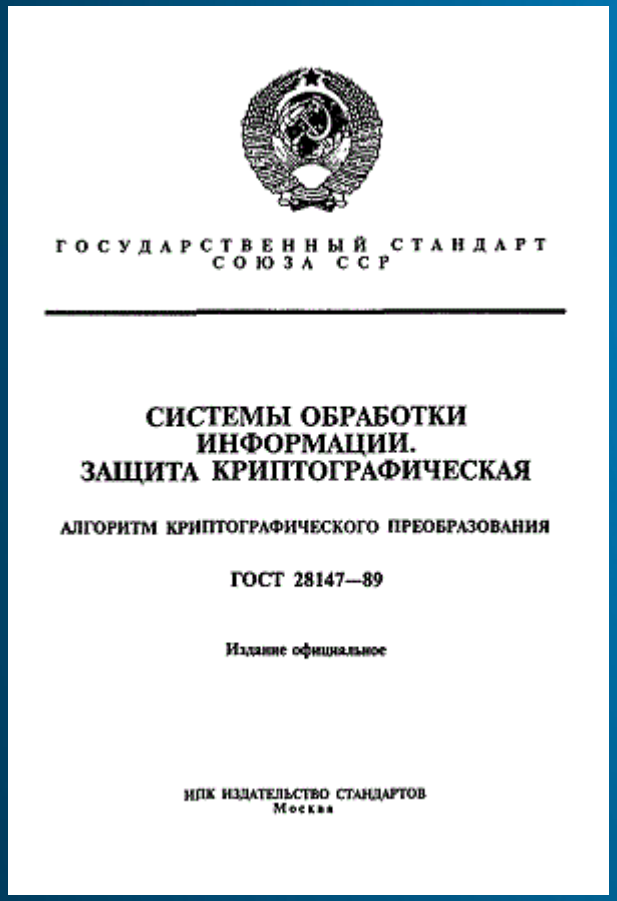
Standardization of cryptographic mechanisms in Russia

Alexander Bondarenko,
Grigory Marshalko
Technical committee for standardization
“Cryptography and security mechanisms”
(TC 26)

Sergei Prokhorov
S.I. Vavilov Institute for the History of Science and Technology of Russian Academy of Sciencis
Moscow Institute of Physics and Technology

GOST 28147-89



ГОСУДАРСТВЕННЫЙ СТАНДАРТ
СОЮЗА ССР

СИСТЕМЫ ОБРАБОТКИ
ИНФОРМАЦИИ.
ЗАЩИТА КРИПТОГРАФИЧЕСКАЯ

АЛГОРИТМ КРИПТОГРАФИЧЕСКОГО ПРЕОБРАЗОВАНИЯ

ГОСТ 28147—89

Издание официальное

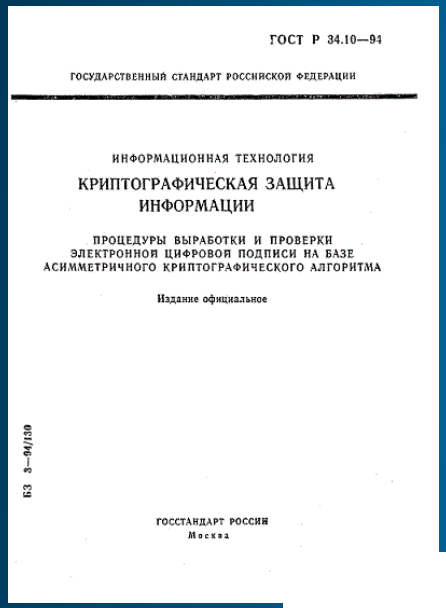
ИПК ИЗДАТЕЛЬСТВО СТАНДАРТОВ
Москва

1989

GOST 28147-89

2020

GOST R 34.10-94/ GOST R 34.11-94



ГОСТ Р 34.10—94

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ИНФОРМАЦИОННАЯ ТЕХНОЛОГИЯ

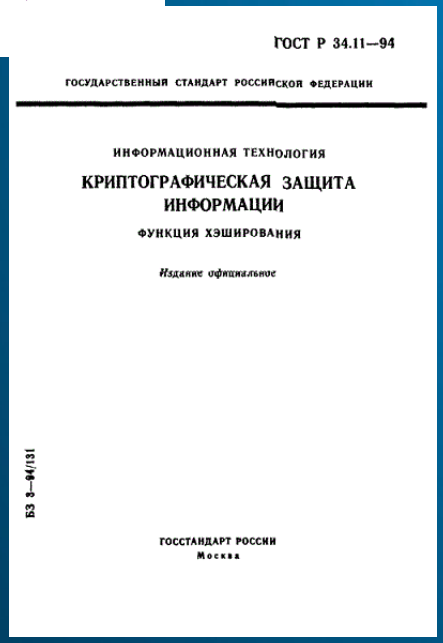
КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

ПРОЦЕДУРЫ ВЫРАБОТКИ И ПРОВЕРКИ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ НА БАЗЕ АСИММЕТРИЧНОГО КРИПТОГРАФИЧЕСКОГО АЛГОРИТМА

