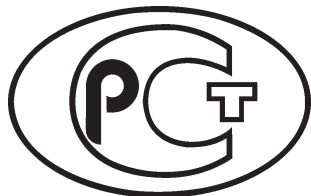

ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ



НАЦИОНАЛЬНЫЙ
СТАНДАРТ
РОССИЙСКОЙ
ФЕДЕРАЦИИ

ГОСТ Р
34.12—
2015

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Блочные шифры

Издание официальное



Москва
Стандартинформ
2018

Предисловие

1 РАЗРАБОТАН Центром защиты информации и специальной связи ФСБ России с участием Открытого акционерного общества «Информационные технологии и коммуникационные системы» (ОАО «ИнфоТеКС»)

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 26 «Криптографическая защита информации»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 19 июня 2015 г. № 749-ст

4 ВВЕДЕН ВПЕРВЫЕ

5 ПЕРЕИЗДАНИЕ. Октябрь 2018 г.

Правила применения настоящего стандарта установлены в статье 26 Федерального закона от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации». Информация об изменениях к настоящему стандарту публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а официальный текст изменений и поправок — в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ближайшем выпуске информационного указателя «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (www.gost.ru)

© Стандартиформ, оформление, 2018

Настоящий стандарт не может быть полностью или частично воспроизведен, тиражирован и распространен в качестве официального издания без разрешения Федерального агентства по техническому регулированию и метрологии

Введение

Настоящий стандарт содержит описание алгоритмов блочного шифрования, которые применяются в криптографических методах защиты информации.

Необходимость разработки стандарта вызвана потребностью в создании блочных шифров с различными длинами блока, соответствующих современным требованиям к криптографической стойкости и эксплуатационным качествам.

Настоящий стандарт терминологически и концептуально увязан с международными стандартами ИСО/МЭК 10116 [1] и серии ИСО/МЭК 18033 [2], [3].

П р и м е ч а н и е — Основная часть стандарта дополнена приложением А.

ФЕДЕРАЛЬНОЕ АГЕНТСТВО ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

ФЕДЕРАЛЬНОЕ АГЕНТСТВО ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

Информационная технология
КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Блочные шифры

Information technology. Cryptographic data security.
Block ciphers

Дата введения — 2016—01—01

1 Область применения

Настоящий стандарт определяет алгоритмы базовых блочных шифров, которые применяются в криптографических методах обработки и защиты информации, в том числе для обеспечения конфиденциальности, аутентичности и целостности информации при ее передаче, обработке и хранении в автоматизированных системах.

Определенные в настоящем стандарте алгоритмы криптографического преобразования предназначены для аппаратной или программной реализации, удовлетворяют современным криптографическим требованиям и по своим возможностям не накладывают ограничений на степень секретности защищаемой информации.

Стандарт рекомендуется использовать при создании, эксплуатации и модернизации систем обработки информации различного назначения.

2 Термины, определения и обозначения

2.1 Термины и определения

В настоящем стандарте применены следующие термины с соответствующими определениями.

2.1.1

алгоритм зашифрования (encryption algorithm): Алгоритм, реализующий зашифрование, т.е. преобразующий открытый текст в шифртекст.
[ИСО/МЭК 18033-1, статья 2.19]

2.1.2

алгоритм расшифрования (decryption algorithm): Алгоритм, реализующий расшифрование, т.е. преобразующий шифртекст в открытый текст.
[ИСО/МЭК 18033-1, статья 2.14]

2.1.3

базовый блочный шифр (basic block cipher): Блочный шифр, реализующий при каждом фиксированном значении ключа одно обратимое отображение множества блоков открытого текста фиксированной длины в блоки шифртекста такой же длины.

2.1.4

блок (block): Строка бит определенной длины.
[ИСО/МЭК 18033-1, статья 2.6]

2.1.5

блочный шифр (block cipher): Шифр из класса симметричных криптографических методов, в котором алгоритм зашифрования применяется к блокам открытого текста для получения блоков шифртекста.

[ИСО/МЭК 18033-1, статья 2.7]

Примечание — В настоящем стандарте установлено, что термины «блочный шифр» и «алгоритм блочного шифрования» являются синонимами.

2.1.6

зашифрование (encryption): Обратимое преобразование данных с помощью шифра, которое формирует шифртекст из открытого текста.

[ИСО/МЭК 18033-1, статья 2.18]

2.1.7

итерационный ключ (round key): Последовательность символов, вычисляемая в процессе развертывания ключа шифра и определяющая преобразование на одной итерации блочного шифра.

2.1.8

ключ (key): Изменяемый параметр в виде последовательности символов, определяющий криптографическое преобразование.

[ИСО/МЭК 18033-1, статья 2.21]

Примечание — В настоящем стандарте рассматриваются ключи только в виде последовательности двоичных символов (битов).

2.1.9

открытый текст (plaintext): Незашифрованная информация.

[ИСО/МЭК 10116, статья 3.11]

2.1.10

развертывание ключа (key schedule): Вычисление итерационных ключей из ключа шифра.

2.1.11

расшифрование (decryption): Операция, обратная к зашифрованию.

[ИСО/МЭК 18033-1, статья 2.13]

Примечание — В настоящем стандарте в целях сохранения терминологической преемственности по отношению к опубликованным научно-техническим изданиям применяется термин «шифрование», объединяющий операции, определенные терминами «зашифрование» и «расшифрование». Конкретное значение термина «шифрование» определяется в зависимости от контекста упоминания.

2.1.12

симметричный криптографический метод (symmetric cryptographic technique): Криптографический метод, использующий один и тот же ключ для преобразования, осуществляемого отправителем, и преобразования, осуществляемого получателем.

