

ГОСТ Р 34.12-2015 - Блочный шифр «Кузнечик» GOST R 34.12-2015: Block Cipher "Kuznyechik"

Аннотация

Этот документ публикуется в качестве источника информации о Национальном стандарте Российской Федерации ГОСТ Р 34.12-2015, описывающем блочное шифрование с размером блока $n=128$ битов и размером ключа $k=256$ битов, называемого также «Кузнечик». Данный алгоритм является одним из множества российских стандартных криптографических алгоритмов (алгоритмы ГОСТ).

Статус документа

Документ не является спецификацией стандарта Internet и публикуется с информационными целями.

Документ включается в серию RFC, но не связан с каким-либо потоком документов RFC. Редактор (RFC Editor) принял решение о публикации документа по своему усмотрению и не делает каких-либо заявления о реализации или развёртывании. Документы, одобренные для публикации их редакторами не претендуют на какой-либо уровень стандартизации Internet (см. раздел 2 в RFC 5741).

Информацию о текущем статусе документа, ошибках и способах обратной связи можно найти по ссылке <http://www.rfc-editor.org/info/rfc7801>.

Авторские права

Авторские права (Copyright (c) 2016) принадлежат IETF Trust и лицам, указанным в качестве авторов документа. Все права защищены.

К этому документу применимы права и ограничения, перечисленные в BCP 78 и IETF Trust Legal Provisions и относящиеся к документам IETF (<http://trustee.ietf.org/license-info>), на момент публикации данного документа. Прочтите упомянутые документы внимательно.

Оглавление

1. Сфера действия стандарта.....	1
2. Общие сведения.....	2
3. Определения и обозначения.....	2
3.1. Определения.....	2
3.2. Обозначения.....	2
4. Значения параметров.....	3
4.1. Нелинейное взаимно-однозначное преобразование.....	3
4.2. Линейное преобразование.....	4
4.3. Преобразования.....	4
4.4. Развёртывание ключа.....	4
4.5. Базовый алгоритм шифрования.....	4
4.5.1. Шифрование.....	4
4.5.2. Дешифрование.....	4
5. Примеры (для информации).....	4
5.1. Преобразование S.....	4
5.2. Преобразование R.....	5
5.3. Преобразование L.....	5
5.4. Развёртывание ключа.....	5
5.5. Тестовое шифрование.....	5
5.6. Тестовая расшифровка.....	6
6. Вопросы безопасности.....	6
7. Литература.....	6
7.1. Нормативные документы.....	6
7.2. Дополнительная литература.....	6
Адрес автора.....	6

1. Сфера действия стандарта

Национальный стандарт Российской Федерации [GOST3412-2015] описывает базовые блочные шифры, используемые в качестве криптографических методов обработки и защиты информации, включая защиту конфиденциальности, достоверности и целостности информации при её передаче, обработке и хранении в компьютерных системах.

Криптографические алгоритмы, описанные в этом стандарте, предназначены как для программно, так и для аппаратной реализации. Они соответствуют современным криптографическим требованиям и не накладывают никаких ограничений на уровень конфиденциальности защищаемой информации.

2. Общие сведения

Блочный шифр «Кузнечик» [GOST3412-2015] Разработан Центром защиты информации и специальной связи Федеральной службы безопасности Российской Федерации с участием ОАО «Инфотекс» («Информационные Технологии и Коммуникационные Системы» - InfoTeCS JSC). Стандарт ГОСТ Р 34.12-2015 одобрен и введён в действие Приказом №749-ст Федерального агентства по техническому регулированию и метрологии от 19 июня 2015 г.

Терминологически и концептуально стандарт согласован с международными стандартами:

- ISO/IEC 10116 [ISO-IEC10116];
- серия стандартов ISO/IEC 18033 [ISO-IEC18033-1] [ISO-IEC18033-3].

3. Определения и обозначения

Ниже приведены используемые в стандарте термины и их определения.

