

INTERNATIONAL STANDARD

ISO/IEC
10116

Second edition
1997-04-15

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

*Technologies de l'information — Techniques de sécurité — Modes
opérateurs d'un chiffrement par blocs de *n*-bits*



Reference number
ISO/IEC 10116:1997(E)

AVA Documents
Document Sharing Hub

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. 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.

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

This second edition cancels and replaces the first edition (ISO/IEC 10116:1991), which has been technically revised.

Annexes A to D of this International Standard are for information only.

© ISO/IEC 1997

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from the publisher.

ISO/IEC Copyright Office • Case postale 56 • CH-1211 Genève 20 • Switzerland

Printed in Switzerland

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

1 Scope

This International Standard describes four modes of operation for an n -bit block cipher.

NOTE - Annex A (informative) contains comments on the properties of each mode.

This International Standard establishes four defined modes of operation so that in applications of an n -bit block cipher (e.g. protection of data transmission, data storage, authentication) this International Standard will provide a useful reference for, for example, the specification of the mode of operation and the values of parameters (as appropriate).

2 Definitions

For the purposes of this International Standard, the following definitions apply.

2.1 block chaining: The encipherment of information such that each block of ciphertext is cryptographically dependent upon the preceding ciphertext block.

2.2 ciphertext: Data which has been transformed to hide its information content.

2.3 cryptographic synchronization: The co-ordination of the encipherment and decipherment processes.

2.4 decipherment: The reversal of a corresponding encipherment.

2.5 encipherment: The (reversible) transformation of data by a cryptographic algorithm to produce ciphertext, i.e. to hide the data.

2.6 feedback buffer (FB): Variable used to store input data for the encipherment process. At the starting point FB has the value of SV .

2.7 initializing value: Value used in defining the starting point of an encipherment process.

2.8 key: A sequence of symbols that controls the operation of a cryptographic transformation (e.g. encipherment, decipherment)

2.9 n -bit block cipher: A block cipher with the property that plaintext blocks and ciphertext blocks are n bits in length.

2.10 plaintext: Unciphered information.

2.11 starting variable (SV): Variable defining the starting point of the mode 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.

3 Notation

3.1 encipherment: For the purposes of this International Standard the functional relation defined by the block cipher is written

$$C = eK(P)$$

where

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

The expression eK is the operation of encipherment using the key K .

3.2 decipherment: The corresponding decipherment function is written

$$P = dK(C)$$

The expression dK is the operation of decipherment using the key K .

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

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

are arrays of m bits, numbered from 1 to m . All arrays of bits are written with the bit with index 1 in the leftmost position.

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

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

3.5 selection of bits: The operation of selecting the j leftmost bits of A to generate a j -bit array is written

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

This operation is defined only when $1 \leq j \leq m$ where m is the number of bits in A .

3.6 shift operation: A "shift function" S_k is defined as follows:

Given an m -bit variable X and a k -bit variable F where $1 \leq k \leq m$, the effect of a shift function $S_k(X|F)$ is to produce the m -bit variable

$$\begin{aligned} S_k(X|F) &= (x_{k+1}, x_{k+2}, \dots, x_m, f_1, f_2, \dots, f_k) & (k < m) \\ S_k(X|F) &= (f_1, \dots, f_k) & (k = m) \end{aligned}$$

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

A special case of this function begins with the m -bit variable $I(m)$ of successive "1" bits and shifts the variable F of k bits into it.

The result is

$$\begin{aligned} S_k(I(m)|F) &= (1, 1, \dots, 1, f_1, f_2, \dots, f_k) & (k < m) \\ S_k(I(m)|F) &= (f_1, f_2, \dots, f_k) & (k = m) \end{aligned}$$

where the $m - k$ leftmost bits are "1".

4 Requirements

For some of the described modes padding of the plaintext variables may be required. Padding techniques are not within the scope of this International Standard.

For the Cipher Feedback (CFB) Mode of operation (see clause 7), three parameters r , j and k are defined. For the Output Feedback (OFB) Mode of operation (see clause 8), one parameter j is defined. When one of these modes of operation is used the same parameter value(s) need(s) to be chosen and used by all communicating parties.