[ИСО/МЭК 18033-1, статья 2.32]

2.1.13

шифр (cipher): Криптографический метод, используемый для обеспечения конфиденциальности данных, включающий алгоритм зашифрования и алгоритм расшифрования.

[ИСО/МЭК 18033-1, статья 2.20]

2.1.14

шифртекст (ciphertext): Данные, полученные в результате зашифрования открытого текста с целью скрытия его содержания.

[ИСО/МЭК 10116, статья 3.3]

2.2 Обозначения

В настоящем стандарте использованы следующие обозначения:

V^* — множество всех двоичных строк конечной длины, включая пустую строку;

V_s	— множество всех двоичных строк длины s , где s — целое неотрицательное число; нумерация подстрок и компонент строки осуществляется справа налево начиная с нуля;
$U \times W$	— прямое (декартово) произведение множества U и множества W ;
$ A $	— число компонент (длина) строки $A \in V^*$ (если A — пустая строка, то $ A = 0$);
$A B$	— конкатенация строк $A, B \in V^*$, т.е. строка из $V_{ A + B }$, в которой подстрока с большими номерами компонент из $V_{ A }$ совпадает со строкой A , а подстрока с меньшими номерами компонент из $V_{ B }$ совпадает со строкой B ;
$A \ll_{11}$	— циклический сдвиг строки $A \in V_{32}$ на 11 компонент в сторону компонент, имеющих большие номера;
\oplus	— операция покомпонентного сложения по модулю 2 двух двоичных строк одинаковой длины;
\mathbb{Z}_{2^s}	— кольцо вычетов по модулю 2^s ;
\boxplus	— операция сложения в кольце $\mathbb{Z}_{2^{32}}$;
\mathbb{F}	— конечное поле $GF(2)[x]/p(x)$, где $p(x) = x^8 + x^7 + x^6 + x + 1 \in GF(2)[x]$; элементы поля \mathbb{F} представляются целыми числами, причем элементу $z_0 + z_1 \cdot \theta + \dots + z_7 \cdot \theta^7 \in \mathbb{F}$ соответствует число $z_0 + 2 \cdot z_1 + \dots + 2^7 \cdot z_7$, где $z_i \in \{0, 1\}$, $i = 0, 1, \dots, 7$, и θ обозначает класс вычетов по модулю $p(x)$, содержащий x ;
$\text{Vec}_s: \mathbb{Z}_{2^s} \rightarrow V_s$	— биективное отображение, сопоставляющее элементу кольца \mathbb{Z}_{2^s} его двоичное представление, т.е. для любого элемента $z \in \mathbb{Z}_{2^s}$, представленного в виде $z = z_0 + 2 \cdot z_1 + \dots + 2^{s-1} \cdot z_{s-1}$, где $z_i \in \{0, 1\}$, $i = 0, 1, \dots, s-1$, выполнено равенство $\text{Vec}_s(z) = z_{s-1} \dots z_1 z_0$;
$\text{Int}_s: V_s \rightarrow \mathbb{Z}_{2^s}$	— отображение, обратное к отображению Vec_s , т.е. $\text{Int}_s = \text{Vec}_s^{-1}$;
$\Delta: V_8 \rightarrow \mathbb{F}$	— биективное отображение, сопоставляющее двоичной строке из V_8 элемент поля \mathbb{F} следующим образом: строке $z_7 \dots z_1 z_0$, $z_i \in \{0, 1\}$, $i = 0, 1, \dots, 7$, соответствует элемент $z_0 + z_1 \cdot \theta + \dots + z_7 \cdot \theta^7 \in \mathbb{F}$;
$\nabla: \mathbb{F} \rightarrow V_8$	— отображение, обратное к отображению Δ , т.е. $\nabla = \Delta^{-1}$;
$\Phi\Psi$	— композиция отображений, при которой отображение Ψ действует первым;
Φ^s	— композиция отображений Φ^{s-1} и Φ , причем $\Phi^1 = \Phi$.

3 Общие положения

В настоящем стандарте приведено описание двух базовых блочных шифров с длинами блоков $n = 128$ бит и $n = 64$ бит и длинами ключей $k = 256$ бит.

Примечания

1 На описанный в настоящем стандарте шифр с длиной блока $n = 128$ бит можно ссылаться как на блочный шифр «Кузнечик» («Kuznyechik»).

2 На описанный в настоящем стандарте шифр с длиной блока $n = 64$ бит можно ссылаться как на блочный шифр «Магма» («Magma»).

4 Алгоритм блочного шифрования с длиной блока $n = 128$ бит

4.1 Значения параметров

4.1.1 Нелинейное биективное преобразование

В качестве нелинейного биективного преобразования выступает подстановка $\pi = \text{Vec}_8 \pi' \text{Int}_8: V_8 \rightarrow V_8$, где $\pi': \mathbb{Z}_{2^8} \rightarrow \mathbb{Z}_{2^8}$. Значения подстановки π' записаны ниже в виде массива $\pi' = (\pi'(0), \pi'(1), \dots, \pi'(255))$:

$\pi' = (252, 238, 221, 17, 207, 110, 49, 22, 251, 196, 250, 218, 35, 197, 4, 77, 233, 119, 240, 219, 147, 46, 153, 186, 23, 54, 241, 187, 20, 205, 95, 193, 249, 24, 101, 90, 226, 92, 239, 33, 129, 28, 60, 66, 139, 1, 142, 79, 5, 132, 2, 174, 227, 106, 143, 160, 6, 11, 237, 152, 127, 212, 211, 31, 235, 52, 44, 81, 234, 200, 72, 171,$

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).

