ФЕДЕРАЛЬНОЕ АГЕНТСТВО
ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ

Р 50. . — 20

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Криптографические алгоритмы, сопутствующие применению алгоритмов блочного шифрования

Издание официальное

Москва
Стандартинформ
2017

Предисловие

1 РАЗРАБОТАНЫ Обществом с ограниченной ответственностью «КРИПТО-ПРО» (ООО «КРИПТО-ПРО»)

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

3 УТВЕРЖДЕНЫ И ВВЕДЕНЫ В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 20 г. № -ст

4 ВВЕДЕНЫ ВПЕРВЫЕ

Правила применения настоящих рекомендаций установлены в статье 26 Федерального закона «О стандартизации в Российской Федерации». Информация об изменениях к настоящим рекомендациям 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 настоящих рекомендаций соответствующее уведомление будет опубликовано в ближайшем выпуске ежемесячного 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)

Содержание

Введение

Настоящие рекомендации содержат описание двух режимов работы блочных шифров с внутренним преобразованием ключа и алгоритмов импорта и экспорта ключей, сопутствующих применению алгоритмов блочного шифрования ГОСТ Р 34.12–2015 и режимов их работы ГОСТ Р 34.13–2015.

Необходимость разработки настоящих рекомендаций вызвана потребностью в обеспечении совместимости криптографических протоколов, использующих алгоритмы ГОСТ Р 34.12–2015 и ГОСТ Р 34.13–2015.

Примечание — Основная часть настоящих рекомендаций дополнена приложениями А и В.

РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Криптографические алгоритмы, сопутствующие применению алгоритмов блочного шифрования

Дата введения — 20 — — _

1 Область применения

Настоящие рекомендации предназначены для применения в информационных системах, использующих механизмы защиты данных, определенных в ГОСТ Р 34.12–2015 и ГОСТ Р 34.13–2015, в общедоступных и корпоративных сетях для защиты информации, не содержащей сведений, составляющих государственную тайну.

2 Нормативные ссылки

В настоящих рекомендациях использованы нормативные ссылки на следующие стандарты:

ГОСТ Р 34.11–2012 Информационная технология. Криптографическая защита информации. Функция хэширования

ГОСТ Р 34.12–2015 Информационная технология. Криптографическая защита информации. Блочные шифры

ГОСТ Р 34.13–2015 Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров

П р и м е ч а н и е — При пользовании настоящими рекомендациями целесообразно проверить действие ссылочных стандартов в информационной системе общего пользования – на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет или по ежегодному информационному указателю «Национальные стандарты», который опубликован по состоянию на 1 января текущего года, и по выпускам ежемесячного информационного указателя «Национальные стандарты» за текущий год. Если заменен ссылочный

Издание официальное

стандарт, на который дана недатированная ссылка, то рекомендуется использовать действующую версию этого стандарта с учетом всех внесенных в данную версию изменений. Если заменен ссылочный стандарт, на который дана датированная ссылка, то рекомендуется использовать версию этого стандарта с указанным выше годом утверждения (принятия). Если после утверждения настоящих рекомендаций в ссылочный стандарт, на который дана датированная ссылка, внесено изменение, затрагивающее положение, на которое дана ссылка, то это положение рекомендуется применять без учета данного изменения. Если ссылочный стандарт отменен без замены, то положение, в котором дана ссылка на него, применяется в части, не затрагивающей эту ссылку.

3 Обозначения

В настоящих рекомендациях используют 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 единицы;

$V_{\geq s}$ – множество всех двоичных строк длины $l \geq s$, где s — целое неотрицательное число: $V_{\geq s} = V^* \setminus \cup_{i=0}^{s-1} V_i$;

$\|$ – конкатенация двоичных строк; если $\alpha = (\alpha_{s_1}, \dots, \alpha_1) \in V_{s_1}$, $\beta = (\beta_{s_2}, \dots, \beta_1) \in V_{s_2}$, то их конкатенацией $\alpha \| \beta$ называется строка $\gamma = (\alpha_{s_1}, \dots, \alpha_1, \beta_{s_2}, \dots, \beta_1) \in V_{s_1+s_2}$;