3.1. Определения

Ниже приведены определения используемых в стандарте терминов.

encryption algorithm - алгоритм шифрования

Процесс, преобразующий открытый текст в зашифрованный (параграф 2.19 [ISO-IEC18033-1]).

decryption algorithm - алгоритм дешифрования

Процесс, преобразующий зашифрованный текст в открытый (параграф 2.14 [ISO-IEC18033-1]).

basic block cipher - базовый блочный шифр

Блочный шифр, в котором для данного ключа выполняется однократное обратимое отображение набора блоков открытого текста с фиксированным размером в блоки шифрованного текста с таким же размером.

block - блок

Строка битов определённого размера (параграф 2.6 [ISO-IEC18033-1])

block cipher – блочный шифр

Симметричная система шифрования, в которой алгоритм применяется к блокам открытого текста (строкам битов определённого размера) для получения блоков шифрованного текста (параграф 2.7 [ISO-IEC18033-1]).

Примечание. В ГОСТ Р 34.12-2015 установлено, что термины «блочный шифр» (block cipher) и «алгоритм блочного шифрования» (block encryption algorithm) являются синонимами.

encryption - шифрование

Обратимое преобразование данных с помощью криптографического алгоритма для создания шифрованного текста, т. е., сокрытия содержимого этих данных (параграф 2.18 [ISO-IEC18033-1]).

round key - итерационный ключ

Последовательность символов, рассчитываемая в процессе развёртывания ключа и определяющая преобразование в рамках одной итерации (round) блочного шифрования.

key - ключ

Последовательность символов, определяющая криптографическое преобразование (например, шифрование или дешифрование) (параграф 2.21 [ISO-IEC18033-1]).

Примечание. В ГОСТ Р 34.12-2015 ключ должен быть двоичной последовательностью.

plaintext - открытый текст

Незашифрованная информация (параграф 3.11 [ISO-IEC10116]).

key schedule - развёртывание ключа

Расчёт итерационного ключа на основе ключа шифра.

decryption - дешифрование

Операция, обратная шифрованию (параграф 2.13 [ISO-IEC18033-1]).

symmetric cryptographic technique - симметричный криптографический метод

Криптографический метод, в котором используется один и тот же секретный ключ как для шифрования, так и для дешифрования (параграф 2.32 [ISO-IEC18033-1]).

cipher - шифр

Другой термин, используемый для обозначения криптографической системы (параграф 2.20 [ISO-IEC18033-1]).

ciphertext - шифрованный текст

Данные, которые были преобразованы с целью сокрытия их содержимого (параграф 3.3 [ISO-IEC10116]).

3.2. Обозначения

Ниже приводятся используемые в стандарте обозначения.

V^*

множество всех двоичных строк конечного размера (далее, строк), включая пустую строку.

V_s

множество всех двоичных строк размера s , где s - неотрицательное целое число; нумерация подстрок и компонент строки осуществляется справа налево, начиная с 0.

$U \times W$

прямое (декартово) произведение множеств U и W .

$|A|$

число компонент (размер) строки A из множества V^* (если A - пустая строка, $|A| = 0$).

$A||B$

конкатенация строки A и B из множества V^* , т.е., строка из $V_{-(|A|+|B|)}$, где левая подстрока из $V_{-|A|}$ равна A , а правая подстрока из $V_{-|B|}$ равна B .

$Z_{(2^n)}$

кольцо вычетов по модулю 2^n ,

Q

конечное поле $GF(2)[x]/p(x)$, где $p(x)=x^8+x^7+x^6+x+1$ принадлежит $GF(2)[x]$; элементы поля Q представлены целыми числами так, что элемент $z_0+z_1\theta+\dots+z_7\theta^7$, принадлежащий Q, соответствует целому числу $z_0+2^1z_1+\dots+2^7z_7$, где $z_i=0$ или $z_i=1$, $i=0,1,\dots,7$, а θ означает класс вычетов по модулю $p(x)$, содержащий x .

(xor)

исключающее ИЛИ для двух двоичных строк одинаковых размеров.