5 Electronic Codebook (ECB) Mode

5.1 The variables employed for the ECB mode of encipherment are

- A sequence of q plaintext blocks $P_1, P_2, \dots, P_q$ each of n bits.
- A key K .
- The resultant sequence of q ciphertext blocks $C_1, C_2, \dots, C_q$ each of n bits.

5.2 The ECB mode of encipherment is described as follows:

$$C_i = eK(P_i) \text{ for } i = 1, 2, \dots, q \quad (1)$$

5.3 The ECB mode of decipherment is described as follows:

$$P_i = dK(C_i) \text{ for } i = 1, 2, \dots, q \quad (2)$$

6 Cipher Block Chaining (CBC) Mode

6.1 The variables employed for the CBC mode of encipherment are

- A sequence of q plaintext blocks $P_1, P_2, \dots, P_q$ each of n bits.
- A key K .
- A starting variable SV of n bits.
- A sequence of q ciphertext blocks $C_1, C_2, \dots, C_q$ each of n bits.

6.2 The CBC mode of encipherment is described as follows:

Encipherment of the first plaintext block,

$$C_1 = eK(P_1 \oplus SV) \quad (3)$$

subsequently,

$$C_i = eK(P_i \oplus C_{i-1}) \text{ for } i = 2, 3, \dots, q \quad (4)$$

This procedure is shown in the upper part of figure 1. The starting variable SV is used in the generation of the first ciphertext output. Subsequently the ciphertext is added, modulo 2, to the next plaintext before encipherment.

6.3 The CBC mode of decipherment is described as follows:

Decipherment of the first ciphertext block,

$$P_1 = dK(C_1) \oplus SV \quad (5)$$

subsequently,

$$P_i = dK(C_i) \oplus C_{i-1} \text{ for } i = 2, 3, \dots, q \quad (6)$$

This procedure is shown in the lower part of figure 1.

7 Cipher Feedback (CFB) Mode

7.1 Three parameters define a CFB mode of operation:

- the size of feedback buffer, r , where $n \leq r \leq 2n$
- the size of feedback variable, k , where $1 \leq k \leq n$
- the size of plaintext variable, j , where $1 \leq j \leq k$

NOTES

1 $r - k$ may be smaller than n . Figure 2 shows the special case where $r - k > n$.

2 If $r = n$ then this mode is compatible with the CFB Mode described in the previous edition of this International Standard.

The variables employed for the CFB mode of operation are

a) The input variables

- A sequence of q plaintext variables $P_1, P_2, \dots, P_q$ each of j bits.
- A key K .
- A starting variable SV of r bits.

b) The intermediate results

- 1) A sequence of q block cipher input blocks $X_1, X_2, \dots, X_q$, each of n bits.
- 2) A sequence of q block cipher output blocks $Y_1, Y_2, \dots, Y_q$, each of n bits.
- 3) A sequence of q variables $E_1, E_2, \dots, E_q$, each of j bits.
- 4) A sequence of $q-1$ feedback variables $F_1, F_2, \dots, F_{q-1}$, each of k bits.
- 5) A sequence of $q-1$ feedback buffer contents $FB_1, FB_2, \dots, FB_{q-1}$, each of r bits.

- c) The output variables, i.e. a sequence of q ciphertext variables $C_1, C_2, \dots, C_q$, each of j bits.

7.2 The feedback buffer FB is set to its initial value

$$FB_1 = SV \quad (7)$$

The operation of enciphering each plaintext variable employs the following six steps:

- a) $X_i = FB_i \sim n$ (8)
- b) Use of block cipher, $Y_i = eK(X_i)$ (9)
- c) Selection of leftmost j bits, $E_i = Y_i \sim j$ (10)
- d) Generation of ciphertext variable, $C_i = P_i \oplus E_i$ (11)
- e) Generation of feedback variable, $F_i = S_j(I(k)|C_i)$ (12)
- f) Shift function on FB , $FB_{i+1} = S_k(FB_i|F_i)$ (13)

These steps are repeated for $i = 1, 2, \dots, q$, ending with equation (11) on the last cycle. The procedure is shown in the left side of figure 2. The leftmost j bits of the output block Y of the block cipher are used to encipher the j -bit plaintext variable by modulo 2 addition. The remaining bits of Y are discarded. The plaintext and ciphertext variables have bits numbered from 1 to j .

