted, after it has been divided into n-bit blocks, i.e. len(D) = $(m\text{-}1)n+r$.
S	Starting Variable (n bits).
T	Tag (t bits), adjoined to an encrypted message to provide integrity protection.
T'	Recomputed tag value, generated during the decryption process.
w	Variable used in the definition of function J.
Z	n-bit block used in the encryption and decryption processes.

6.3 Specific requirements

In advance of any use of the mechanism, the originator and recipient of the data to which the authenticated encryption mechanism is to be applied must agree on the tag length t in bits, where $0 < t \leq n$.

6.4 Definition of function M_2

Definition of the encryption and decryption procedures requires the definition of a function M_2 that takes an n-bit block as input and gives an n-bit block as output. The definition of this function depends on an n-bit block P. Since n must correspond to the bit length of a block cipher chosen from amongst those specified in ISO/IEC 18033-3, we only define P for n=64 and n=128.

a) If n=64, then $P = 0^{59}||11011$.

b) If n=128, then $P = 0^{120}||10000111$.

The function M_2 is defined as follows. If X is an n-bit block, then:

a) If the left-most (most significant) bit of X is zero, then $M_2(X) = X<<1$;

b) If the left-most (most significant) bit of X is one, then $M_2(X) = [X<<1] \oplus P$.

6.5 Definition of function M_3

Definition of the procedure for handling additional authenticated data requires the definition of a function M_3 that takes an n-bit block as input and gives an n-bit block as output. If X is an n-bit block, then:

$$M_3(X) = M_2(X) \oplus X.$$

6.6 Definition of function *J*

This function takes a block of bits B as input (where len(B) > 0), and gives an n-bit block $J(B)$ as output. The value $J(B)$ is computed as follows.

a) Partition B into a sequence of blocks: B_1, B_2, …, B_w, as follows. Let B_1 contain the first n bits of B, B_2 the next n bits, and so on, until B_w contains the final k bits, where $0 < k \leq n$. Thus, len(B) = (w-1)n+k.

b) Let $F = M_3(M_3(e_K(0^n)))$.

c) Let $C_0 = 0^n$.

d) For i = 1, 2, ..., w-1, perform the following two steps:

   1) Let $F = M_2(F)$;

   2) Let $C_i = C_{i-1} \oplus e_K(B_i \oplus F)$.

e) Let $F = M_3(M_2(F))$.

f) If $k<n$ then perform the following two steps:

   1) Let $F = M_3(F)$;

   2) Let $B_w = B_w \,||\, 1 \,||\, 0^{n-k-1}$.

g) $J(B) = e_K(C_{w-1} \oplus B_w \oplus F)$.

6.7 Encryption procedure

The originator shall perform the following steps to protect a data string D.

a) An n-bit Starting Variable S shall be selected. This variable shall be distinct for every message to be protected, and must be made available to the recipient of the message. However, it is not necessary that this value be unpredictable or secret.

   NOTE The value S could, for example, be generated using a counter maintained by the originator, and sent in cleartext along with the protected message.

b) Partition D into a sequence of blocks: D_1, D_2, …, D_m, as follows. Let D_1 contain the first n bits of D, D_2 the next n bits, and so on, until D_m contains the final r bits, where $0 < r \leq n$. Thus, len(D) = (m-1)n+r.

c) Let $F = e_K(S)$ and let $H = 0^n$.

d) For i = 1, 2, ..., m-1, perform the following three steps:

   1) Let $F = M_2(F)$;

   2) Let $H = H \oplus D_i$;

   3) Let $C_i = F \oplus e_K(D_i \oplus F)$.

e) Let $F = M_2(F)$.

f) Let $Z = e_K(\#_n(r) \oplus F)$.

g) Let $C_m = D_m \oplus Z|_r$.