

STN	Informačné technológie Bezpečnostné metódy Šifrovacie algoritmy Časť 4: Prúdové šifry	STN ISO/IEC 18033-4 97 4121
------------	--	---

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

Informationstechnik
Sicherheitsverfahren
Verschlüsselungsalgorithmen
Teil 4: Stromchiffren

Táto norma obsahuje anglickú verziu ISO/IEC 18033-4: 2011.

This standard includes the English version of ISO/IEC 18033-4: 2011.

132934

Úrad pre normalizáciu, metrológiu a skúšobníctvo Slovenskej republiky, 2021

Slovenská technická norma a technická normalizačná informácia je chránená zákonom č. 60/2018 Z. z. o technickej normalizácii.

Anotácia

Táto časť ISO/IEC 18033 obsahuje algoritmy prúdovej šifry. Prúdová šifra je šifrovací mechanizmus, ktorý využíva kľúčový prúd na šifrovanie otvoreného textu bitovým alebo blokovým spôsobom. Existujú dva typy prúdových šifier: synchronna prúdová šifra, v ktorej sa kľúčový tok generuje iba z tajného kľúča (a inicializačný vektor) a samosynchronizačná prúdová šifra, v ktorej sa kľúčový prúd generuje z tajného kľúča a niektoré minulé šifrované texty (a inicializačný vektor).

Táto časť ISO/IEC 18033 popisuje generátory pseudonáhodných čísel na produkciu kľúčových tokov a výstupné funkcie na kombináciu kľúčového toku s otvoreným textom.

Táto časť ISO/IEC 18033 špecifikuje

- a) výstupné funkcie na kombináciu kľúčového toku v otvorenom texte,
- b) generátory kľúčového toku na výrobu kľúčového toku a
- c) identifikátory objektov pridelené špecializovaným generátorom kľúčových prúdov v súlade s ISO/IEC 9834.

Národný predhovor

Normatívne referenčné dokumenty

Nasledujúce dokumenty, celé alebo ich časti, sú v tomto dokumente normatívnymi odkazmi a sú nevyhnutné pri jeho používaní. Pri datovaných odkazoch sa použije len citované vydanie. Pri nedatovaných odkazoch sa použije najnovšie vydanie citovaného dokumentu (vrátane všetkých zmien).

POZNÁMKA 1. – Ak bola medzinárodná publikácia zmenená spoločnými modifikáciami, čo je indikované označením (mod), použije sa príslušná EN/HD.

POZNÁMKA 2. – Aktuálne informácie o platných a zrušených STN možno získať na webovej stránke www.unms.sk.

ISO/IEC 18033-1 dosiaľ nezavedená

Vypracovanie normy

Spracovateľ: Úrad pre normalizáciu, metrológiu a skúšobníctvo SR, Bratislava

Technická komisia: TK 37 Informačné technológie

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

ISO/IEC 18033-4:2011(E)**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*

koniec náhľadu – text ďalej pokračuje v platenej verzii STN