4.1.2 Линейное преобразование

Линейное преобразование задается отображением $\ell: V_8^{16} \rightarrow V_8$, которое определяется следующим образом:

$$\begin{aligned} \ell(a_{15}, \dots, a_0) = & \nabla(148 \cdot \Delta(a_{15}) + 32 \cdot \Delta(a_{14}) + 133 \cdot \Delta(a_{13}) + 16 \cdot \Delta(a_{12}) + \\ & + 194 \cdot \Delta(a_{11}) + 192 \cdot \Delta(a_{10}) + 1 \cdot \Delta(a_9) + 251 \cdot \Delta(a_8) + 1 \cdot \Delta(a_7) + 192 \cdot \Delta(a_6) + \\ & + 194 \cdot \Delta(a_5) + 16 \cdot \Delta(a_4) + 133 \cdot \Delta(a_3) + 32 \cdot \Delta(a_2) + 148 \cdot \Delta(a_1) + 1 \cdot \Delta(a_0)) \end{aligned} \quad (1)$$

для любых $a_i \in V_8$, $i = 0, 1, \dots, 15$, где операции сложения и умножения осуществляются в поле \mathbb{F} , а константы являются элементами поля в указанном ранее смысле.

4.2 Преобразования

При реализации алгоритмов зашифрования и расшифрования используются следующие преобразования:

$$X[k]: V_{128} \rightarrow V_{128} \quad X[k](a) = k \oplus a, \quad \text{где } k, a \in V_{128}; \quad (2)$$

$$S: V_{128} \rightarrow V_{128} \quad S(a) = S(a_{15} \parallel \dots \parallel a_0) = \pi(a_{15}) \parallel \dots \parallel \pi(a_0), \quad (3)$$

где $a = a_{15} \parallel \dots \parallel a_0 \in V_{128}$, $a_i \in V_8$, $i = 0, 1, \dots, 15$;

$$S^{-1}: V_{128} \rightarrow V_{128} \quad \text{преобразование, обратное к преобразованию } S, \text{ которое может} \quad (4)$$

быть вычислено, например, следующим образом:
 $S^{-1}(a) = S^{-1}(a_{15} \parallel \dots \parallel a_0) = \pi^{-1}(a_{15}) \parallel \dots \parallel \pi^{-1}(a_0)$,
 где $a = a_{15} \parallel \dots \parallel a_0 \in V_{128}$, $a_i \in V_8$, $i = 0, 1, \dots, 15$;
 π^{-1} — подстановка, обратная к подстановке π ;

$$R: V_{128} \rightarrow V_{128} \quad R(a) = R(a_{15} \parallel \dots \parallel a_0) = \ell(a_{15}, \dots, a_0) \parallel a_{15} \parallel \dots \parallel a_1, \quad (5)$$

где $a = a_{15} \parallel \dots \parallel a_0 \in V_{128}$, $a_i \in V_8$, $i = 0, 1, \dots, 15$;

$$L: V_{128} \rightarrow V_{128} \quad L(a) = R^{16}(a), \quad (6)$$

где $a \in V_{128}$;

$$R^{-1}: V_{128} \rightarrow V_{128} \quad \text{преобразование, обратное к преобразованию } R, \text{ которое может} \quad (7)$$

быть вычислено, например, следующим образом:
 $R^{-1}(a) = R^{-1}(a_{15} \parallel \dots \parallel a_0) = a_{14} \parallel a_{13} \parallel \dots \parallel a_0 \parallel \ell(a_{14}, a_{13}, \dots, a_0, a_{15})$,
 где $a = a_{15} \parallel \dots \parallel a_0 \in V_{128}$, $a_i \in V_8$, $i = 0, 1, \dots, 15$;

$$L^{-1}: V_{128} \rightarrow V_{128} \quad L^{-1}(a) = (R^{-1})^{16}(a), \quad (8)$$

где $a \in V_{128}$;

$$F[k]: V_{128} \times V_{128} \rightarrow V_{128} \times V_{128} \quad F[k](a_1, a_0) = (LSX[k]((a_1) \oplus a_0, a_1), \quad (9)$$

где $k, a_0, a_1 \in V_{128}$.

4.3 Алгоритм развертывания ключа

Алгоритм развертывания ключа использует итерационные константы $C_i \in V_{128}$, $i = 1, 2, \dots, 32$, которые определены следующим образом:

$$C_i = L(\text{Vec}_{128}(i)), \quad i = 1, 2, \dots, 32. \quad (10)$$

Итерационные ключи $K_i \in V_{128}$, $i = 1, 2, \dots, 10$ вырабатываются на основе ключа $K = k_{255} \parallel \dots \parallel k_0 \in V_{256}$, $k_i \in V_1$, $i = 0, 1, \dots, 255$ и определяются равенствами:

$$K_1 = k_{255} \parallel \dots \parallel k_{128};$$

$$K_2 = k_{127} \parallel \dots \parallel k_0; \quad (11)$$

$$(K_{2i+1}, K_{2i+2}) = F[C_{8(i-1)+8}] \dots F[C_{8(i-1)+1}](K_{2i-1}, K_{2i}), i = 1, 2, 3, 4.$$

4.4 Базовый алгоритм шифрования

4.4.1 Алгоритм зашифрования

Алгоритм зашифрования в зависимости от значений итерационных ключей $K_i \in V_{128}$, $i = 1, 2, \dots, 10$ реализует подстановку $E_{K_1, \dots, K_{10}}$, заданную на множестве V_{128} в соответствии с равенством

$$E_{K_1, \dots, K_{10}}(a) = X[K_{10}]LSX[K_9] \dots LSX[K_2][K_1](a), \quad (12)$$

где $a \in V_{128}$.