Vec_s: $Z_{(2^s)} \rightarrow V_s$

взаимно-однозначное¹ отображение, сопоставляющее элемент из кольца $Z_{(2^s)}$ с его двоичным представлением; т.е., для любого элемента z в кольце $Z_{(2^s)}$, представленного в виде $z_0 + (2^1z_1) + \dots + (2^{s-1}z_{s-1})$, где z_i принадлежит $\{0, 1\}$, $i = 0, \dots, s-1$, справедливо равенство $Vec_s(z) = z_{s-1}||\dots||z_1||z_0$.

Int_s: $V_s \rightarrow Z_{(2^s)}$

отображение, обратное по отношению к Vec_s (т.е., $Int_s = Vec_s^{-1}$).

delta: $V_8 \rightarrow Q$

взаимно-однозначное отображение, сопоставляющее двоичную строку из V_8 с элементом из поля Q следующим образом - строке $z_7||\dots||z_1||z_0$, где z_i принадлежит $\{0, 1\}$, $i = 0, \dots, 7$, соответствует элемент $z_0+(z_1\theta)+\dots+(z_7\theta^7)$, принадлежащий Q^2 .

nabla: $Q \rightarrow V_8$

отображение, обратное по отношению к delta, т.е., $delta = nabla^{-1}$.

PS

композиция отображений, в которой отображение S выполняется первым.

P^s

композиция отображений P^{s-1} и P, где $P^1=P$.

4. Значения параметров

4.1. Нелинейное взаимно-однозначное преобразование

Нелинейное взаимно-однозначное преобразование представляет собой подстановку $P_i = (Vec_8)P_i'(Int_8): V_8 \rightarrow V_8$, где $P_i': Z_{(2^8)} \rightarrow Z_{(2^8)}$. Значения для подстановки P_i' приведены ниже в форме массива $P_i' = (P_i'(0), P_i'(1), \dots, P_i'(255))$:

```
Pi' =
( 252, 238, 221, 17, 207, 110, 49, 22, 251, 196, 250,
  218, 35, 197, 4, 77, 233, 119, 240, 219, 147, 46,
  153, 186, 23, 54, 241, 187, 20, 205, 95, 193, 249,
    24, 101, 90, 226, 92, 239, 33, 129, 28, 60, 66,
  139, 1, 142, 79, 5, 132, 2, 174, 227, 106, 143,
  160, 6, 11, 237, 152, 127, 212, 211, 31, 235, 52,
  44, 81, 234, 200, 72, 171, 242, 42, 104, 162, 253,
  58, 206, 204, 181, 112, 14, 86, 8, 12, 118, 18,
  191, 114, 19, 71, 156, 183, 93, 135, 21, 161, 150,
  41, 16, 123, 154, 199, 243, 145, 120, 111, 157, 158,
  178, 177, 50, 117, 25, 61, 255, 53, 138, 126, 109,
  84, 198, 128, 195, 189, 13, 87, 223, 245, 36, 169,
  62, 168, 67, 201, 215, 121, 214, 246, 124, 34, 185,
    3, 224, 15, 236, 222, 122, 148, 176, 188, 220, 232,
  40, 80, 78, 51, 10, 74, 167, 151, 96, 115, 30,
    0, 98, 68, 26, 184, 56, 130, 100, 159, 38, 65,
  173, 69, 70, 146, 39, 94, 85, 47, 140, 163, 165,
  125, 105, 213, 149, 59, 7, 88, 179, 64, 134, 172,
  29, 247, 48, 55, 107, 228, 136, 217, 231, 137, 225,
  27, 131, 73, 76, 63, 248, 254, 141, 83, 170, 144,
  202, 216, 133, 97, 32, 113, 103, 164, 45, 43, 9,
  91, 203, 155, 37, 208, 190, 229, 108, 82, 89, 166,
  116, 210, 230, 244, 180, 192, 209, 102, 175, 194, 57,
    75, 99, 182)
```

