
**Information security — Lightweight
cryptography —**

**Part 2:
Block ciphers**

*Sécurité de l'information — Cryptographie pour environnements
contraints —*

Partie 2: Chiffrements par blocs



This document is a preview generated by EMS



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2019

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

	Page
Foreword	iv
Introduction	v
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Symbols	2
5 Lightweight block cipher with a block size of 64 bits	2
5.1 General	2
5.2 PRESENT	2
5.2.1 PRESENT algorithm	2
5.2.2 PRESENT specific notation	2
5.2.3 PRESENT encryption	3
5.2.4 PRESENT decryption	4
5.2.5 PRESENT transformations	4
5.2.6 PRESENT key schedule	5
6 Lightweight block ciphers with a block size of 128 bits	7
6.1 General	7
6.2 CLEFIA	7
6.2.1 CLEFIA algorithm	7
6.2.2 CLEFIA specific notation	7
6.2.3 CLEFIA encryption	7
6.2.4 CLEFIA decryption	8
6.2.5 CLEFIA building blocks	9
6.2.6 CLEFIA key schedule	14
6.3 LEA	24
6.3.1 LEA algorithm	24
6.3.2 LEA specific notation	24
6.3.3 LEA encryption	24
6.3.4 LEA decryption	26
6.3.5 LEA key schedule	27
Annex A (normative) Object identifiers	30
Annex B (informative) Numerical examples	31
Annex C (informative) Feature tables	53
Annex D (informative) A limitation of a block cipher under a single key	55
Bibliography	56

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.

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) or the IEC list of patent declarations received (see <http://patents.iec.ch>).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

This document was prepared by Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

This second edition cancels and replaces the first edition (ISO/IEC 29192-2:2012), which has been technically revised.

The main changes compared to the previous edition are as follows:

- the LEA algorithm has been added to [6.3](#);
- numerical examples and feature tables of LEA have been added to [B.3](#) and [Annex C](#).

A list of all parts in the ISO/IEC 29192 series can be found on the ISO website.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

ISO/IEC 29192-1 specifies the requirements for lightweight cryptography.

A block cipher maps blocks of n bits to blocks of n bits, under the control of a key of k bits.

The International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) draws attention to the fact that it is claimed that compliance with this document may involve the use of a patent.

ISO and IEC takes no position concerning the evidence, validity and scope of this patent right.

The holder of this patent right has assured ISO and IEC that he/she is willing to negotiate licences under reasonable and non-discriminatory terms and conditions with applicants throughout the world. In this respect, the statement of the holder of this patent right is registered with ISO and IEC. Information may be obtained from the patent database available at www.iso.org/patents.

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

Information security — Lightweight cryptography —

Part 2: Block ciphers

1 Scope

This document specifies three block ciphers suitable for applications requiring lightweight cryptographic implementations:

- PRESENT: a lightweight block cipher with a block size of 64 bits and a key size of 80 or 128 bits;
- CLEFIA: a lightweight block cipher with a block size of 128 bits and a key size of 128, 192 or 256 bits;
- LEA: a lightweight block cipher with a block size of 128 bits and a key size of 128, 192 or 256 bits.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

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

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- ISO Online browsing platform: available at <https://www.iso.org/obp>
- IEC Electropedia: available at <http://www.electropedia.org/>

3.1 block

string of bits of defined length

[SOURCE: ISO/IEC 18033-1:2015, 2.8]

3.2 block cipher

symmetric encipherment system with the property that the encryption algorithm operates on a *block* (3.1) of *plaintext* (3.6), i.e. a string of bits of a defined length, to yield a block of *ciphertext* (3.3)

[SOURCE: ISO/IEC 18033-1:2015, 2.9]

3.3 ciphertext

data which has been transformed to hide its information content

[SOURCE: ISO/IEC 10116:2017, 3.2]

3.4 key

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

[SOURCE: ISO/IEC 18033-1:2015, 2.27]