4.4.2 Алгоритм расшифрования

Алгоритм расшифрования в зависимости от значений итерационных ключей $K_i \in V_{128}$, $i = 1, 2, \dots, 10$ реализует подстановку $D_{K_1, \dots, K_{10}}$, заданную на множестве V_{128} в соответствии с равенством

$$D_{K_1, \dots, K_{10}}(a) = X[K_1]S^{-1}L^{-1}X[K_2] \dots S^{-1}L^{-1}X[K_9]S^{-1}L^{-1}X[K_{10}](a), \quad (13)$$

где $a \in V_{128}$.

5 Алгоритм блочного шифрования с длиной блока $n = 64$ бит

5.1 Значения параметров

5.1.1 Нелинейное биективное преобразование

В качестве нелинейного биективного преобразования выступают подстановки $\pi_i = \text{Vec}_4 \pi'_i \text{Int}_4: V_4 \rightarrow V_4$, где $\pi'_i: \mathbb{Z}_{2^4} \rightarrow \mathbb{Z}_{2^4}$, $i = 0, 1, \dots, 7$. Значения подстановок π'_i записаны ниже в виде массивов $\pi'_i = (\pi'_i(0), \pi'_i(1), \dots, \pi'_i(15))$, $i = 0, 1, \dots, 7$:

$$\begin{aligned} \pi'_0 &= (12, 4, 6, 2, 10, 5, 11, 9, 14, 8, 13, 7, 0, 3, 15, 1); \\ \pi'_1 &= (6, 8, 2, 3, 9, 10, 5, 12, 1, 14, 4, 7, 11, 13, 0, 15); \\ \pi'_2 &= (11, 3, 5, 8, 2, 15, 10, 13, 14, 1, 7, 4, 12, 9, 6, 0); \\ \pi'_3 &= (12, 8, 2, 1, 13, 4, 15, 6, 7, 0, 10, 5, 3, 14, 9, 11); \\ \pi'_4 &= (7, 15, 5, 10, 8, 1, 6, 13, 0, 9, 3, 14, 11, 4, 2, 12); \\ \pi'_5 &= (5, 13, 15, 6, 9, 2, 12, 10, 11, 7, 8, 1, 4, 3, 14, 0); \\ \pi'_6 &= (8, 14, 2, 5, 6, 9, 1, 12, 15, 4, 11, 0, 13, 10, 3, 7); \\ \pi'_7 &= (1, 7, 14, 13, 0, 5, 8, 3, 4, 15, 10, 6, 9, 12, 11, 2). \end{aligned}$$

5.2 Преобразования

При реализации алгоритмов зашифрования и расшифрования используются следующие преобразования:

$$t: V_{32} \rightarrow V_{32} \quad t(a) = t(a_7 \parallel \dots \parallel a_0) = \pi_7(a_7) \parallel \dots \parallel \pi_0(a_0), \quad (14)$$

$$\text{где } a = a_7 \parallel \dots \parallel a_0 \in V_{32}, a_i \in V_4, i = 0, 1, \dots, 7;$$

$$g[k]: V_{32} \rightarrow V_{32} \quad g[k](a) = (t(\text{Vec}_{32}(\text{Int}_{32}(a) \boxplus \text{Int}_{32}(k)))) \lll_{11}, \quad (15)$$

$$\text{где } k, a \in V_{32};$$

$$G[k]: V_{32} \times V_{32} \rightarrow V_{32} \times V_{32} \quad G[k](a_1, a_0) = (a_0, g[k](a_0) \oplus a_1), \quad (16)$$

$$\text{где } k, a_0, a_1 \in V_{32};$$

$$G^*[k]: V_{32} \times V_{32} \rightarrow V_{64} \quad G^*[k](a_1, a_0) = (g[k](a_0) \oplus a_1) \parallel a_0, \quad (17)$$

$$\text{где } k, a_0, a_1 \in V_{32}.$$

5.3 Алгоритм развертывания ключа

Итерационные ключи $K_i \in V_{32}$, $i = 1, 2, \dots, 32$ вырабатываются на основе ключа $K = k_{255} \parallel \dots \parallel k_0 \in V_{256}$, $k_i \in V_1$, $i = 0, 1, \dots, 255$ и определяются равенствами:

$$K_1 = k_{255} \parallel \dots \parallel k_{224};$$

$$K_2 = k_{223} \parallel \dots \parallel k_{192};$$

$$\begin{aligned}
K_3 &= k_{191} \parallel \dots \parallel k_{160}; \\
K_4 &= k_{159} \parallel \dots \parallel k_{128}; \\
K_5 &= k_{127} \parallel \dots \parallel k_{96}; \\
K_6 &= k_{95} \parallel \dots \parallel k_{64}; \\
K_7 &= k_{63} \parallel \dots \parallel k_{32}; \\
K_8 &= k_{31} \parallel \dots \parallel k_0; \\
K_{i+8} &= K_i, i = 1, 2, \dots, 8; \\
K_{i+16} &= K_i, i = 1, 2, \dots, 8; \\
K_{i+24} &= K_{9-i}, i = 1, 2, \dots, 8.
\end{aligned} \tag{18}$$

5.4 Базовый алгоритм шифрования

5.4.1 Алгоритм зашифрования

Алгоритм зашифрования в зависимости от значений итерационных ключей $K_i \in V_{32}$, $i = 1, 2, \dots, 32$ реализует подстановку $E_{K_1, \dots, K_{32}}$, заданную на множестве V_{64} в соответствии с равенством

$$E_{K_1, \dots, K_{32}}(a) = G^*[K_{32}]G[K_{31}] \dots G[K_2]G[K_1](a_1, a_0), \tag{19}$$

где $a = a_1 \parallel a_0 \in V_{64}$, $a_0, a_1 \in V_{32}$.