P_i^{-1} представляет собой значение, обратное P_i ($1/P_i$); значения для подстановки P_i^{-1} приведены ниже в форме массива $P_i^{-1} = (P_i^{-1}(0), P_i^{-1}(1), \dots, P_i^{-1}(255))$:

```
Pi^-1 =
( 165, 45, 50, 143, 14, 48, 56, 192, 84, 230, 158,
  57, 85, 126, 82, 145, 100, 3, 87, 90, 28, 96,
    7, 24, 33, 114, 168, 209, 41, 198, 164, 63, 224,
  39, 141, 12, 130, 234, 174, 180, 154, 99, 73, 229,
  66, 228, 21, 183, 200, 6, 112, 157, 65, 117, 25,
  201, 170, 252, 77, 191, 42, 115, 132, 213, 195, 175,
  43, 134, 167, 177, 178, 91, 70, 211, 159, 253, 212,
  15, 156, 47, 155, 67, 239, 217, 121, 182, 83, 127,
  193, 240, 35, 231, 37, 94, 181, 30, 162, 223, 166,
  254, 172, 34, 249, 226, 74, 188, 53, 202, 238, 120,
    5, 107, 81, 225, 89, 163, 242, 113, 86, 17, 106,
  137, 148, 101, 140, 187, 119, 60, 123, 40, 171, 210,
    49, 222, 196, 95, 204, 207, 118, 44, 184, 216, 46,
    54, 219, 105, 179, 20, 149, 190, 98, 161, 59, 22,
  102, 233, 92, 108, 109, 173, 55, 97, 75, 185, 227,
  186, 241, 160, 133, 131, 218, 71, 197, 176, 51, 250,
  150, 111, 110, 194, 246, 80, 255, 93, 169, 142, 23,
    27, 151, 125, 236, 88, 247, 31, 251, 124, 9, 13,
  122, 103, 69, 135, 220, 232, 79, 29, 78, 4, 235,
  248, 243, 62, 61, 189, 138, 136, 221, 205, 11, 19,
  152, 2, 147, 128, 144, 208, 36, 52, 203, 237, 244,
  206, 153, 16, 68, 64, 146, 58, 1, 38, 18, 26,
```

¹Используется также термин «биективное». Прим. перев.

²В исходном документе ошибочно сказано «Z». См. [RFC Errata](#). Прим. перев.

4.2. Линейное преобразование

Линейное преобразование обозначается $l: (V_8)^{16} \rightarrow V_8$ и определяется выражением

$$l(a_{15}, \dots, a_0) = \text{nabla}(148 \cdot \delta(a_{15}) + 32 \cdot \delta(a_{15}) + 133 \cdot \delta(a_{13}) + 16 \cdot \delta(a_{12}) + 194 \cdot \delta(a_{11}) + 192 \cdot \delta(a_{10}) + 1 \cdot \delta(a_9) + 251 \cdot \delta(a_8) + 1 \cdot \delta(a_7) + 192 \cdot \delta(a_6) + 194 \cdot \delta(a_5) + 16 \cdot \delta(a_4) + 133 \cdot \delta(a_3) + 32 \cdot \delta(a_2) + 148 \cdot \delta(a_1) + 1 \cdot \delta(a_0))$$

для всех a_i , принадлежащих V_8 , $i = 0, 1, \dots, 15$, где операции сложения и умножения выполняются в поле Q , а постоянные являются элементами поля, как указано выше.

4.3. Преобразования

Для реализации алгоритмов шифрования и дешифрования используются следующие преобразования:

$x[x]: V_{128} \rightarrow V_{128}$ $x[k](a) = k(\text{xor}) a$
где k принадлежит V_{128} ,

$s: V_{128} \rightarrow V_{128}$ $s(a) = (a_{15} || \dots || a_0) = \text{pi}(a_{15}) || \dots || \text{pi}(a_0)$
где $a_{15} || \dots || a_0$ принадлежит V_{128} , a_i принадлежит V_8 , $i = 0, 1, \dots, 15$,

$s^{-1}: V_{128} \rightarrow V_{128}$
значение, обратное по отношению к результату преобразования S , которое можно выполнить, как показано ниже

$s^{-1}(a_{15} || \dots || a_0) = \text{pi}^{-1}(a_{15}) || \dots || \text{pi}^{-1}(a_0)$
где $a_{15} || \dots || a_0$ принадлежит V_{128} , a_i принадлежит V_8 , $i = 0, 1, \dots, 15$,

$r: V_{128} \rightarrow V_{128}$ $r(a_{15} || \dots || a_0) = l(a_{15}, \dots, a_0) || a_{15} || \dots || a_1$
где $a_{15} || \dots || a_0$ принадлежит V_{128} , a_i принадлежит V_8 , $i = 0, 1, \dots, 15$,

$l: V_{128} \rightarrow V_{128}$ $l(a) = R^{16}(a)$
где a принадлежит V_{128} ,

$r^{-1}: V_{128} \rightarrow V_{128}$
значение, обратное по отношению к результату преобразования R , которое можно выполнить, как показано ниже

$r^{-1}(a_{15} || \dots || a_0) = a_{14} || a_{13} || \dots || a_0 || l(a_{14}, a_{13}, \dots, a_0, a_{15})$
где $a_{15} || \dots || a_0$ принадлежит V_{128} , a_i принадлежит V_8 , $i = 0, 1, \dots, 15$,

$l^{-1}: V_{128} \rightarrow V_{128}$ $l^{-1}(a) = (R^{-1})(a)$
где a принадлежит V_{128} ,

$f[k]: V_{128}[*]V_{128} \rightarrow V_{128}[*]V_{128}$ $f[k](a_1, a_0) = (LSX[k](a_1) (\text{xor}) a_0, a_1)$
где k, a_0, a_1 принадлежат V_{128} .

4.4. Развёртывание ключа

При развёртывании ключа используются итерационные константы C_i принадлежащие V_{128} , $i = 1, 2, \dots, 32$, и определяемые, как

$$C_i = l(\text{Vec}_{128}(i))$$

Итерационные ключи (Round key) K_i , $i = 1, 2, \dots, 10$ создаются на основе ключа $K = k_{255} || \dots || k_0$ принадлежащего V_{256} , k_i принадлежащих V_1 , $i = 0, 1, \dots, 255$, как показано ниже

$$K_1 = k_{255} || \dots || k_{128}$$

$$K_2 = k_{127} || \dots || k_0$$

$$(K_{(2i+1)}, K_{(2i+2)}) = F[C_{(8(i-1)+8)}] \dots F[C_{(8(i-1)+1)}](K_{(2i-1)}, K_{(2i)})$$

$$i = 1, 2, 3, 4$$

4.5. Базовый алгоритм шифрования

4.5.1. Шифрование

В зависимости от значений итерационных ключей K_1, \dots, K_{10} алгоритм шифрования определяется подстановкой $E(K_1, \dots, K_{10})$, определяемой как:

$E(K_1, \dots, K_{10})(a) = x[K_{10}]LSX[K_9] \dots LSX[K_2]LSX[K_1](a)$
где a принадлежит V_{128} .

4.5.2. Дешифрование

В зависимости от значений итерационных ключей K_1, \dots, K_{10} алгоритм дешифрования определяется подстановкой $D(K_1, \dots, K_{10})$, определяемой как:

$D(K_1, \dots, K_{10})(a) = x[K_1]L^{-1}S^{-1}x[K_2] \dots L^{-1}S^{-1}x[K_9] L^{-1}S^{-1}x[K_{10}](a)$
где a принадлежит V_{128} .

5. Примеры (для информации)

Приведённая в этом разделе информация не относится к нормативной части стандарта.

5.1. Преобразование S

$$S(\text{ffeeddccbbaa99881122334455667700}) = \text{b66cd8887d38e8d77765aeea0c9a7efc}$$

$$S(\text{b66cd8887d38e8d77765aeea0c9a7efc}) = \text{559d8dd7bd06cbfe7e7b262523280d39}$$

$$S(\text{559d8dd7bd06cbfe7e7b262523280d39}) = \text{0c3322fed531e4630d80ef5c5a81c50b}$$

Зашифрованный текст будет иметь вид

$$b = x[k_{10}]LSx[k_9] \dots LSx[k_1] (a) = 7f679d90bebc24305a468d42b9d4edcd$$

5.6. Тестовая расшифровка

В этом примере выполняется тестовое дешифрование с использованием итерационных ключей, указанных в параграфе 5.4. Пусть зашифрованный текст имеет вид

$$b = 7f679d90bebc24305a468d42b9d4edcd$$

тогда

$$\begin{aligned} X[k_{10}](b) &= 0d8e40e4a800d06b2f1b37ea379ead8e \\ L^{(-1)}X[k_{10}](b) &= 8a6b930a52211b45c5baa43ff8b91319 \\ S^{(-1)}L^{(-1)}X[k_{10}](b) &= 76ca149eef27d1b10d17e3d5d68e5a72 \\ S^{(-1)}L^{(-1)}X[k_9]S^{(-1)}L^{(-1)}X[k_{10}](b) &= 5d9b06d41b9d1d2d04df7755363e94a9 \\ S^{(-1)}L^{(-1)}X[k_8] \dots S^{(-1)}L^{(-1)}X[k_{10}](b) &= 79487192aa45709c115559d6e9280f6e \\ S^{(-1)}L^{(-1)}X[k_7] \dots S^{(-1)}L^{(-1)}X[k_{10}](b) &= ae506924c8ce331bb918fc5bdfb195fa \\ S^{(-1)}L^{(-1)}X[k_6] \dots S^{(-1)}L^{(-1)}X[k_{10}](b) &= bbfbfbc8939eaaaffafb8e22769e323aa \\ S^{(-1)}L^{(-1)}X[k_5] \dots S^{(-1)}L^{(-1)}X[k_{10}](b) &= 3cc2f07cc07a8bec0f3ea0ed2ae33e4a \\ S^{(-1)}L^{(-1)}X[k_4] \dots S^{(-1)}L^{(-1)}X[k_{10}](b) &= f36f01291d0b96d591e228b72d011c36 \\ S^{(-1)}L^{(-1)}X[k_3] \dots S^{(-1)}L^{(-1)}X[k_{10}](b) &= 1c4b0c1e950182b1ce696af5c0bfc5df \\ S^{(-1)}L^{(-1)}X[k_2] \dots S^{(-1)}L^{(-1)}X[k_{10}](b) &= 99bb99ff99bb99ffffffffffffffffffff \end{aligned}$$

Расшифрованный текст имеет вид

$$a = x[k_1]S^{(-1)}L^{(-1)}X[k_2] \dots S^{(-1)}L^{(-1)}X[k_{10}](b) = 1122334455667700ffeaddccbbaa9988$$

6. Вопросы безопасности

Документ целиком посвящён вопросам безопасности.

7. Литература

7.1. Нормативные документы

[GOST3412-2015] "Information technology. Cryptographic data security. Block ciphers", GOST R 34.12-2015, Federal Agency on Technical Regulating and Metrology, 2015.

7.2. Дополнительная литература

[ISO-IEC10116] ISO/IEC, "Information technology -- Security techniques -- Modes of operation for an n-bit block cipher", ISO/IEC 10116, 2006.

[ISO-IEC18033-1] ISO/IEC, "Information technology -- Security techniques -- Encryption algorithms -- Part 1: General", ISO/IEC 18033-1, 2015.

[ISO-IEC18033-3] ISO/IEC, "Information technology -- Security techniques -- Encryption algorithms -- Part 3: Block ciphers", ISO/IEC 18033-3, 2010.

Адрес автора

Василий Долматов (редактор)

Research Computer Center MSU

Leninskiye Gory, 1, Building 4, MGU NIVC

Moscow 119991

Russian Federation

Email: dol@srcc.msu.ru

Перевод на русский язык

Николай Малых

nmalykh@protokols.ru