

Second edition
2011-12-15

Information technology — Security techniques — Encryption algorithms —

Part 4: Stream ciphers

Technologies de l'information — Techniques de sécurité — Algorithmes de chiffrement —

Partie 4: Chiffrements en flot

Reference number
ISO/IEC 18033-4:2011(E)



This is a preview of "ISO/IEC 18033-4:2011". [Click here to purchase the full version from the ANSI store.](#)



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2011

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 either ISO at the address below or ISO's member body in the country of the requester.

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

This is a preview of "ISO/IEC 18033-4:2011". Click here to purchase the full version from the ANSI store.

Contents

Page

Foreword	iv
Introduction.....	v
1 Scope	1
2 Normative references.....	1
3 Terms and definitions	1
4 Symbols and abbreviated terms	3
4.1 Symbols.....	3
4.2 Functions	5
5 Framework for stream ciphers	6
6 General models for stream ciphers	6
6.1 Keystream generators.....	6
6.2 Output functions.....	7
7 Constructing keystream generators from block ciphers	10
7.1 Block cipher modes for a synchronous keystream generator	10
7.2 Block cipher mode for a self-synchronizing keystream generator	12
8 Dedicated keystream generators	13
8.1 MUGI keystream generator	13
8.2 SNOW 2.0 keystream generator	18
8.3 Rabbit keystream generator	23
8.4 Decim ^{v2} keystream generator	27
8.5 KCipher-2 (K2) keystream generator	33
Annex A (normative) Object Identifiers	43
Annex B (informative) Operations over the finite field $GF(2^n)$	45
Annex C (informative) Examples	46
Annex D (informative) Security information.....	88
Bibliography.....	91

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 18033-4 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 18033-4:2005), which has been technically revised. It also incorporates the Amendment ISO/IEC 18033-4:2005/Amd.1:2009.

ISO/IEC 18033 consists of the following parts, under the general title *Information technology — Security techniques — Encryption algorithms*:

- *Part 1: General*
- *Part 2: Asymmetric ciphers*
- *Part 3: Block ciphers*
- *Part 4: Stream ciphers*

This is a preview of "ISO/IEC 18033-4:2011". [Click here to purchase the full version from the ANSI store.](#)

Introduction

This part of ISO/IEC 18033 includes stream cipher algorithms. A stream cipher is an encryption mechanism that uses a keystream to encrypt a plaintext in a bitwise or a block-wise manner. There are two types of stream ciphers: a synchronous stream cipher, in which the keystream is generated from only the secret key (and an initialization vector) and a self-synchronizing stream cipher, in which the keystream is generated from the secret key and some past ciphertexts (and an initialization vector). This part of ISO/IEC 18033 describes both pseudorandom number generators for producing keystream and output functions to combine a keystream with plaintext.

This part of ISO/IEC 18033 includes two output functions:

- Binary-additive output function; and
- MULTI-S01 output function.

This part of ISO/IEC 18033 includes five dedicated keystream generators:

- MUGI keystream generator;
- SNOW 2.0 keystream generator;
- Rabbit keystream generator;
- Decim^{v2} keystream generator; and
- KCipher-2 (K2) keystream generator.