5.4.2 Алгоритм расшифрования

Алгоритм расшифрования в зависимости от значений итерационных ключей $K_i \in V_{32}$, $i = 1, 2, \dots, 32$ реализует подстановку $D_{K_1, \dots, K_{32}}$, заданную на множестве V_{64} в соответствии с равенством

$$D_{K_1, \dots, K_{32}}(a) = G^*[K_1]G[K_2] \dots G[K_{31}]G[K_{32}](a_1, a_0), \tag{20}$$

где $a = a_1 \parallel a_0 \in V_{64}$, $a_0, a_1 \in V_{32}$.

Контрольные примеры

В данном приложении двоичные строки из V^* , длина которых кратна 4, записываются в шестнадцатеричном виде, а символ конкатенации ("||") опускается. То есть строка $a \in V_{4r}$ будет представлена в виде

$$a_{r-1}a_{r-2} \dots a_0,$$

где $a_i \in \{0, 1, \dots, 9, a, b, c, d, e, f\}$, $i = 0, 1, \dots, r-1$. Соответствие между двоичными строками длины 4 и шестнадцатеричными строками длины 1 задает естественным образом (таблица А.1). Преобразование, ставящее в соответствие двоичной строке длины $4r$ шестнадцатеричную строку длины r , и соответствующее обратное преобразование для простоты записи опускаются.

Т а б л и ц а А.1 — Соответствие между двоичными и шестнадцатеричными строками

0000	0
0001	1
0010	2
0011	3
0100	4
0101	5
0110	6
0111	7
1000	8
1001	9
1010	a
1011	b
1100	c
1101	d
1110	e
1111	f

А.1.1 Преобразование S

S(feedcdccbbaa99881122334455667700) = b66cd8887d38e8d77765aeaa0c9a7efc,
S(b66cd8887d38e8d77765aeaa0c9a7efc) = 559d8dd7bd06cbfe7e7b262523280d39,
S(559d8dd7bd06cbfe7e7b262523280d39) = 0c3322fed531e4630d80ef5c5a81c50b,
S(0c3322fed531e4630d80ef5c5a81c50b) = 23ae65633f842d29c5df529c13f5acda.

[illegible]

L(64a594000000000000000000000000) = d456584dd0e3e84cc3166e4b7fa2890d,
L(d456584dd0e3e84cc3166e4b7fa2890d) = 79d26221b87b584cd42fbc4ffea5de9a,
L(79d26221b87b584cd42fbc4ffea5de9a) = 0e93691a0cfc60408b7b68f66b513c13,
L(0e93691a0cfc60408b7b68f66b513c13) = e6a8094fee0aa204fd97bcb0b44b8580.

В настоящем контрольном примере ключ имеет значение:

$K = 8899aabbccddeeff0011223344556677fedcba98765432100123456789abcdef.$

$K_1 = 8899aabbccddeeff0011223344556677.$

$K_2 = \text{fedcba98765432100123456789abcdef.}$

$C_1 = 6ea276726c487ab85d27bd10dd849401$,
 $X[C_1](K_1) = e63bdcc9a09594475d369f2399d1f276$,
 $SX[C_1](K_1) = 0998ca37a7947aabb78f4a5ae81b748a$,
 $LSX[C_1](K_1) = 3d0940999db75d6a9257071d5e6144a6$,
 $F[C_1](K_1, K_2) = (c3d5fa01ebe36f7a9374427ad7ca8949, 8899aabbccddeeff0011223344556677)$.

$C_2 = dc87ece4d890f4b3ba4eb92079cbeb02$,
 $F[C_2]F[C_1](K_1, K_2) = (37777748e56453377d5e262d90903f87, c3d5fa01ebe36f7a9374427ad7ca8949)$.

$C_3 = b2259a96b4d88e0be7690430a44f7f03$,
 $F[C_3] \dots F[C_1](K_1, K_2) = (f9eae5f29b2815e31f11ac5d9c29fb01, 37777748e56453377d5e262d90903f87)$.

$C_4 = 7bcd1b0b73e32ba5b79cb140f2551504$,
 $F[C_4] \dots F[C_1](K_1, K_2) = (e980089683d00d4be37dd3434699b98f, f9eae5f29b2815e31f11ac5d9c29fb01)$.

$C_5 = 156f6d791fab511deabb0c502fd18105$,
 $F[C_5] \dots F[C_1](K_1, K_2) = (b7bd70acea4460714f4ebe13835cf004, e980089683d00d4be37dd3434699b98f)$.

$C_6 = a74af7efab73df160dd208608b9efe06$,
 $F[C_6] \dots F[C_1](K_1, K_2) = (1a46ea1cf6ccd236467287df93fdf974, b7bd70acea4460714f4ebe13835cf004)$.

$C_7 = c9e8819dc73ba5ae50f5b570561a6a07$,
 $F[C_7] \dots F[C_1](K_1, K_2) = (3d4553d8e9cfec6815ebadc40a9ffd04, 1a46ea1cf6ccd236467287df93fdf974)$.

$C_8 = f6593616e6055689adfb18027aa2a08$,
 $(K_3, K_4) = F[C_8] \dots F[C_1](K_1, K_2) = (db31485315694343228d6aef8cc78c44, 3d4553d8e9cfec6815ebadc40a9ffd04)$.

Итерационные ключи $K_i, i = 1, 2, \dots, 10$ принимают следующие значения:

$K_1 = 8899aabbccddeeff0011223344556677$,
 $K_2 = fedcba98765432100123456789abcdef$,
 $K_3 = db31485315694343228d6aef8cc78c44$,
 $K_4 = 3d4553d8e9cfec6815ebadc40a9ffd04$,
 $K_5 = 57646468c44a5e28d3e59246f429f1ac$,
 $K_6 = bd079435165c6432b532e82834da581b$,
 $K_7 = 51e640757e8745de705727265a0098b1$,
 $K_8 = 5a7925017b9fdd3ed72a91a22286f984$,
 $K_9 = bb44e25378c73123a5f32f73cdb6e517$,
 $K_{10} = 72e9dd7416bcf45b755dbaa88e4a4043$.