The ciphertext variable is augmented by placing $k-j$ "1" bits in its leftmost bit positions to become the k -bit feedback variable F . Then the bits of the feedback buffer FB are shifted left by k places and F is inserted in the rightmost k places, to produce the new value of the feedback buffer FB . In this shift operation, the leftmost k bits of FB are discarded. The new n leftmost bits of FB are used as the next input X of the encipherment process.

7.3 The variables employed for decipherment are the same as those employed for encipherment.

The feedback buffer FB is set to its initial value

$$FB_1 = SV \quad (14)$$

The operation of deciphering each ciphertext variable employs the following six steps:

- a) $X_i = FB_i \sim n$ (15)
- b) Use of block cipher, $Y_i = eK(X_i)$ (16)
- c) Selection of leftmost j bits, $E_i = Y_i \sim j$ (17)
- d) Generation of plaintext variable, $P_i = C_i \oplus E_i$ (18)
- e) Generation of feedback variable, $F_i = S_j(I(k)|C_i)$ (19)
- f) Shift function on FB , $FB_{i+1} = S_k(FB_i|F_i)$ (20)

These steps are repeated for $i = 1, 2, \dots, q$, ending with equation (18) on the last cycle. The procedure is shown in the right side of figure 2. The leftmost j bits of the output block Y of the block cipher are used to decipher the j -bit ciphertext variable by modulo 2 addition. The remaining bits of Y are discarded. The plaintext and ciphertext variables have bits numbered from 1 to j .

The ciphertext variable is augmented by placing $k-j$ "1" bits in its leftmost bit positions to become the k -bit feedback variable F . Then the bits of the feedback buffer FB are shifted left by k places and F is inserted in the rightmost k places to produce the new value of FB . In this shift operation, the leftmost k bits of FB are discarded. The new n leftmost bits of FB are used as the next input X of the encipherment process.

7.4 It is recommended that CFB should be used with equal values of j and k . In this recommended form ($j = k$) the equations (12) and (19) can be written

$$F_i = C_i \text{ (case } j = k)$$

8 Output Feedback (OFB) Mode

8.1 The OFB mode of operation is defined by one parameter, i.e. the size of plaintext variable j where $1 \leq j \leq n$.

The variables employed for the OFB mode of operation are

a) The input variables

- 1) A sequence of q plaintext variables $P_1, P_2, \dots, P_q$, each of j bits.
- 2) A key K .
- 3) A starting variable SV of n bits.

b) The intermediate results

- 1) A sequence of q block cipher input blocks $X_1, X_2, \dots, X_q$, each of n bits.
- 2) A sequence of q block cipher output blocks $Y_1, Y_2, \dots, Y_q$, each of n bits.
- 3) A sequence of q variables $E_1, E_2, \dots, E_q$, each of j bits.
- c) The output variables, i.e. a sequence of q ciphertext variables $C_1, C_2, \dots, C_q$, each of j bits.

8.2 The input block X is set to its initial value

$$X_1 = SV \quad (21)$$

The operation of enciphering each plaintext variable employs the following four steps:

- a) Use of block cipher, $Y_i = eK(X_i)$ (22)
- b) Selection of leftmost j bits, $E_i = Y_i \sim j$ (23)
- c) Generation of ciphertext variable, $C_i = P_i \oplus E_i$ (24)
- d) Feedback operation, $X_{i+1} = Y_i$ (25)

These steps are repeated for $i = 1, 2, \dots, q$, ending with equation (24) on the last cycle. The procedure is shown on the left side of figure 3. The result of each use of the block