ICS 35.030 SLOVENSKÁ TECHNICKÁ NORMA Apríl 2022

STN	**Informačná bezpečnosť** **Generovanie prvočísel**	**STN** **ISO/IEC 18032** 97 4120

Information security
Prime number generation

Sécurité de l'information
Génération de nombres premiers

Informationstechnik
Sicherheitsverfahren
Generierung von Primzahlen

Táto norma obsahuje anglickú verziu ISO/IEC 18032: 2020.

This standard includes the English version of ISO/IEC 18032: 2020.

134595

Anotácia

Tento dokument špecifikuje metódy na generovanie a testovanie prvočísel, ako sa to vyžaduje v kryptografických protokoloch a algoritmoch.

Po prvé, tento dokument špecifikuje metódy na testovanie, či je dané číslo prvočíslo. Testovacie metódy zahrnuté v tomto dokumente sú rozdelené do dvoch skupín:

– testy pravdepodobnosti prvočíselnosti, ktoré majú malú pravdepodobnosť chyby. Všetky tu opísané pravdepodobnostné testy môžu vyhlásiť kompozit za prvočíslo;

– deterministické metódy, ktoré zaručene poskytnú správny výsledok. Tieto metódy využívajú takzvané certifikáty prvočíselnosti.

Po druhé, tento dokument špecifikuje metódy na generovanie prvočísel. Opäť sú prezentované pravdepodobnostné aj deterministické metódy.

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 18031 dosiaľ nezavedená

Vypracovanie normy

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

Technická komisia: TK 37 Informačné technológie

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.

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.

This document was prepared by Joint 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 18032:2005), which has been technically revised.

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

— the Frobenius-Grantham primality test in 6.2, the Lehmann primality test in 6.3 and Maurer's algorithm in 8.3.1, have been removed;

– the Elliptic curve primality proving algorithm, The Shawe-Taylor algorithm and the algorithm to generate primes with side conditions, have been added or substantially revised.

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.

INTERNATIONAL STANDARD ISO/IEC 18032:2020(E)

Information security — Prime number generation

1 Scope

This document specifies methods for generating and testing prime numbers as required in cryptographic protocols and algorithms.

Firstly, this document specifies methods for testing whether a given number is prime. The testing methods included in this document are divided into two groups:

— probabilistic primality tests, which have a small error probability. All probabilistic tests described here can declare a composite to be a prime;

— deterministic methods, which are guaranteed to give the right verdict. These methods use so-called primality certificates.

Secondly, this document specifies methods to generate prime numbers. Again, both probabilistic and deterministic methods are presented.

NOTE It is possible that readers with a background in algorithm theory have already had previous encounters with probabilistic and deterministic algorithms. The deterministic methods in this document internally still make use of random bits (to be generated via methods described in ISO/IEC 18031), and "deterministic" only refers to the fact that the output is correct with probability one.

Annex A provides error probabilities that are utilized by the Miller-Rabin primality test.

Annex B describes variants of the methods for generating primes so that particular cryptographic requirements can be met.

Annex C defines primitives utilized by the prime generation and verification methods.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements 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 18031, *Information technology — Security techniques — Random bit generation*