A.1.5 Алгоритм зашифрования

В настоящем контрольном примере зашифрование производится при значениях итерационных ключей из

A.1.4. Пусть открытый текст, подлежащий зашифрованию, равен

$a = 1122334455667700ffeeddccbbaa9988$,

тогда

$X[K_1](a) = 99bb99ff99bb99ffffffffffff$,
 $SX[K_1](a) = e87de8b6e87de8b6b6b6b6b6b6b6b6b6$,
 $LSX[K_1](a) = e297b686e355b0a1cf4a2f9249140830$,
 $LSX[K_2]LSX[K_1](a) = 285e497a0862d596b36f4258a1c69072$,
 $LSX[K_3] \dots LSX[K_1](a) = 0187a3a429b567841ad50d29207cc34e$,
 $LSX[K_4] \dots LSX[K_1](a) = ec9bdba057d4f4d77c5d70619dcad206$,
 $LSX[K_5] \dots LSX[K_1](a) = 1357fd11de9257290c2a1473eb6bcde1$,
 $LSX[K_6] \dots LSX[K_1](a) = 28ae31e7d4c2354261027ef0b32897df$,
 $LSX[K_7] \dots LSX[K_1](a) = 07e223d56002c013d3f5e6f714b86d2d$,
 $LSX[K_8] \dots LSX[K_1](a) = cd8ef6cd97e0e092a8e4cca61b38bf65$,
 $LSX[K_9] \dots LSX[K_1](a) = 0d8e40e4a800d06b2f1b37ea379ead8e$.

Результатом зашифрования является шифртекст

$b = X[K_{10}]LSX[K_9] \dots LSX[K_1](a) = 7f679d90bebc24305a468d42b9d4edcd$.

A.1.6 Алгоритм расшифрования

В настоящем контрольном примере расшифрование производится при значениях итерационных ключей из

A.1.4. Пусть шифртекст, подлежащий расшифрованию, равен шифртексту, полученному в предыдущем пункте:

$b = 7f679d90bebc24305a468d42b9d4edcd$,

тогда

$X[K_{10}](b) = 0d8e40e4a800d06b2f1b37ea379ead8e$,

$L^{-1}X[K_{10}](b) = 8a6b930a52211b45c5baa43ff8b91319,$
 $S^{-1}L^{-1}X[K_{10}](b) = 76ca149eef27d1b10d17e3d5d68e5a72,$
 $S^{-1}L^{-1}X[K_9] \dots S^{-1}L^{-1}X[K_{10}](b) = 5d9b06d41b9d1d2d04df7755363e94a9,$
 $S^{-1}L^{-1}X[K_8] \dots S^{-1}L^{-1}X[K_{10}](b) = 79487192aa45709c115559d6e9280f6e,$
 $S^{-1}L^{-1}X[K_7] \dots S^{-1}L^{-1}X[K_{10}](b) = ae506924c8ce331bb918fc5bdfb195fa,$
 $S^{-1}L^{-1}X[K_6] \dots S^{-1}L^{-1}X[K_{10}](b) = bbfbc8939eaaffab8e22769e323aa,$
 $S^{-1}L^{-1}X[K_5] \dots S^{-1}L^{-1}X[K_{10}](b) = 3cc2f07cc07a8bec0f3ea0ed2ae33e4a,$
 $S^{-1}L^{-1}X[K_4] \dots S^{-1}L^{-1}X[K_{10}](b) = f36f01291d0b96d591e228b72d011c36,$
 $S^{-1}L^{-1}X[K_3] \dots S^{-1}L^{-1}X[K_{10}](b) = 1c4b0c1e950182b1ce696af5c0bfc5df,$
 $S^{-1}L^{-1}X[K_2] \dots S^{-1}L^{-1}X[K_{10}](b) = 99bb99ff99bb99ffffffffffff.$

Результатом расшифрования является открытый текст

$a = X[K_1]S^{-1}L^{-1}X[K_2] \dots S^{-1}L^{-1}X[K_{10}](b) = 1122334455667700ffeeddccbbaa9988.$

А.2 Алгоритм блочного шифрования с длиной блока $n = 64$ бит

А.2.1 Преобразование t

$t(\text{fdb97531}) = 2a196f34,$

$t(2a196f34) = \text{ebd9f03a},$

$t(\text{ebd9f03a}) = \text{b039bb3d},$

$t(\text{b039bb3d}) = 68695433.$

А.2.2 Преобразование g

$g[87654321](\text{fedcba98}) = \text{fdcbc20c},$

$g[\text{fdcbc20c}](87654321) = 7e791a4b,$

$g[7e791a4b](\text{fdcbc20c}) = \text{c76549ec},$

$g[\text{c76549ec}](7e791a4b) = 9791c849.$

А.2.3 Алгоритм развертывания ключа

В настоящем контрольном примере ключ имеет значение:

$K = \text{ffeeddccbbaa99887766554433221100f0f1f2f3f4f5f6f7f8f9fafbfcdfeff}.$

Итерационные ключи $K_i, i = 1, 2, \dots, 32$ принимают следующие значения:

