INTERNATIONAL STANDARD

ISO/IEC 10116

Third edition
2006-02-01

Information technology — Security techniques — Modes of operation for an *n*-bit block cipher

Technologies de l'information — Techniques de sécurité — Modes opératoires pour un chiffrement par blocs de n-bits

Reference number
ISO/IEC 10116:2006(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

Figures

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 identfying any or all such patent rights.

ISO/IEC 10116 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcomittee SC 27, *IT Security techniques*.

This third edition cancels and replaces the second edition (ISO/IEC 10116:1997) which has been revised. Implementations that comply with ISO/IEC 10116:1997 will also comply with this third edition.

The main technical changes between the second edition and this third edition are as follows:

a) CBC mode has been extended to permit interleaving; and

b) a new mode (Counter mode) has been introduced.

Introduction

ISO/IEC 10116 specifies modes of operation for an n-bit block cipher. These modes provide methods for encrypting and decrypting data where the bit length of the data may exceed the size n of the block cipher.

This third edition of ISO/IEC 10116 specifies five modes of operation:

a) Electronic Codebook (ECB);

b) Cipher Block Chaining (CBC);

c) Cipher Feedback (CFB);

d) Output Feedback (OFB); and

e) Counter (CTR).

Information technology — Security techniques — Modes of operation for an n-bit block cipher

1 Scope

This International Standard establishes five modes of operation for applications of an n-bit block cipher (e.g. protection of data transmission, data storage). The defined modes only provide protection of data confidentiality. Protection of data integrity and requirements for padding the data are not within the scope of this International Standard. Also most modes do not protect the confidentiality of message length information.

This International Standard specifies the modes of operation and gives recommendations for choosing values of parameters (as appropriate).

The modes of operation specified in this International Standard have been assigned object identifiers in accordance with ISO/IEC 9834. The list of assigned object identifiers is given in Annex A. In applications in which object identifiers are used, the object identifiers specified in Annex A are to be used in preference to any other object identifiers that may exist for the mode concerned.

NOTE Annex B (informative) contains comments on the properties of each mode. Block ciphers are specified in ISO/IEC 18033-3.

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 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.

3.1
block chaining
encryption of information in such a way that each block of ciphertext is cryptographically dependent upon a preceding ciphertext block.

3.2
block cipher
symmetric encryption algorithm 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]

3.3
ciphertext
data which has been transformed to hide its information content.

3.4
counter
bit array of length n bits (where n is the size of the underlying block cipher) which is used in the Counter mode; its value when considered as the binary representation of an integer increases by one (modulo 2^n) after each block of plaintext is processed.

3.5
cryptographic synchronization
co-ordination of the encryption and decryption processes.

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
feedback buffer (*FB*)
variable used to store input data for the encryption process. At the starting point FB has the value of SV.

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

3.10
***n*-bit block cipher**
block cipher with the property that plaintext blocks and ciphertext blocks are n bits in length.

3.11
plaintext
unencrypted information.

3.12
starting variable (SV)
variable possibly derived from some initialization value and used in defining the starting point of the modes of operation.

NOTE The method of deriving the starting variable from the initializing value is not defined in this International Standard. It needs to be described in any application of the modes of operation.

4 Symbols (and abbreviated terms)

C	Ciphertext block.
CTR	Counter value.
d_K	Decryption function of the block cipher keyed by key K.
E	Intermediate variable.
e_K	Encryption function of the block cipher keyed by key K.
F	Intermediate variable.
FB	Feedback buffer.
i	Iteration.
j	Size of plaintext/ciphertext variable.
K	Key.
n	Plaintext/ciphertext block length for a block cipher.
m	Number of stored ciphertext blocks.
P	Plaintext block.
q	Number of plaintext/ciphertext variables.
r	Size of feedback buffer.
SV	Starting variable.
X	Block cipher input block.
Y	Block cipher output block.
$\|$	Concatenation of bit strings.

4.1 *a* mod *n*

For integers a and n, $a \mod n$ denotes the (non-negative) remainder obtained when a is divided by n. Equivalently if $b = a \mod n$, then b is the unique integer satisfying:

— $0 \leq b < n$, and

— $(b - a)$ is an integer multiple of n

4.2 array of bits

A variable denoted by a capital letter, such as P and C, represents a one-dimensional array of bits. For example,

$$A = (a_1, a_2, \ldots, a_m) \text{ and } B = (b_1, b_2, \ldots, b_m)$$

are arrays of m bits, numbered from 1 to m. All arrays of bits are written with the bit with the index 1 in the leftmost position. When interpreting a bit array as an integer the leftmost bit shall be the most significant bit.

4.3 bitwise addition modulo 2

The operation of bitwise addition, modulo 2, also known as the "exclusive or" function, is shown by the symbol $\oplus$. The operation when applied to arrays A and B of the same length is defined as

$$A \oplus B = (a_1 \oplus b_1, a_2 \oplus b_2, \ldots, a_m \oplus b_m)$$

4.4 decryption

The decryption relation defined by the block cipher is written

$$P = d_K(C)$$

where

— P is the plaintext block;
— C is the ciphertext block;
— K is the key.