Издание официальное

БЗ 3—94/130

ГОССТАНДАРТ РОССИИ
Москва



ГОСТ Р 34.11—94

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ИНФОРМАЦИОННАЯ ТЕХНОЛОГИЯ

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

ФУНКЦИЯ ХЭШИРОВАНИЯ

Издание официальное

БЗ 3—94/131

ГОССТАНДАРТ РОССИИ
Москва

1989

GOST 28147-89

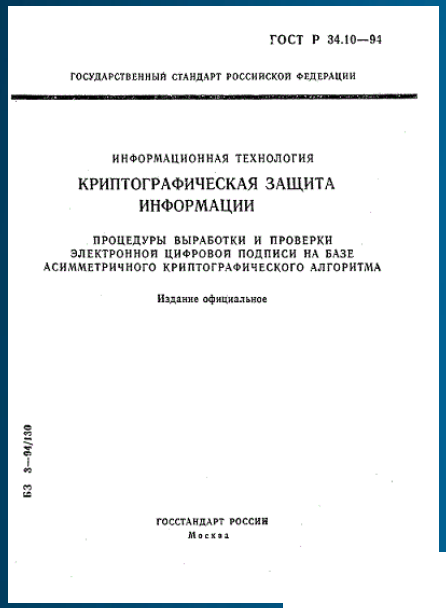
1994

GOST R 34.10-94

GOST R 34.11-94

2020

GOST 34.310-95/ GOST 34.311-95



ГОСТ Р 34.10—94

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ИНФОРМАЦИОННАЯ ТЕХНОЛОГИЯ

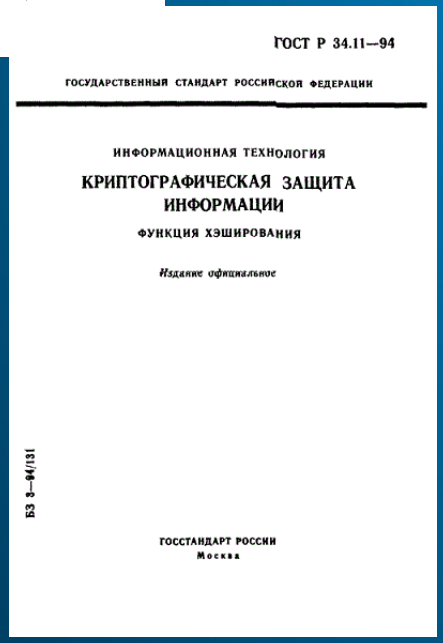
КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

ПРОЦЕДУРЫ ВЫРАБОТКИ И ПРОВЕРКИ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ НА БАЗЕ АСИММЕТРИЧНОГО КРИПТОГРАФИЧЕСКОГО АЛГОРИТМА

Издание официальное

БЗ 3—94/130

ГОССТАНДАРТ РОССИИ
Москва



ГОСТ Р 34.11—94

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ИНФОРМАЦИОННАЯ ТЕХНОЛОГИЯ

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

ФУНКЦИЯ ХЭШИРОВАНИЯ

Издание официальное

БЗ 3—94/131

ГОССТАНДАРТ РОССИИ
Москва

1989

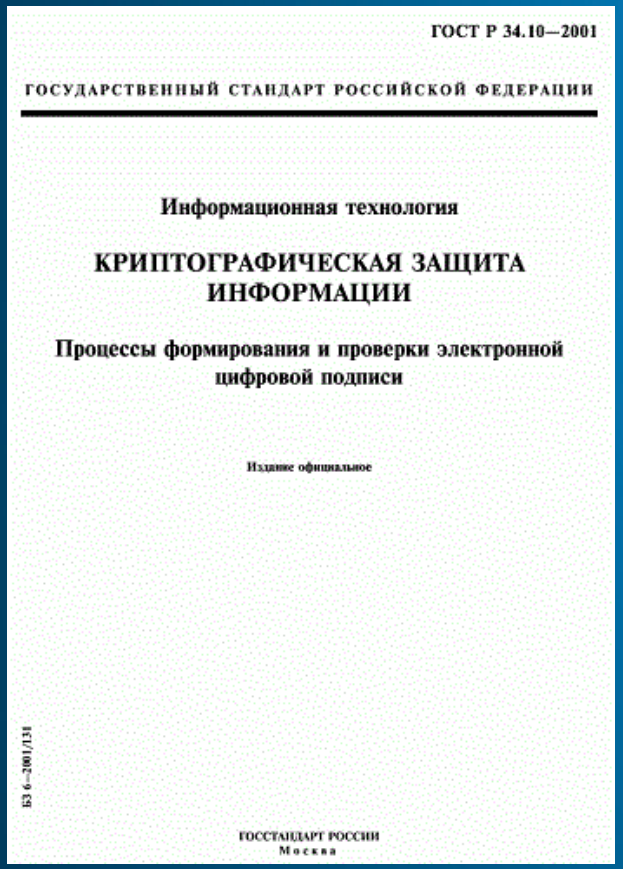
GOST 28147-89

1995

GOST R 34.10-94	GOST R 34.11-94
GOST 34.310-95	GOST 34.311-95

2020

GOST R 34.10-2001



ГОСТ Р 34.10—2001

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Процессы формирования и проверки электронной цифровой подписи

Издание официальное

БЗ 6—2001/131

ГОССТАНДАРТ РОССИИ
Москва

1989

2001

2020

GOST 28147-89

GOST R 34.10-94

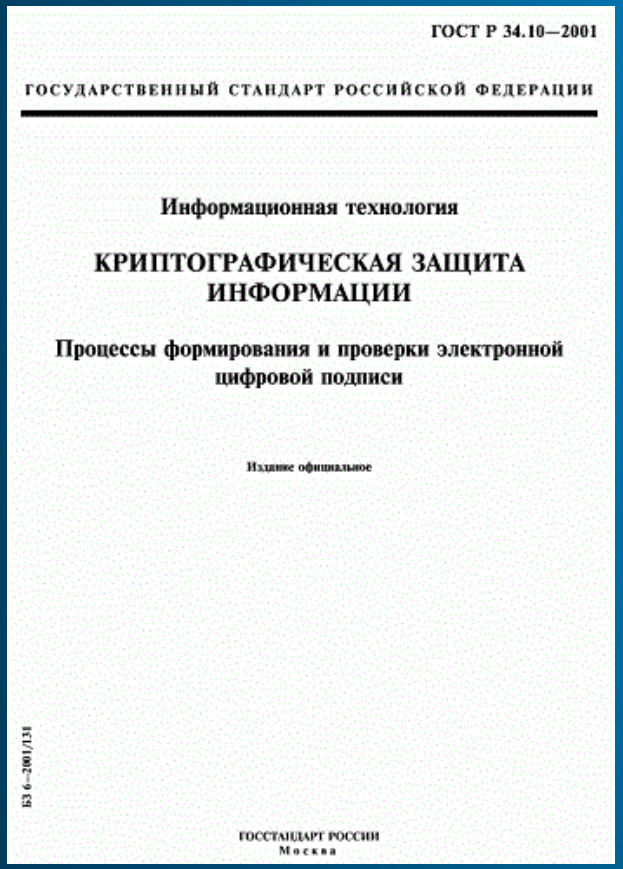
GOST 34.310-95

GOST R 34.11-94

GOST 34.311-95

GOST R 34.10-2001

GOST 34.310-2004



ГОСТ Р 34.10—2001

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Процессы формирования и проверки электронной цифровой подписи