$K_1 = \text{ffeeddcc},$	$K_9 = \text{ffeeddcc},$	$K_{17} = \text{ffeeddcc},$	$K_{25} = \text{fcfdfeff},$
$K_2 = \text{bbaa9988},$	$K_{10} = \text{bbaa9988},$	$K_{18} = \text{bbaa9988},$	$K_{26} = \text{f8f9fafb},$
$K_3 = 77665544,$	$K_{11} = 77665544,$	$K_{19} = 77665544,$	$K_{27} = \text{f4f5f6f7},$
$K_4 = 33221100,$	$K_{12} = 33221100,$	$K_{20} = 33221100,$	$K_{28} = \text{f0f1f2f3},$
$K_5 = \text{f0f1f2f3},$	$K_{13} = \text{f0f1f2f3},$	$K_{21} = \text{f0f1f2f3},$	$K_{29} = 33221100,$
$K_6 = \text{f4f5f6f7},$	$K_{14} = \text{f4f5f6f7},$	$K_{22} = \text{f4f5f6f7},$	$K_{30} = 77665544,$
$K_7 = \text{f8f9fafb},$	$K_{15} = \text{f8f9fafb},$	$K_{23} = \text{f8f9fafb},$	$K_{31} = \text{bbaa9988},$
$K_8 = \text{fcfdfeff},$	$K_{16} = \text{fcfdfeff},$	$K_{24} = \text{fcfdfeff},$	$K_{32} = \text{ffeeddcc}.$

А.2.4 Алгоритм зашифрования

В настоящем контрольном примере зашифрование производится при значениях итерационных ключей из

А.2.3. Пусть открытый текст, подлежащий зашифрованию, равен

$a = \text{fedcba9876543210},$

тогда

$(a_1, a_0) = (\text{fedcba98}, 76543210),$
 $G[K_1](a_1, a_0) = (76543210, 28da3b14),$
 $G[K_2]G[K_1](a_1, a_0) = (28da3b14, b14337a5),$
 $G[K_3] \dots G[K_1](a_1, a_0) = (b14337a5, 633a7c68),$
 $G[K_4] \dots G[K_1](a_1, a_0) = (633a7c68, ea89c02c),$
 $G[K_5] \dots G[K_1](a_1, a_0) = (ea89c02c, 11fe726d),$
 $G[K_6] \dots G[K_1](a_1, a_0) = (11fe726d, ad0310a4),$
 $G[K_7] \dots G[K_1](a_1, a_0) = (ad0310a4, 37d97f25),$
 $G[K_8] \dots G[K_1](a_1, a_0) = (37d97f25, 46324615),$
 $G[K_9] \dots G[K_1](a_1, a_0) = (46324615, ce995f2a),$
 $G[K_{10}] \dots G[K_1](a_1, a_0) = (ce995f2a, 93c1f449),$
 $G[K_{11}] \dots G[K_1](a_1, a_0) = (93c1f449, 4811c7ad),$
 $G[K_{12}] \dots G[K_1](a_1, a_0) = (4811c7ad, c4b3edca),$
 $G[K_{13}] \dots G[K_1](a_1, a_0) = (c4b3edca, 44ca5ce1),$
 $G[K_{14}] \dots G[K_1](a_1, a_0) = (44ca5ce1, fef51b68),$

$G[K_{15}] \dots G[K_1](a_1, a_0) = (\text{fef51b68}, 2098\text{cd86}),$
 $G[K_{16}] \dots G[K_1](a_1, a_0) = (2098\text{cd86}, 4\text{f15b0bb}),$
 $G[K_{17}] \dots G[K_1](a_1, a_0) = (4\text{f15b0bb}, \text{e32805bc}),$
 $G[K_{18}] \dots G[K_1](a_1, a_0) = (\text{e32805bc}, \text{e7116722}),$
 $G[K_{19}] \dots G[K_1](a_1, a_0) = (\text{e7116722}, 89\text{cadf21}),$
 $G[K_{20}] \dots G[K_1](a_1, a_0) = (89\text{cadf21}, \text{bac8444d}),$
 $G[K_{21}] \dots G[K_1](a_1, a_0) = (\text{bac8444d}, 11263\text{a21}),$
 $G[K_{22}] \dots G[K_1](a_1, a_0) = (11263\text{a21}, 62543\text{c3}),$
 $G[K_{23}] \dots G[K_1](a_1, a_0) = (62543\text{c3}, 8025\text{c0a5}),$
 $G[K_{24}] \dots G[K_1](a_1, a_0) = (8025\text{c0a5}, \text{b0d66514}),$
 $G[K_{25}] \dots G[K_1](a_1, a_0) = (\text{b0d66514}, 47\text{b1d5f4}),$
 $G[K_{26}] \dots G[K_1](a_1, a_0) = (47\text{b1d5f4}, \text{c78e6d50}),$
 $G[K_{27}] \dots G[K_1](a_1, a_0) = (\text{c78e6d50}, 8025\text{1e99}),$
 $G[K_{28}] \dots G[K_1](a_1, a_0) = (8025\text{1e99}, 2\text{b96eca6}),$
 $G[K_{29}] \dots G[K_1](a_1, a_0) = (2\text{b96eca6}, 05\text{ef4401}),$
 $G[K_{30}] \dots G[K_1](a_1, a_0) = (05\text{ef4401}, 239\text{a4577}),$
 $G[K_{31}] \dots G[K_1](a_1, a_0) = (239\text{a4577}, \text{c2d8ca3d}).$

