

---

6 Ub b]ýhj c'!'Dcglcd\_]`Yb\_f]dWj`Y'gdcfc ]`ftlcc`cj Ub`Y'g'dfUj b]a ]`cgYVUa ]L!'&"XY.  
8 95 `fU[ cf]hYa `nUYb\_f]dWj`c`dcXUh\_cj Ł

Banking -- Procedures for message encipherment (wholesale) -- Part 2: DEA algorithm

Banque -- Procédures de chiffrement de messages (service aux entreprises) -- Partie 2:  
Algorithme DEA

**ITeH STANDARD PREVIEW**  
**(standards.iteh.ai)**

Ta slovenski standard je istoveten z: **ISO 10126-2:1991**  
<https://standards.iteh.ai/catalog/standards/sist/ccc68da7-7bed-46e2-80c1-f41c02cd2977/sist-iso-10126-2-1995>

**ICS:**

35.240.40      Wj [ |æ} ā\^Á^zāç^ÁVÁç      IT applications in banking  
àæ } āç

**SIST ISO 10126-2:1995****en**

**iTeh STANDARD PREVIEW**  
**(standards.iteh.ai)**

[SIST ISO 10126-2:1995](#)

<https://standards.iteh.ai/catalog/standards/sist/cee68da7-7bed-46e2-80c1-f41c02cd2977/sist-iso-10126-2-1995>

# INTERNATIONAL STANDARD

**ISO**  
**10126-2**

First edition  
1991-07-15

---

---

## Banking - Procedures for message encipherment (wholesale) —

### Part 2: DEA algorithm

iTeh STANDARD PREVIEW  
(standards.iteh.ai)

*Banque — Procédures de chiffrement de messages (service aux  
entreprises)*  
[https://standards.iteh.ai/catalog/standards/sist/cee68da7-7bed-46e2-80c1-  
429110126-2](https://standards.iteh.ai/catalog/standards/sist/cee68da7-7bed-46e2-80c1-429110126-2) *Partie 2: Algorithme DEA 1995*



Reference number  
ISO 10126-2:1991(E)

## ISO 10126-2:1991(E)

## Contents

	Page
1 Scope .....	1
2 Normative references .....	1
3 Modes of operation .....	1
4 Initialization Vectors (IVs) .....	1
5 Initial Text Sequence (ITS) .....	2
6 Padding field (CBC mode only) .....	2
7 Independent encipherment and decipherment of encipherment elements .....	3

**iTeh STANDARD PREVIEW**  
**(standards.iteh.ai)**

[SIST ISO 10126-2:1995](https://standards.iteh.ai/catalog/standards/sist/cee68da7-7bed-46e2-80c1-f41c02cd2977/sist-iso-10126-2-1995)

<https://standards.iteh.ai/catalog/standards/sist/cee68da7-7bed-46e2-80c1-f41c02cd2977/sist-iso-10126-2-1995>

© ISO 1991

All rights reserved. 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.

International Organization for Standardization  
Case Postale 56 • CH-1211 Genève 20 • Switzerland

Printed in Switzerland

## Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75% of the member bodies casting a vote.

International Standard ISO 10126-2 was prepared by Technical Committee ISO/TC 68, *Banking and related financial services*.

ISO 10126 consists of the following parts, under the general title *Banking - Procedures for message encipherment (wholesale)*:

— Part 1: *General principles*

— Part 2: *DEA algorithm*

ISO 10126 originates from work done in ANSI, and is a development of (while remaining compatible with) ANSI X9.23 (1988), *Financial Institution: Encryption of Wholesale Financial Messages*.

**iTeh STANDARD PREVIEW**  
**(standards.iteh.ai)**

This page intentionally left blank

[SIST ISO 10126-2:1995](#)

<https://standards.iteh.ai/catalog/standards/sist/cee68da7-7bed-46e2-80c1-f41c02cd2977/sist-iso-10126-2-1995>

# Banking - Procedures for message encipherment (wholesale) —

## Part 2: DEA algorithm

### 1 Scope

ISO 10126-1 specifies a method for the encipherment and decipherment of entire (or part of) wholesale financial messages by the use of application level encipherment, for the purpose of providing confidentiality.

DEA may be used as a suitable algorithm to implement ISO 10126-1. It is specified in ANSI X3.92. Keys shall be managed in accordance with ISO 8732.

### 2 Normative references

The following standards contain provisions which, through reference in this text, constitute provisions of this part of ISO 10126. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this part of ISO 10126 are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below. Members of IEC and ISO maintain registers of currently valid International Standards.

ISO 8372:1987, *Information processing — Modes of operation for a 64-bit block cipher algorithm*.

ISO 8732:1988, *Banking — Key management (wholesale)*.

ISO 10126-1:1991<sup>1)</sup>, *Banking — Procedures for message encipherment (wholesale) — Part 1: General principles*.

ANSI X3.92:1981, *American National Standard for information Systems — Data Encryption Algorithm*.

### 3 Modes of operation

The modes of operation that shall be used are Cipher Block Chaining (CBC), One Bit Cipher Feedback (CFB-1) or Eight Bit Cipher Feedback (CFB-8) as defined in ISO 8372-1.

### 4 Initialization Vectors (IVs)

An IV is used as a starting point for the encipherment and decipherment of a data sequence to increase security by introducing additional cryptographic variance (i.e. a repeated plaintext sequence will not result in a repeated ciphertext sequence) and to synchronize cryptographic equipment.

#### 4.1 Cipher Block Chaining (CBC)

A new random, pseudo-random or non-repeating 64-bit IV shall be used for each cryptoperiod. The same IV may be used within the cryptoperiod of the associated key.

#### 4.2 Cipher Feedback (CFB)

A new random, pseudo-random, or non-repeating 48- or 64-bit IV shall be used for each message.

1) To be published.

## ISO 10126-2:1991(E)

## 5 Initial Text Sequence (ITS)

In the case of CBC, if the IV is not changed for each message, then a new random, pseudo-random, or non-repeating 64-bit Initial Text Sequence (ITS) shall immediately precede the message data to be protected. If a new random, pseudo-random, or non-repeating IV is used for each message, then no ITS is required.

## 6 Padding field (CBC mode only)

Padding shall be present in every CBC message. Plaintext shall be padded to a multiple of 64 bits before encipherment using the CBC mode. Padding shall be performed using either bits or octets by appending a padding field to the end of the plaintext (as shown cross-hatched in figure 1). After decipherment, the padding field shall be discarded.

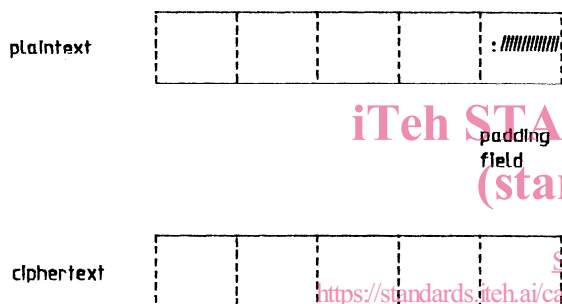
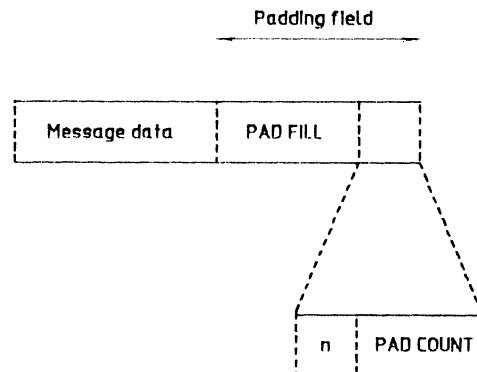


Figure 1 — Message padding

When padding with bits, the padding field shall consist of 8 to 71 bits divided into two subfields (see figure 2). The first subfield (pad fill) shall consist of 0 to 63 bits with arbitrary contents. The second subfield (pad count) shall consist of 8 bits containing the number of bits in the padding field, in the range of

8 to 71. The left-most bit of the pad count shall indicate that the pad count is given in bits (value of 1). The remaining bits of the pad count shall contain an unsigned binary number. That number shall be the total number of bits in the padding field. See table 1 for further information on padding with bits (CBC mode only).



NOTE — When  $n = 1$ , pad count in bits;  
when  $n = 0$ , pad count in octets.

Figure 2 — Padding field format

iTeh STANDARD PREVIEW  
(standards.iteh.ai)

When padding with octets, the padding field shall consist of 1 to 8 octets divided into two subfields (see figure 2). The first subfield (pad fill) shall consist of 0 to 7 octets with arbitrary contents. The second subfield (pad count) shall consist of one octet containing the number of octets in the padding field in the range of 1 to 8. The left-most bit of the pad count shall indicate that the pad count is given in octets (value of 0). The remaining bits of the pad count shall contain an unsigned binary number. That number shall be the total number of padding octets in the padding field. See table 2 for further information on padding with octets (CBC mode only).