Издание официальное

БЗ 6—2001/131

ГОССТАНДАРТ РОССИИ
Москва

1989

GOST 28147-89

GOST R 34.10-94 / GOST 34.310-95

GOST R 34.11-94 / GOST 34.311-95

2004

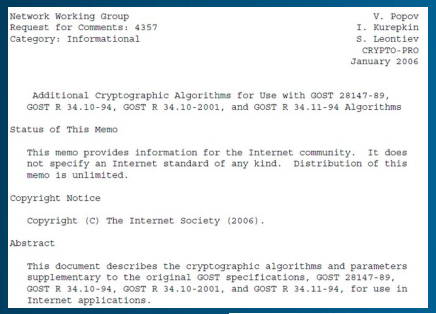
GOST R 34.10-2001 / GOST 34.310-2004

2020

RCF 4357/4490/4491

IETF

IRTF



Network Working Group
Request for Comments: 4357
Category: Informational

V. Popov
I. Kurepkin
S. Leontiev
CRYPTO-PRO
January 2006

Additional Cryptographic Algorithms for Use with GOST 28147-89, GOST R 34.10-94, GOST R 34.10-2001, and GOST R 34.11-94 Algorithms

Status of This Memo

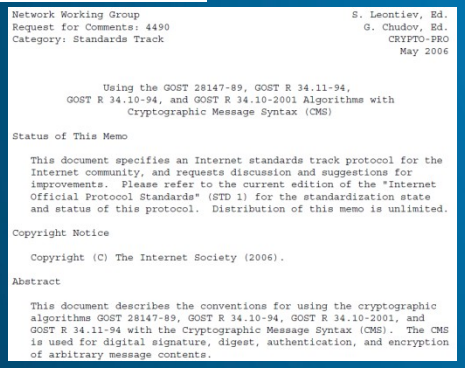
This memo provides information for the Internet community. It does not specify an Internet standard of any kind. Distribution of this memo is unlimited.

Copyright Notice

Copyright (C) The Internet Society (2006).

Abstract

This document describes the cryptographic algorithms and parameters supplementary to the original GOST specifications, GOST 28147-89, GOST R 34.10-94, GOST R 34.10-2001, and GOST R 34.11-94, for use in Internet applications.



Network Working Group
Request for Comments: 4490
Category: Standards Track

S. Leontiev, Ed.
G. Chudov, Ed.
CRYPTO-PRO
May 2006

Using the GOST 28147-89, GOST R 34.11-94, GOST R 34.10-94, and GOST R 34.10-2001 Algorithms with Cryptographic Message Syntax (CMS)

Status of This Memo

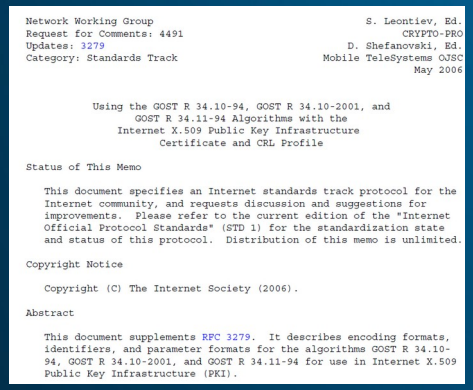
This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "Internet Official Protocol Standards" (STD 1) for the standardization state and status of this protocol. Distribution of this memo is unlimited.

Copyright Notice

Copyright (C) The Internet Society (2006).

Abstract

This document describes the conventions for using the cryptographic algorithms GOST 28147-89, GOST R 34.10-94, GOST R 34.10-2001, and GOST R 34.11-94 with the Cryptographic Message Syntax (CMS). The CMS is used for digital signature, digest, authentication, and encryption of arbitrary message contents.



Network Working Group
Request for Comments: 4491
Updates: 3279
Category: Standards Track

S. Leontiev, Ed.
CRYPTO-PRO
D. Shefanovski, Ed.
Mobile TeleSystems OJSC
May 2006

Using the GOST R 34.10-94, GOST R 34.10-2001, and GOST R 34.11-94 Algorithms with the Internet X.509 Public Key Infrastructure Certificate and CRL Profile

Status of This Memo

This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "Internet Official Protocol Standards" (STD 1) for the standardization state and status of this protocol. Distribution of this memo is unlimited.

Copyright Notice

Copyright (C) The Internet Society (2006).

Abstract

This document supplements RFC 3279. It describes encoding formats, identifiers, and parameter formats for the algorithms GOST R 34.10-94, GOST R 34.10-2001, and GOST R 34.11-94 for use in Internet X.509 Public Key Infrastructure (PKI).

1989

2006

2020

GOST 28147-89

GOST R 34.10-94

GOST 34.310-95

GOST R 34.11-94

GOST 34.311-95

GOST R 34.10-2001

GOST 34.310-2004

RFC 5830/5831/5832

IETF

IRTF

Independent Submission
Request for Comments: 5830
Category: Informational
ISSN: 2070-1721

V. Dolmatov, Ed.
Cryptocom, Ltd.
March 2010

GOST 28147-89: Encryption, Decryption, and Message Authentication Code (MAC) Algorithms

Abstract

This document is intended to be a source of information about the Russian Federal standard for electronic encryption, decryption, and message authentication algorithms (GOST 28147-89), which is one of the Russian cryptographic standard algorithms called GOST algorithms). Recently, Russian cryptography is being used in Internet applications, and this document has been created as information for developers and users of GOST 28147-89 for encryption, decryption, and message authentication.