Результатом зашифрования является шифртекст

$$b = G^*[K_{32}]G[K_{31}] \dots G[K_1](a_1, a_0) = 4\text{ee901e5c2d8ca3d}.$$

А.2.5 Алгоритм расшифрования

В настоящем контрольном примере расшифрование производится при значениях итерационных ключей из А.2.3. Пусть шифртекст, подлежащий расшифрованию, равен шифртексту, полученному в предыдущем пункте:

$$b = 4\text{ee901e5c2d8ca3d},$$

тогда

$(b_1, b_0) = (4\text{ee901e5}, \text{c2d8ca3d}),$
 $G[K_{32}](b_1, b_0) = (\text{c2d8ca3d}, 239\text{a4577}),$
 $G[K_{31}]G[K_{32}](b_1, b_0) = (239\text{a4577}, 05\text{ef4401}),$
 $G[K_{30}] \dots G[K_{32}](b_1, b_0) = (05\text{ef4401}, 2\text{b96eca6}),$
 $G[K_{29}] \dots G[K_{32}](b_1, b_0) = (2\text{b96eca6}, 8025\text{1e99}),$
 $G[K_{28}] \dots G[K_{32}](b_1, b_0) = (8025\text{1e99}, \text{c78e6d50}),$
 $G[K_{27}] \dots G[K_{32}](b_1, b_0) = (\text{c78e6d50}, 47\text{b1d5f4}),$
 $G[K_{26}] \dots G[K_{32}](b_1, b_0) = (47\text{b1d5f4}, \text{b0d66514}),$
 $G[K_{25}] \dots G[K_{32}](b_1, b_0) = (\text{b0d66514}, 8025\text{c0a5}),$
 $G[K_{24}] \dots G[K_{32}](b_1, b_0) = (8025\text{c0a5}, 62543\text{c3}),$
 $G[K_{23}] \dots G[K_{32}](b_1, b_0) = (62543\text{c3}, 11263\text{a21}),$
 $G[K_{22}] \dots G[K_{32}](b_1, b_0) = (11263\text{a21}, \text{bac8444d}),$
 $G[K_{21}] \dots G[K_{32}](b_1, b_0) = (\text{bac8444d}, 89\text{cadf21}),$
 $G[K_{20}] \dots G[K_{32}](b_1, b_0) = (89\text{cadf21}, \text{e7116722}),$
 $G[K_{19}] \dots G[K_{32}](b_1, b_0) = (\text{e7116722}, \text{e32805bc}),$
 $G[K_{18}] \dots G[K_{32}](b_1, b_0) = (\text{e32805bc}, 4\text{f15b0bb}),$
 $G[K_{17}] \dots G[K_{32}](b_1, b_0) = (4\text{f15b0bb}, 2098\text{cd86}),$
 $G[K_{16}] \dots G[K_{32}](b_1, b_0) = (2098\text{cd86}, \text{fef51b68}),$
 $G[K_{15}] \dots G[K_{32}](b_1, b_0) = (\text{fef51b68}, 44\text{ca5ce1}),$
 $G[K_{14}] \dots G[K_{32}](b_1, b_0) = (44\text{ca5ce1}, \text{c4b3edca}),$
 $G[K_{13}] \dots G[K_{32}](b_1, b_0) = (\text{c4b3edca}, 4811\text{c7ad}),$
 $G[K_{12}] \dots G[K_{32}](b_1, b_0) = (4811\text{c7ad}, 93\text{c1f449}),$
 $G[K_{11}] \dots G[K_{32}](b_1, b_0) = (93\text{c1f449}, \text{ce995f2a}),$
 $G[K_{10}] \dots G[K_{32}](b_1, b_0) = (\text{ce995f2a}, 46324615),$
 $G[K_9] \dots G[K_{32}](b_1, b_0) = (46324615, 37\text{d97f25}),$
 $G[K_8] \dots G[K_{32}](b_1, b_0) = (37\text{d97f25}, \text{ad0310a4}),$
 $G[K_7] \dots G[K_{32}](b_1, b_0) = (\text{ad0310a4}, 11\text{fe726d}),$
 $G[K_6] \dots G[K_{32}](b_1, b_0) = (11\text{fe726d}, \text{ea89c02c}),$
 $G[K_5] \dots G[K_{32}](b_1, b_0) = (\text{ea89c02c}, 633\text{a7c68}),$
 $G[K_4] \dots G[K_{32}](b_1, b_0) = (633\text{a7c68}, \text{b14337a5}),$
 $G[K_3] \dots G[K_{32}](b_1, b_0) = (\text{b14337a5}, 28\text{da3b14}),$
 $G[K_2] \dots G[K_{32}](b_1, b_0) = (28\text{da3b14}, 76543210).$

Результатом расшифрования является открытый текст

$$a = G^*[K_1]G[K_2] \dots G[K_{32}](b_1, b_0) = \text{fedcba9876543210}.$$

Библиография*

- [1] ИСО/МЭК 10116:2006 (ISO/IEC 10116:2006) Информационные технологии. Методы обеспечения безопасности. Режимы работы для n -битовых блочных шифров (Information technology — Security techniques — Modes of operation for an n -bit block cipher)
- [2] ИСО/МЭК 18033-1:2005 (ISO/IEC 18033-1:2005) Информационные технологии. Методы и средства обеспечения безопасности. Алгоритмы шифрования. Часть 1. Общие положения (Information technology — Security techniques — Encryption algorithms — Part 1: General)
- [3] ИСО/МЭК 18033-3:2010 (ISO/IEC 18033-3:2010) Информационные технологии. Методы и средства обеспечения безопасности. Алгоритмы шифрования. Часть 3. Блочные шифры (Information technology — Security techniques — Encryption algorithms — Part 3: Block ciphers)

* Оригиналы международных стандартов ИСО/МЭК находятся во ФГУП «Стандартинформ» Федерального агентства по техническому регулированию и метрологии.

УДК 681.3.06:006.354

ОКС 35. 040

Ключевые слова: информационная технология, криптографическая защита информации, симметричный криптографический метод, зашифрование, расшифрование, блочный шифр, ключ

ФЕДЕРАЛЬНОЕ АГЕНТСТВО ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

Редактор *Л.В. Лукьянова*
Технический редактор *В.Н. Прусакова*
Корректор *И.А. Королева*
Компьютерная верстка *Е.О. Асташина*

Сдано в набор 01.10.2018. Подписано в печать 22.10.2018. Формат 60×84¹/₈. Гарнитура Ариал.
Усл. печ. л. 1,86. Уч.-изд. л. 1,68.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта