BS ISO/IEC 18033-4:2011

BSI Standards Publication

Information technology — Security techniques — Encryption algorithms — Part 4: Stream ciphers

This British Standard is the UK implementation of ISO/IEC 18033-4:2011. It supersedes BS ISO/IEC 18033-4:2005+A1:2009 which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee IST/33, IT - Security techniques.

A list of organizations represented on this committee can be obtained on request to its secretary.

ISBN 978 0 580 68085 4

ICS 35.040

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 January 2012.

Amendments issued since publication

Date	Text affected

INTERNATIONAL **ISO/IEC**

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)

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

Page

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*

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.

Information technology — Security techniques — Encryption algorithms —

Part 4: Stream ciphers

1 Scope

This part of ISO/IEC 18033 specifies

a) output functions to combine a keystream with plaintext,

b) keystream generators for producing keystream, and

c) object identifiers assigned to dedicated keystream generators in accordance with ISO/IEC 9834.

NOTE 1 The list of assigned object identifiers is given in Annex A.

NOTE 2 Any change to the specification of these algorithms resulting in a change of functional behaviour will result in a change of the object identifier assigned to the algorithms concerned.

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 18033-1, *Information technology — Security techniques — Encryption algorithms — Part 1: General*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 18033-1 and the following apply.

3.1
big-endian
method of storage of multi-byte numbers with the most significant bytes at the lowest memory addresses

[ISO/IEC 10118-1:2000]

3.2
ciphertext
data which has been transformed to hide its information content

[ISO/IEC 10116:2006]