Independent Submission
Request for Comments: 5831
Category: Informational
ISSN: 2070-1721

V. Dolmatov, Ed.
Cryptocom, Ltd.
March 2010

GOST R 34.11-94: Hash Function Algorithm

Abstract

This document is intended to be a source of information about the Russian Federal standard hash function (GOST R 34.11-94), which is one of the Russian cryptographic standard algorithms (called GOST algorithms). Recently, Russian cryptography is being used in Internet applications, and this document has been created as information for developers and users of GOST R 34.11-94 for hash computation.

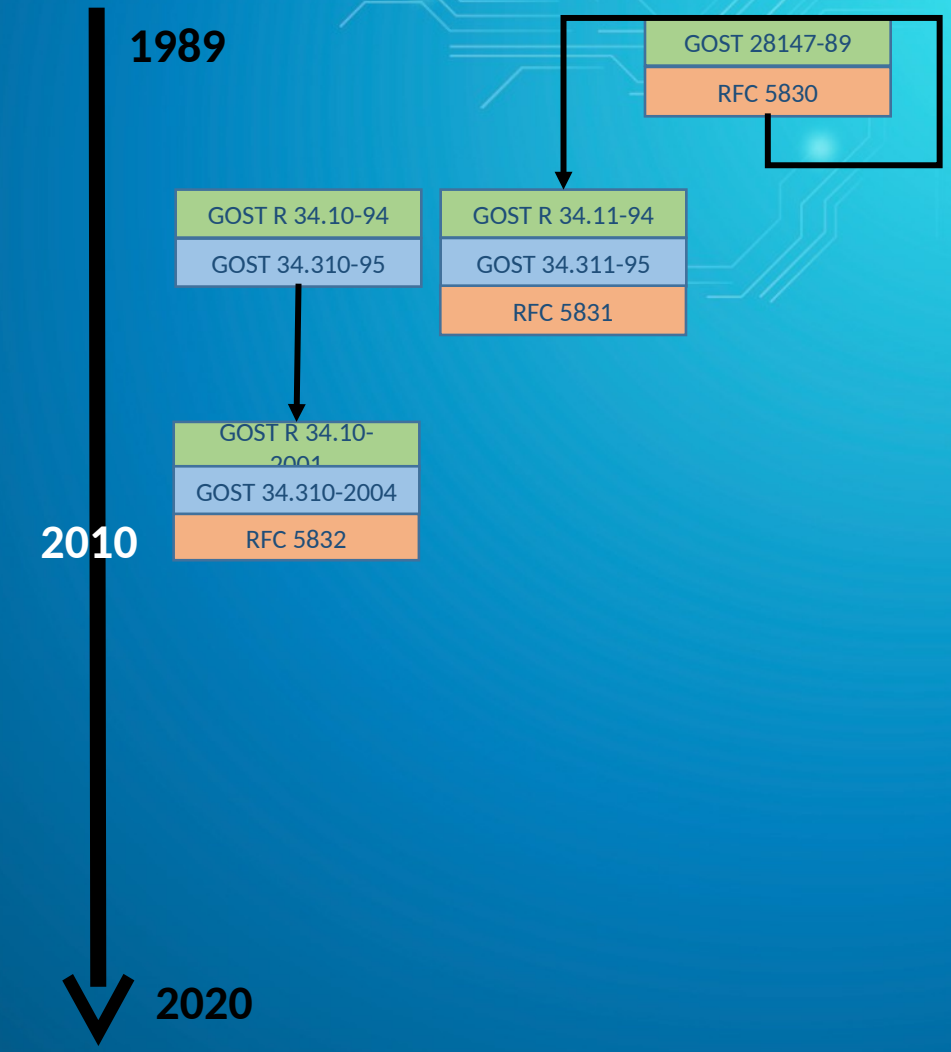
Independent Submission
Request for Comments: 5832
Category: Informational
ISSN: 2070-1721

V. Dolmatov, Ed.
Cryptocom, Ltd.
March 2010

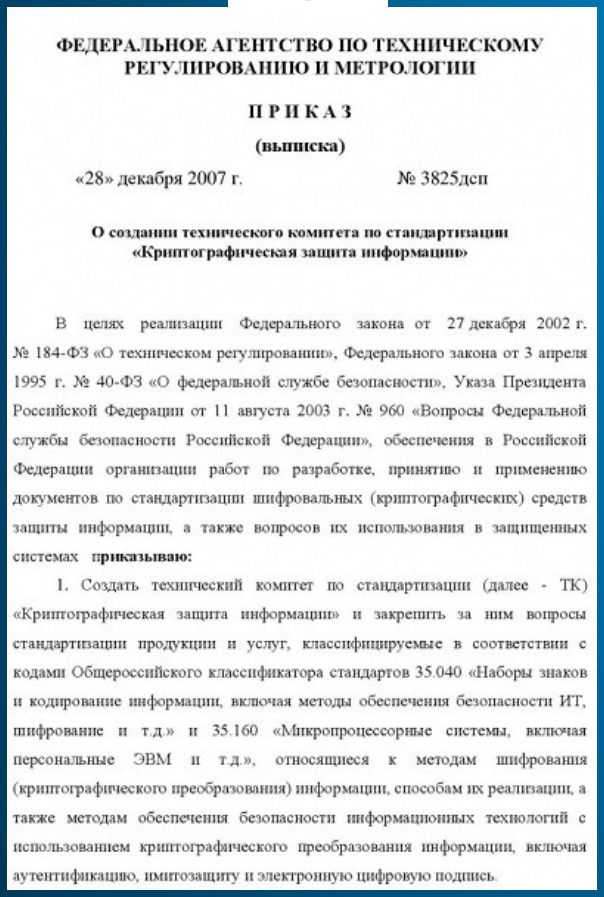
GOST R 34.10-2001: Digital Signature Algorithm

Abstract

This document is intended to be a source of information about the Russian Federal standard for digital signatures (GOST R 34.10-2001), which is one of the Russian cryptographic standard algorithms (called GOST algorithms). Recently, Russian cryptography is being used in Internet applications, and this document has been created as information for developers and users of GOST R 34.10-2001 for digital signature generation and verification.



Technical committee for standardization “Cryptography and security mechanisms” (TC 26)



ФЕДЕРАЛЬНОЕ АГЕНТСТВО ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

П Р И К А З

(выписка)

«28» декабря 2007 г. № 3825дсп

О создании технического комитета по стандартизации «Криптографическая защита информации»

В целях реализации Федерального закона от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании», Федерального закона от 3 апреля 1995 г. № 40-ФЗ «О федеральной службе безопасности», Указа Президента Российской Федерации от 11 августа 2003 г. № 960 «Вопросы Федеральной службы безопасности Российской Федерации», обеспечения в Российской Федерации организации работ по разработке, принятию и применению документов по стандартизации шифровальных (криптографических) средств защиты информации, а также вопросов их использования в защищенных системах **приказываю:**

1. Создать технический комитет по стандартизации (далее - ТК) «Криптографическая защита информации» и закрепить за ним вопросы стандартизации продукции и услуг, классифицируемые в соответствии с кодами Общероссийского классификатора стандартов 35.040 «Наборы знаков и кодирование информации, включая методы обеспечения безопасности ИТ, шифрование и т.д.» и 35.160 «Микропроцессорные системы, включая персональные ЭВМ и т.д.», относящиеся к методам шифрования (криптографического преобразования) информации, способам их реализации, а также методам обеспечения безопасности информационных технологий с использованием криптографического преобразования информации, включая аутентификацию, имитозащиту и электронную цифровую подпись.

1989

GOST 28147-89

RFC 5830

GOST R 34.10-94

GOST 34.310-95

GOST R 34.11-94

GOST 34.311-95

RFC 5831

2010

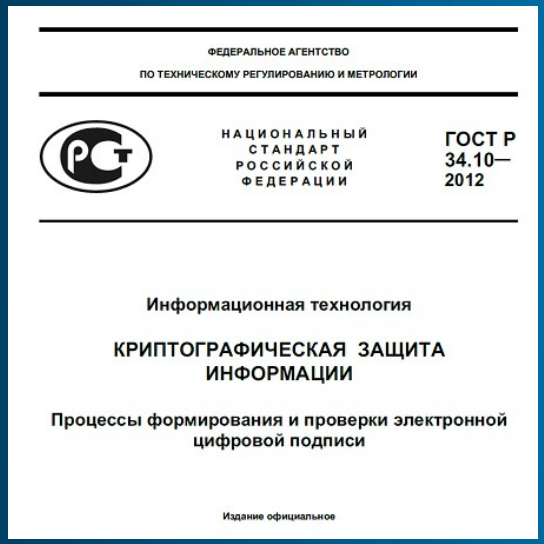
GOST R 34.10-2001

GOST 34.310-2004

RFC 5832

2020

GOST R 34.10-2012/ GOST R 34.11-2012



ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

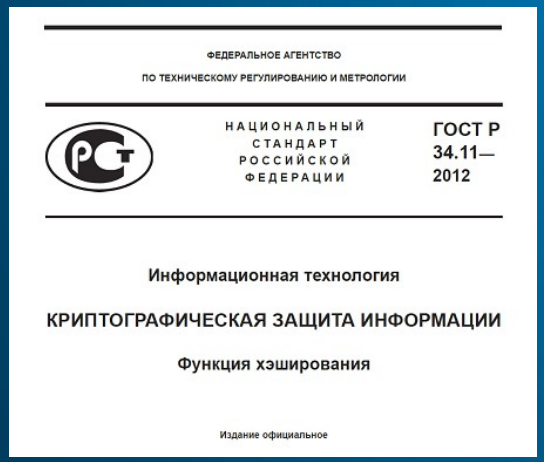
ГОСТ Р 34.10— 2012

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Процессы формирования и проверки электронной цифровой подписи

Издание официальное



ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

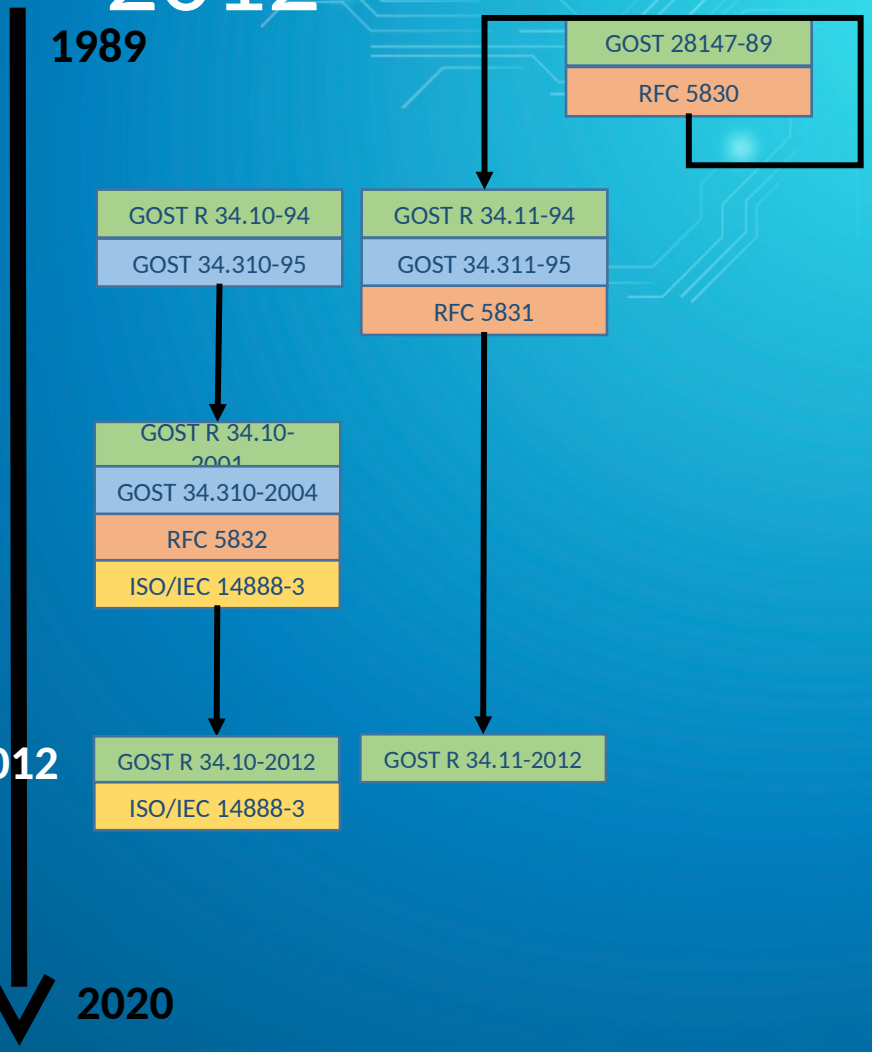
ГОСТ Р 34.11— 2012

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Функция хэширования

Издание официальное



GOST R 34.12-2015/ GOST R 34.13-2015

ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

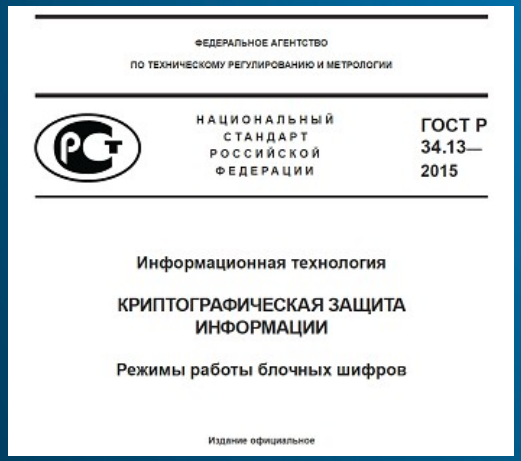
ГОСТ Р 34.12— 2015

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Блочные шифры

Издание официальное



ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

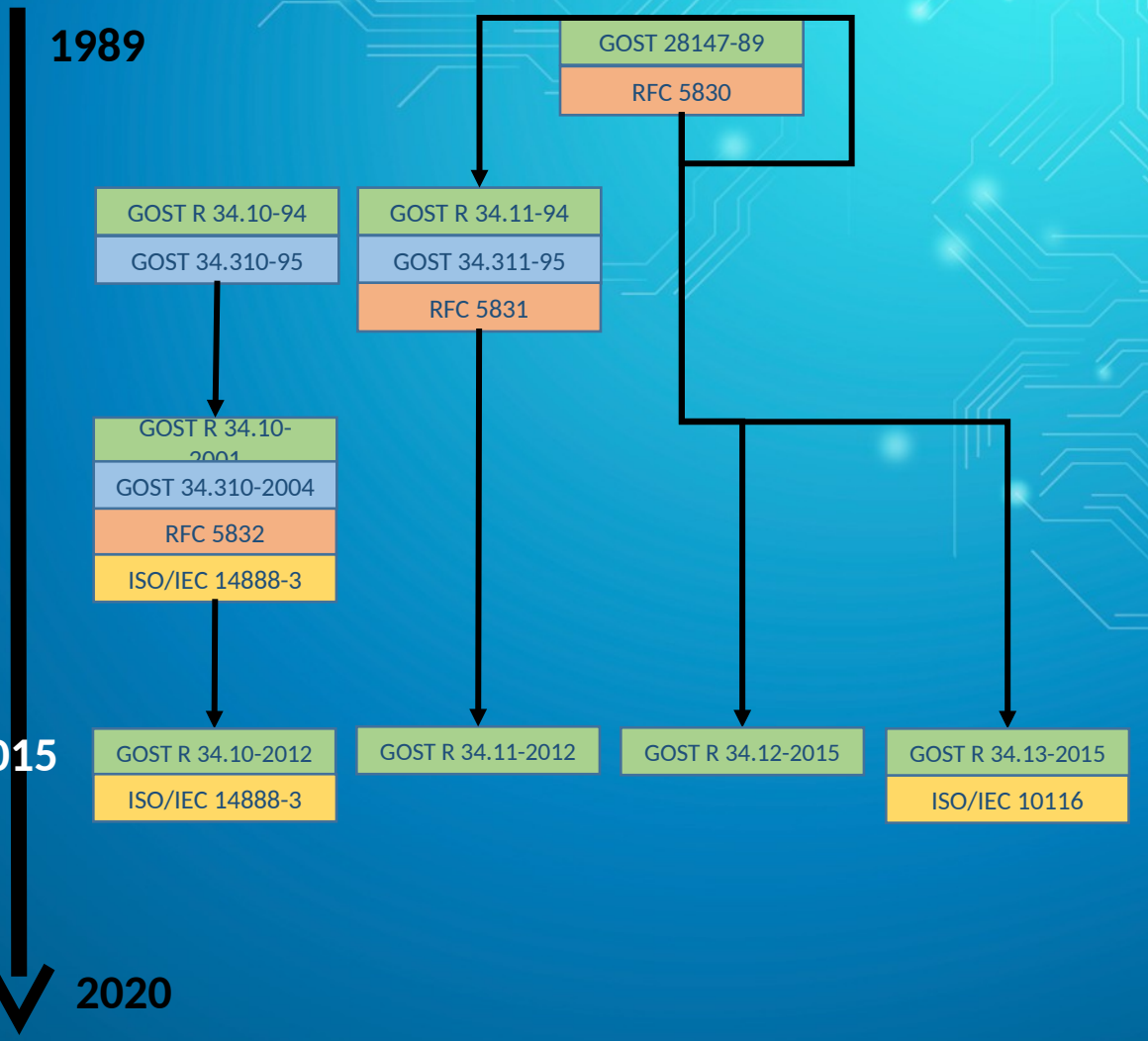
ГОСТ Р 34.13— 2015

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Режимы работы блочных шифров

Издание официальное



RFC 6986/7091/7801

IETF IRTF

Independent Submission
Request for Comments: 6986
Updates: 5831
Category: Informational
ISSN: 2070-1721

V. Dolmatov, Ed.
A. Degtyarev
Cryptocom, Ltd.
August 2013

GOST R 34.11-2012: Hash Function

Abstract

This document is intended to be a source of information about the Russian Federal standard hash function (GOST R 34.11-2012), which is one of the Russian cryptographic standard algorithms (called GOST algorithms). This document updates RFC 5831.

Independent Submission
Request for Comments: 7091
Updates: 5832
Category: Informational
ISSN: 2070-1721

V. Dolmatov, Ed.
A. Degtyarev
Cryptocom, Ltd.
December 2013

GOST R 34.10-2012: Digital Signature Algorithm

Abstract

This document provides information about the Russian Federal standard for digital signatures (GOST R 34.10-2012), which is one of the Russian cryptographic standard algorithms (called GOST algorithms). Recently, Russian cryptography is being used in Internet applications, and this document provides information for developers and users of GOST R 34.10-2012 regarding digital signature generation and verification. This document updates RFC 5832.

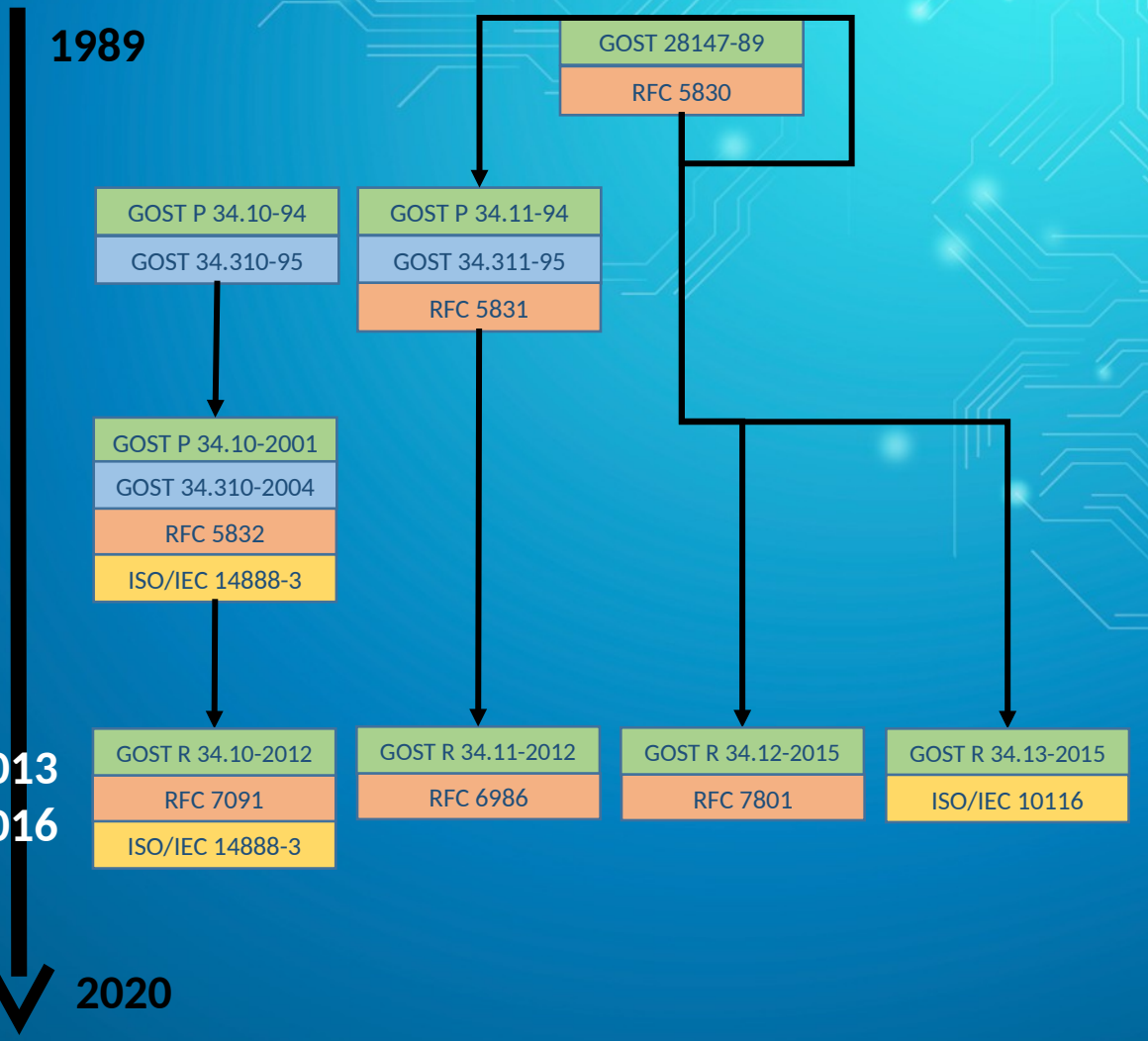
Independent Submission
Request for Comments: 7801
Category: Informational
ISSN: 2070-1721

V. Dolmatov, Ed.
Research Computer Center MSU
March 2016

GOST R 34.12-2015: Block Cipher "Kuznyechik"

Abstract

This document is intended to be a source of information about the Russian Federal standard GOST R 34.12-2015 describing the block cipher with a block length of n=128 bits and a key length of k=256 bits, which is also referred to as "Kuznyechik". This algorithm is one of the set of Russian cryptographic standard algorithms (called GOST algorithms).



GOST 34.10-2018/ GOST 34.11-2018
GOST 34.12-2018/ GOST 34.13-2018

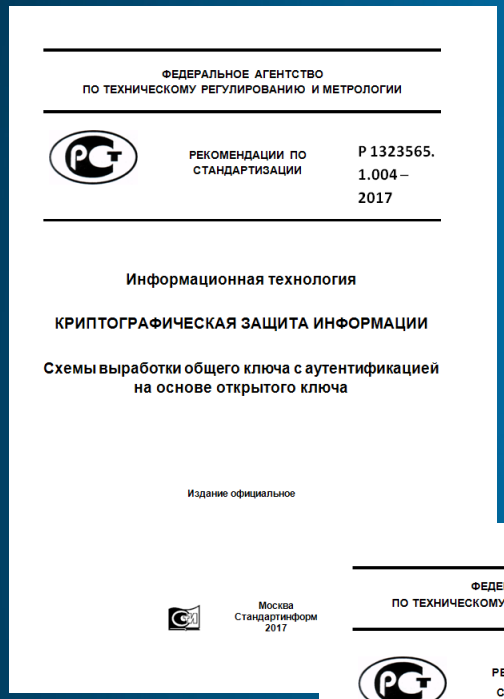
1989

2018

2020

- GOST 28147-89
  - RFC 5830
- GOST R 34.10-94
  - GOST 34.310-95
  - GOST R 34.10-2001
    - GOST 34.310-2004
    - RFC 5832
    - ISO/IEC 14888-3
    - GOST R 34.10-2012
      - GOST 34.10-2018
      - RFC 7091
      - ISO/IEC 14888-3
- GOST R 34.11-94
  - GOST 34.311-95
  - RFC 5831
  - GOST R 34.11-2012
    - GOST 34.11-2018
    - RFC 6986
    - ISO/IEC 10118-3
- GOST R 34.12-2015
  - GOST 34.12-2018
  - RFC 7801
- GOST R 34.13-2015
  - GOST 34.13-2018
  - ISO/IEC 10116

Recommendations for standardization



ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ

Р 1323565.1.004 – 2017

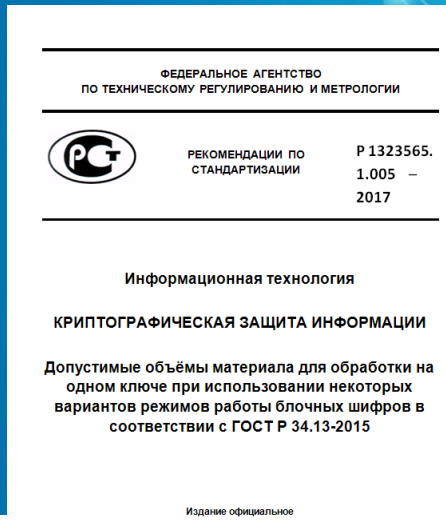
Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Схемы выработки общего ключа с аутентификацией на основе открытого ключа

Издание официальное

Москва
Стандартинформ
2017



ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ

Р 1323565.1.005 – 2017

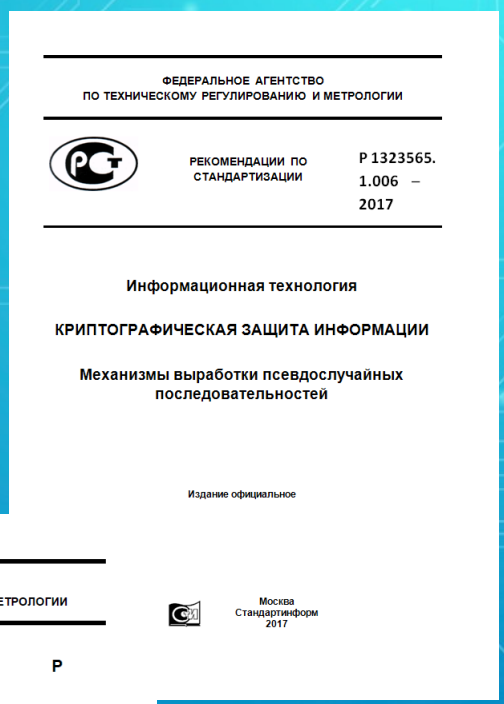
Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Допустимые объёмы материала для обработки на одном ключе при использовании некоторых вариантов режимов работы блочных шифров в соответствии с ГОСТ Р 34.13-2015

Издание официальное

Москва
Стандартинформ
2017



ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ

Р 1323565.1.006 – 2017

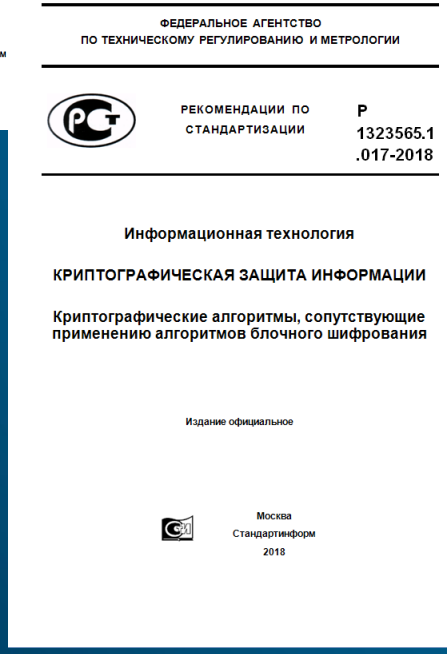
Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Механизмы выработки псевдослучайных последовательностей

Издание официальное

Москва
Стандартинформ
2017



ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ

Р 1323565.1.017-2018

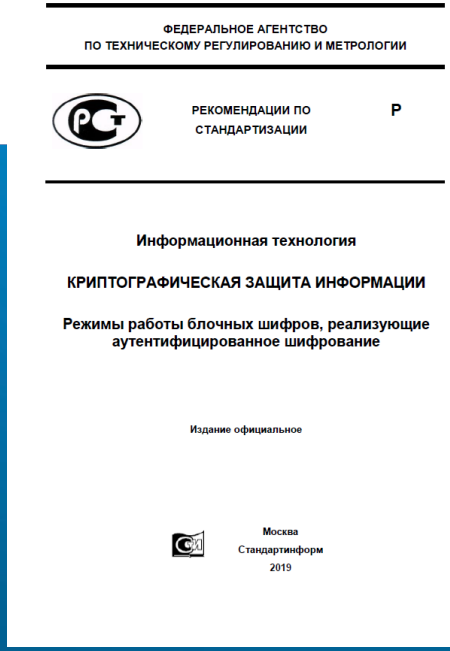
Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Криптографические алгоритмы, сопутствующие применению алгоритмов блочного шифрования

Издание официальное

Москва
Стандартинформ
2018



ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ

Р

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Режимы работы блочных шифров, реализующие аутентифицированное шифрование

Издание официальное

Москва
Стандартинформ
2019

Recommendations for standardization

GOST R 34.10-2012

GOST R 34.11-2012

GOST R 34.12-2015

GOST R 34.13-2015