4.5 encryption

The encryption relation defined by the block cipher is written

$$C = e_K(P)$$

where

— P is the plaintext block;

— C is the ciphertext block;
— K is the key.

4.6 selection of bits

The operation of selecting the j leftmost bits of an array $A = (a_1, a_2, \ldots, a_m)$ to generate a j-bit array is written

$$(j \sim A) = (a_1, a_2, \ldots, a_j)$$

The operation is defined only when $1 \leq j \leq m$.

4.7 shift operation

A "shift function" S_t is defined as follows: Given an m-bit variable X and a t-bit variable F where $1 \leq t \leq m$, the effect of the shift function $S_t(X \mid F)$ is to produce the m-bit variable

$$S_t(X \mid F) = (x_{t+1}, x_{t+2}, \ldots, x_m, f_1, f_2, \ldots, f_t) \qquad (t < m)$$
$$S_t(X \mid F) = (f_1, f_2, \ldots, f_t) \qquad (t = m)$$

The effect is to shift the bits of array X left by t places, discarding $x_1, x_2, \ldots, x_t$, and to place the array F in the rightmost t places of X. When $t = m$ the effect is to totally replace X by F.

4.8 $I(t)$

The variable $I(t)$ is a t-bit variable where the value 1 is assigned to every bit.

5 Requirements

For some of the described modes, padding of the plaintext variables may be required. Padding techniques, although important from a security perspective, are not within the scope of this International Standard, and throughout this standard it is assumed that any padding, as necessary, has already occurred.

NOTE Advice on the selection of a padding method for use with the CBC mode of operation is provided in Annex B.2.3.

For the Cipher Block Chaining (CBC) mode of operation (see clause 7), one parameter m needs to be selected. For the Cipher Feedback (CFB) mode of operation (see clause 8), three parameters r, j and k need to be selected. For the Output Feedback (OFB) mode of operation (see clause 9) and the Counter (CTR) mode of operation (see clause 10), one parameter j needs to be selected. When one of these modes of operation is used the same parameter value(s) need to be chosen and used by all communicating parties. These parameters need not be kept secret.

All modes of operation specified in this International Standard require the parties encrypting and decrypting a data string to share a secret key K for the block cipher in use. All modes of

operation apart from the Electronic Codebook (ECB) mode also require the parties to share a starting variable SV, where the length of SV will depend on the mode in use. The value of the starting variable should normally be different for every data string encrypted using a particular key (see also Annex B). How keys and starting variables are managed and distributed is outside the scope of this International Standard.

6 Electronic Codebook (ECB) mode

6.1 Preliminaries

The variables employed by the ECB mode of encryption are

a) The input variables

   1) A sequence of q plaintext blocks $P_1, P_2, \ldots, P_q$, each of n bits.
   2) A key K.

b) The output variables, i.e. a sequence of q ciphertext variables $C_1, C_2, \ldots, C_q$, each of n bits.

6.2 Encryption

The ECB mode of encryption operates as follows:

$$C_i = e_K(P_i) \text{ for } i = 1, 2, \ldots, q.$$

6.3 Decryption

The ECB mode of decryption operates as follows:

$$P_i = d_K(C_i) \text{ for } i = 1, 2, ..., q.$$

7 Cipher Block Chaining (CBC) mode

7.1 Preliminaries

The CBC mode of operation is defined by an interleave parameter $m > 0$, the number of ciphertext blocks that must be stored whilst processing the mode. The value of m should be small (typically $m = 1$) and at most 1024.

NOTE The choice of 1024 as the upper limit for m is somewhat arbitrary. It is intended to provide a realistic upper bound on the number of hardware processors.

The variables employed by the CBC mode are

a) The input variables

1) A sequence of q plaintext blocks $P_1, P_2, \ldots, P_q$, each of n bits.
2) A key K.
3) A sequence of m starting variables $SV_1, SV_2, \ldots, SV_m$ each of n bits.

NOTE If $m = 1$ then this mode is compatible with the CBC mode described in the second edition of this standard (ISO/IEC 10116:1997).

b) The output variables, i.e. a sequence of q ciphertext variables $C_1, C_2, \ldots, C_q$, each of n bits.

7.2 Encryption

The CBC mode of encryption operates as follows:

$$C_i = e_K(P_i \oplus SV_i), 1 \leq i \leq \min(m, q)$$

If $q > m$, all subsequent plaintext blocks are encrypted as:

$$C_i = e_K(P_i \oplus C_{i-m}), m + 1 \leq i \leq q$$

NOTE At any time during the computation, the values of the m most recent ciphertext blocks need to be stored, e.g. in a cyclically used "feedback buffer" FB (see figure C.2).

This procedure is shown in the left side of figure C.2.

7.3 Decryption

The CBC mode of decryption operates as follows:

$$P_i = d_K(C_i) \oplus SV_i, 1 \leq i \leq \min(m, q)$$

If $q > m$, all subsequent plaintext blocks are computed as:

$$P_i = d_K(C_i) \oplus C_{i-m}, m + 1 \leq i \leq q$$

NOTE At any time during the computation, the values of the m most recent ciphertext blocks need to be stored, e.g. in a cyclically used 'feedback buffer' FB (see figure C.2).

This procedure is shown in the right side of figure C.2.