$\oplus$ – операция покомпонентного сложения по модулю 2 двух двоичных строк одинаковой длины;

$\mathbb{Z}_{2^s}$ – кольцо вычетов по модулю 2^s;

$\boxplus_s$ – операция сложения в кольце $\mathbb{Z}_{2^s}$;

$\alpha \ll r$ – операция логического сдвига строки α на r компонент в сторону компонент, имеющих большие номера;

$|\alpha|$ – битовая длина строки α;

$E_K: V_n \to V_n$ – отображение, реализующее базовый алгоритм блочного шифрования на ключе K;

n – параметр алгоритма блочного шифрования, называемый длиной блока. В рамках данного документа измеряется в битах;

k – параметр алгоритма блочного шифрования, называемый длиной ключа. В рамках данного документа измеряется в битах и принимает значение 256;

a^r – строка, состоящая из r элементов $a \in \{0,1\}$;

$Int_s: V_s \to \mathbb{Z}_{2^s}$: – отображение, ставящее в соответствие строке $\alpha = (\alpha_s, \dots, \alpha_1) \in V_s$ число $Int_s(\alpha) = 256^{s-1}\alpha_s + \cdots + 256^0\alpha_1$;

$Vec_s: \mathbb{Z} \to V_s$ – отображение, обратное к отображению Int_s;

$Inc_s: V_s \to V_s$ – отображение, ставящее в соответствие строке $\alpha = (\alpha_s, \dots, \alpha_1) \in V_s$ строку $Vec_s(Int_s(\alpha) \boxplus_s 1)$;

$MSB_t: V_{\geq t} \to V_t$ – отображение, ставящее в соответствие строке $\alpha = (\alpha_s, \dots, \alpha_1) \in V_s$, строку $MSB_t(\alpha) = (\alpha_s, \dots, \alpha_{s-t+1}) \in V_t$, $1 \leq t \leq s$.

Примечание — Константы, определяемые в данных рекомендациях, приводятся в виде байтовой строки в шестнадцатеричном виде.

4 Режимы работы блочных шифров с преобразованием ключа

Настоящие рекомендации определяют следующие режимы работы алгоритмов блочного шифрования, которые используют в процессе своей работы механизмы преобразования ключа ACPKM и ACPKM-Master:

- режим шифрования CTR-ACPKM;
- режим выработки имитовставки OMAC-ACPKM.

Данные режимы могут использоваться в качестве режимов для блочных шифров Магма или Кузнечик, определенных в ГОСТ Р 34.12–2015. В первом случае подразумевается, что в качестве отображения E_K используется блочный шифр Магма с длиной блока $n = 64$, во втором случае подразумевается, что в качестве отображения E_K используется блочный шифр Кузнечик с длиной блока $n = 128$. Использование двух разных блочных шифров в рамках одного режима шифрования не допускается.

4.1 Режим шифрования CTR-ACPKM

В данном подразделе описан режим шифрования CTR-ACPKM. В основе режима CTR-ACPKM лежит режим гаммирования, в который встраивается механизм преобразования ключа ACPKM, описанный в 4.1.1.

При обработке сообщений в режиме CTR-ACPKM каждое сообщение разбивается на секции, где под секцией понимается строка, состоящая из данных, обрабатываемых на одном секционном ключе до применения к нему механизма преобразования ACPKM.

Параметром, определяющим порядок функционирования режима CTR-ACPKM, является длина секции N. Значение N измеряется в битах и фиксируется в рамках каждого конкретного протокола исходя из требований к производительности системы и нагрузке на ключ. Длина секции N должна быть кратна длине блока n используемого блочного

шифра. Дополнительным параметром режима CTR-ACPKM является длина блока гаммы s, $0 < s \leq n$, измеряющаяся в битах. В отличие от режима гаммирования, описанного в ГОСТ Р 34.13–2015, величина s должна делить длину блока n.

Процесс обработки сообщений в режиме CTR-ACPKM схематично отражен на Рисунке 1:

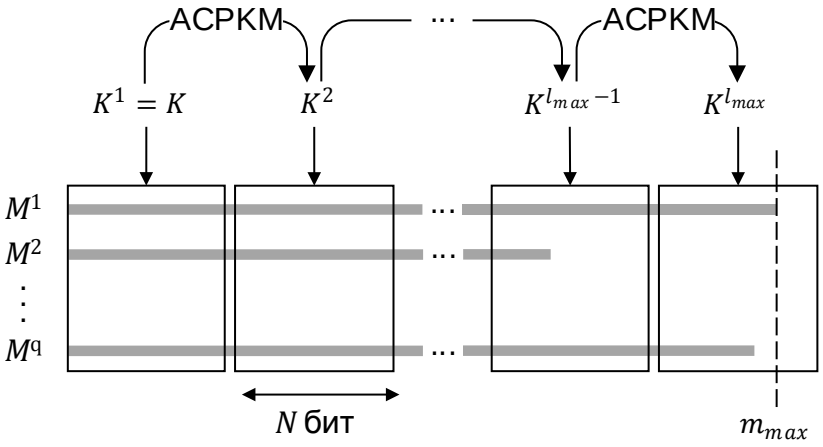

Рисунок 1 — Обработка сообщений в режиме CTR-ACPKM

Примечание — На Рисунке 1 через m_{max} обозначается максимальная длина сообщения, $l_{max} = \lceil m_{max}/N \rceil$.

При обработке сообщения M^j в режиме CTR-ACPKM сообщение разбивается на $l = \lceil |M^j|/N \rceil$ секций и представляется в виде $M^j = M_1^j \,|\, M_2^j \,|\, \dots \,|\, M_l^j$, где $M_i^j \in V_N$, $i = 1, 2, \dots, l-1$, $M_l^j \in V_w$, $w \leq N$. Первая секция каждого сообщения обрабатывается на секционном ключе K^1, который равен начальному ключу K. Для обработки i-ой секции каждого сообщения, $i = 2, \dots, l$, значение секционного ключа K^i вычисляется из значения ключа K^{i-1} с помощью механизма преобразования ключа ACPKM.

Результатом зашифрования сообщения M длины m в режиме CTR-ACPKM на начальном ключе K с длиной секции N и вектором инициализации IV является строка C, $|C| = |M|$, которая формируется по следующей схеме:

$$
\begin{gathered}
q = \lceil m/s \rceil,\ l = \lceil m/N \rceil; \\
M = P_1 \,|\, P_2 \,|\, \dots \,|\, P_q,\ P_i \in V_s,\ i = 1, 2, \dots, q-1,\ P_q \in V_r,\ r \leq s; \\
CTR_1 = IV \,|\, 0^{n/2}; \\
CTR_i = Inc_n(CTR_{i-1}),\ i = 2,3, \dots, q; \\
K^1 = K; \\
K^i = ACPKM(K^{i-1}),\ i = 2,3, \dots, l; \\
C_i = P_i \oplus MSB_{|P_i|}\left(E_{K^j}(CTR_i)\right),\ i = 1,2, \dots, q,\ j = \lceil i \cdot s/N \rceil;
\end{gathered}
\tag{1}
$$

$$C = C_1 \,|\, \dots \,|\, C_q.$$

При использовании режима CTR-ACPKM не требуется применение процедуры дополнения сообщения.

Длина m сообщения, обрабатываемого в режиме CTR-ACPKM, не должна превышать значения $2^{n/2-1} \cdot s$ бит.

Для обработки каждого отдельного сообщения в режиме CTR-ACPKM на одном начальном ключе K используется значение уникальной синхропосылки $IV \in V_{n/2}$.

4.1.1 Механизм преобразования ключа ACPKM

Механизм ACPKM принимает на вход ключ K^i длины 256 бит и преобразует его в ключ K^{i+1} той же длины. Механизм ACPKM определяется в зависимости от используемого блочного шифра Магма или Кузнечик, определенного в ГОСТ Р 34.12–2015, следующим образом:

$$K^{i+1} = ACPKM\left(K^i\right) = E_{K^i}(D_1) \,|\, \dots \,|\, E_{K^i}\left(D_J\right), \tag{2}$$

где $J = k/n, D_1 \,|\, \dots \,|\, D_J = D, D_1, \dots, D_J \in V_n$, а константа $D \in V_k$ задается следующим образом:

$$D = (80 \,|\, 81 \,|\, 82 \,|\, 83 \,|\, 84 \,|\, 85 \,|\, 86 \,|\, 87 \,|\, 88 \,|\, 89 \,|\, 8A \,|\, 8B \,|\, 8C \,|\, 8D \,|\, 8E \,|\, 8F \,|$$
$$90 \,|\, 91 \,|\, 92 \,|\, 93 \,|\, 94 \,|\, 95 \,|\, 96 \,|\, 97 \,|\, 98 \,|\, 99 \,|\, 9A \,|\, 9B \,|\, 9C \,|\, 9D \,|\, 9E \,|\, 9F).$$

4.2 Режим выработки имитовставки OMAC-ACPKM

В данном подразделе описан режим выработки имитовставки OMAC-ACPKM. В основе режима OMAC-ACPKM лежит режим выработки имитовставки, определенный в ГОСТ Р 34.13–2015, в который встраивается механизм преобразования ключа ACPKM-Master, описанный в 4.2.1.

При вычислении имитовставки сообщения в режиме OMAC-ACPKM каждое сообщение разбивается на секции, где под секцией понимается строка, состоящая из данных, обрабатываемых на одном секционном ключе до применения к нему механизма преобразования ACPKM-Master.

При формировании имитовставки в режиме OMAC-ACPKM начальный ключ K не используется непосредственно для обработки данных и задействуется только для порождения последовательности секционных ключей. Параметрами, определяющим порядок функционирования режима OMAC-ACPKM, является длина секции N и частота смены T^* мастер-ключей, обозначенных на Рисунке 2 через $K_1^*, K_2^*, \dots, K_{l_{max}}^*$. Параметры N и T^* измеряются в битах. Значения N и T^* фиксируются в рамках каждого конкретного протокола исходя из требований к производительности системы и нагрузке на ключ. Длина секции N должна быть кратна длине блока n используемого блочного шифра. Частота

смены ключа T^* должна быть кратна $k+n$. Дополнительным параметром режима OMAC-ACPKM является длина имитовставки s, $0 < s \leq n$, измеряющаяся в битах.

Процесс обработки сообщений в режиме OMAC-ACPKM схематично отражен на Рисунке 2:

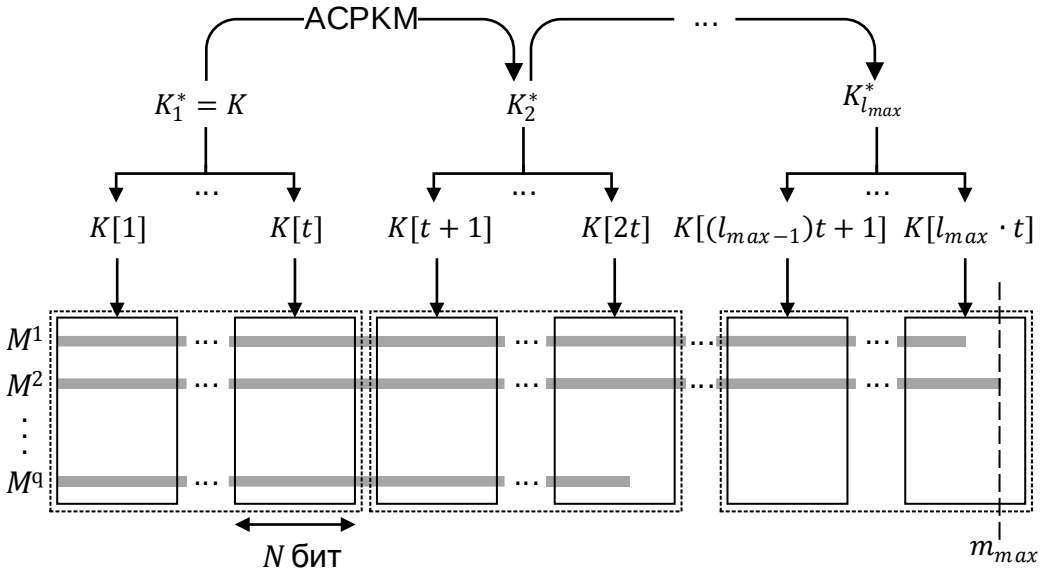

Рисунок 2 — Обработка сообщений в режиме OMAC-ACPKM

Примечание — На Рисунке 2 через m_{max} обозначается максимальная длина сообщения, $l_{max} = \lceil m_{max}/N \rceil$, $t = T^*/(k+n)$.

При обработке сообщения M^j длины m в режиме OMAC-ACPKM на начальном ключе K сообщение разбивается на $l = \lceil |M^j|/N \rceil$ секций и представляется в виде $M^j = M_1^j \,|\, M_2^j \,|\, \ldots \,|\, M_l^j$, где $M_i^j \in V_N$, $i = 1, 2, \ldots, l-1$, $M_l^j \in V_w$, $w \leq N$. Для обработки секции из начального ключа K с помощью механизма ACPKM-Master вырабатывается последовательность ключевого материала секций $K[1] = \{K^1, K_1^1\}$, $K[2] = \{K^2, K_1^2\}$,…, $K[l] = \{K^l, K_1^l\}$. Каждая i-я секция, $i = 1, 2, \ldots, l-1$, обрабатывается на ключе K^i. Для обработки l-ой секции используется ключ K^l и вспомогательный ключ K_1^l.

Результатом вычисления имитовставки сообщения M длины m в режиме OMAC-ACPKM на начальном ключе K с длиной секции N и частотой смены ключа T^* является строка MAC длины s, которая формируется по следующей схеме:

$$
\begin{gathered}
q = \lceil m/s \rceil,\ l = \lceil m/N \rceil; \\
M = P_1 \,|\, P_2 \,|\, \ldots \,|\, P_q,\ P_i \in V_n,\ i = 1, 2, \ldots, q-1,\ P_q \in V_r,\ r \leq n; \\
K^1 \,|\, K_1^1 \,|\, \ldots \,|\, K^l \,|\, K_1^l = ACPKM\text{-}Master(K, T^*, l); \\
K_2^l = \begin{cases} K_1^l \ll 1, & \text{если } MSB_1(K_1^l) = 0 \\ (K_1^l \ll 1) \oplus B_n, & \text{иначе} \end{cases}, \\
\text{где } B_{64} = 0^{59} \,|\, 11011,\ B_{128} = 0^{120} \,|\, 10000111;
\end{gathered}
\tag{3}
$$

$$K' = \begin{cases} K_1^l, & \text{если } r = n \\ K_2^l, & \text{если } r < n \end{cases};$$

$$C_0 = 0^n;$$

$$C_i = E_{K^j}(P_i \oplus C_{i-1}),\ i = 1,2,\dots,q-1,\ j = \lceil i \cdot n/N \rceil;$$

$$P_q^* = \begin{cases} P_q, & \text{если } r = n \\ P_q \,\|\, 1 \,\|\, 0^{n-1-r}, & \text{если } r < n \end{cases};$$

$$MAC = MSB_s\left(E_{K^l}\left(P_q^* \oplus C_{q-1} \oplus K'\right)\right).$$

Длина m сообщения, обрабатываемого в режиме OMAC-ACPKM, не должна превышать значения $2^{n/2-1} \cdot \frac{n \cdot N}{k+n}$ бит.

Очередная часть ключевого материала секции $K[i]$ может вычисляться по мере необходимости при поступлении данных на вход (может обеспечиваться потоковый режим обработки данных).

4.2.1 Механизм преобразования ключа ACPKM-Master

Механизм ACPKM-Master принимает на вход начальный ключ K длины 256 бит, параметр частоты смены мастер-ключа T^*, и количество элементов l в последовательности ключевого материала секций, которые необходимо выработать. Механизм ACPKM-Master задается в соответствии с выбранным блочным шифром Магма или Кузнечик, определенным в ГОСТ Р 34.12–2015, следующим образом:

$$ACPKM\text{-}Master(K, T^*, l) = K^1 \,\|\, K_1^1 \,\|\, \dots \,\|\, K^l \,\|\, K_1^l = CTR\text{-}ACPKM\left(K, T^*, 1^{n/2}, 0^{l\cdot(k+n)}\right), \qquad (4)$$

где $K^i \in V_{256}$, $K_1^i \in V_n$, $i \in \{1,2,\dots,\mathrm{l}\}$, $CTR\text{-}ACPKM(K, N, IV, M)$ является функцией зашифрования в режиме CTR-ACPKM, которая принимает на вход ключ K, размер секции N, значение вектора инициализации $IV \in V_{n/2}$ и сообщение M.

4.3 Пример порядка использования ключа при использовании режимов работы с механизмом преобразованием ключа

Для блочного шифра Магма при запрете на обработку более 4 МБ данных на одном ключе (без его преобразования) может быть определен следующий порядок использования режимов CTR-ACPKM и OMAC-ACPKM: размер секции равен 1 КБ, не допускается обработка более 4096 сообщений.

Для блочного шифра Кузнечик при запрете на обработку более 256 КБ данных на одном ключе (без его преобразования) может быть определен следующий порядок использования режимов CTR-ACPKM и OMAC-ACPKM: размер секции равен 4 КБ, не допускается обработка более 64 сообщений.

5 Алгоритмы экспорта KExp15 и импорта KImp15 ключа

В данном разделе описываются алгоритмы экспорта и импорта ключа, использующие в своей работе один из блочных шифров, определенных в ГОСТ Р 34.12–2015 (Магма или Кузнечик).

Входными параметрами алгоритма экспорта ключа KExp15 являются экспортируемый ключ K, ключ вычисления имитовставки K_{MAC}^{Exp}, ключ шифрования K_{ENC}^{Exp} ($K_{MAC}^{Exp}, K_{ENC}^{Exp} \in V_{256}$) и значение $IV \in V_{n/2}$. При этом должна обеспечиваться независимость ключей K_{MAC}^{Exp} и K_{ENC}^{Exp}. Экспортное представление ключа K формируется по следующей схеме:

1) Вычисляется значение имитовставки $KEYMAC$ длины n бит:

$$KEYMAC = OMAC\left(K_{MAC}^{Exp}, IV \middle| K\right), \tag{5}$$

где $OMAC(K, M)$ — функция выработки имитовставки, описанная в ГОСТ Р 34.13–2015, на ключе K от данных M.

2) Вычисляется значение $KEXP$:

$$KEXP = encKey \,\middle|\, encKeyMAC = CTR\left(K_{ENC}^{Exp}, IV, K \middle| KEYMAC\right), \tag{6}$$

где $|encKey| = |K|$, $|encKeyMAC| = |KEYMAC|$, $CTR(K, IV, M)$ — функция зашифрования в режиме гаммирования с длиной блока гаммы $s = n$, описанном в ГОСТ Р 34.13–2015, принимающая на вход ключ K, вектор инициализации IV и данные M.

3) Результат работы алгоритма экспорта ключа K называется экспортным представлением ключа K, обозначается через $KExp15\left(K, K_{MAC}^{Exp}, K_{ENC}^{Exp}, IV\right)$ и полагается равным строке $KEXP$:

$$KExp15\left(K, K_{MAC}^{Exp}, K_{ENC}^{Exp}, IV\right) = KEXP. \tag{7}$$

Импорт ключа в алгоритме KImp15 (получение ключа K по экспортному представлению $KEXP$ с помощью ключей K_{MAC}^{Exp}, $K_{ENC}^{Exp} \in V_{256}$ и значения $IV \in V_{n/2}$) осуществляется по следующей схеме:

1) Набор $KEXP$ расшифровывается на ключе K_{ENC}^{Exp} в с соответствии с режимом гаммирования с длиной блока гаммы s, равной длине блока n, описанным в ГОСТ Р 34.13–2015, при этом вектор инициализации полагается равным IV. Строка $K \,\big|\, KEYMAC$ полагается равной результату расшифрования.

2) Вычисляется значение имитовставки длины n бит в с соответствии с режимом выработки имитовставки, описанным в ГОСТ Р 34.13–2015, от данных $IV \,\big|\, K$ на ключе K_{MAC}^{Exp}. Если результат отличен от $KEYMAC$, возвращается ошибка.

3) Результат работы алгоритма импорта ключа от его экспортного представления обозначается через $KImp15\left(KEXP, K_{MAC}^{Exp}, K_{ENC}^{Exp}, IV\right)$ и полагается равным строке K:

$$KImp15\left(KEXP, K_{MAC}^{Exp}, K_{ENC}^{Exp}, IV\right) = K. \quad (8)$$

Приложение А

(справочное)

Контрольные примеры для режимов работы блочных шифров с преобразованием ключа

Данное приложение носит справочный характер и не является частью настоящих рекомендаций.

В данном приложении содержатся контрольные примеры работы режимов работы блочных шифров с преобразованием ключа, описанных в 0. Параметры s, m, N и T^* выбраны из соображений демонстрации особенностей работы алгоритмов.

Все данные приведены в виде байтовых строк. Битовые строки, имеющие длину, кратную 8, преобразуются в байтовые строки и обратно в прямом порядке слева направо. Соседние байты отделяются друг от друга пробелом. Например, битовой строке `1100101100011000` соответствует байтовая строка `CB 18`.

А.1 Режим шифрования CTR-ACPKM для шифра Магма

В настоящем разделе приведены тестовые примеры работы режима шифрования CTR-ACPKM для шифра Магма со следующими входными данными:

- длина блока n: 64 бита;
- длина блока гаммы s: 64 бита;
- размер секции N: 128 бит;
- ключ K:

```
88 99 AA BB CC DD EE FF 00 11 22 33 44 55 66 77
FE DC BA 98 76 54 32 10 01 23 45 67 89 AB CD EF
```

- вектор инициализации IV:

```
12 34 56 78
```

- открытый текст M:

```
11 22 33 44 55 66 77 00 FF EE DD CC BB AA 99 88
00 11 22 33 44 55 66 77 88 99 AA BB CC EE FF 0A
11 22 33 44 55 66 77 88 99 AA BB CC EE FF 0A 00
22 33 44 55 66 77 88 99
```

Сообщение M разбивается на 4 секции M_1, M_2, M_3, M_4, каждая из которых разбивается на блоки. Обработка данных производится следующим образом:

Т а б л и ц а А.1.1 – Обработка секции M_1 в режиме CTR-ACPKM для шифра Магма

Секция M_1	`11 22 33 44 55 66 77 00 FF EE DD CC BB AA 99 88`
Ключ K^1	`88 99 AA BB CC DD EE FF 00 11 22 33 44 55 66 77` `FE DC BA 98 76 54 32 10 01 23 45 67 89 AB CD EF`
Обработка 1-го блока:	

Счетчик CTR_1	12 34 56 78 00 00 00 00
Блок гаммы	3B 9A 2E AA BE 78 3B AB
Блок открытого текста P_1	11 22 33 44 55 66 77 00
Блок шифртекста C_1	2A B8 1D EE EB 1E 4C AB
Обработка 2-го блока:	
Счетчик CTR_2	12 34 56 78 00 00 00 01
Блок гаммы	97 0F D9 08 06 C1 0D 62
Блок открытого текста P_2	FF EE DD CC BB AA 99 88
Блок шифртекста C_2	68 E1 04 C4 BD 6B 94 EA

Т а б л и ц а А.1.2 – Обработка секции M_2 в режиме CTR-ACPKM для шифра Магма

Секция M_2	00 11 22 33 44 55 66 77 88 99 AA BB CC EE FF 0A
Ключ K^2	86 3E A0 17 84 2C 3D 37 2B 18 A8 5A 28 E2 31 7D 74 BE FC 10 77 20 DE 0C 9E 8A B9 74 AB D0 0C A0
Обработка 3-го блока:	
Счетчик CTR_3	12 34 56 78 00 00 00 02
Блок гаммы	C7 3D 45 9C 28 7B 3D 1C
Блок открытого текста P_3	00 11 22 33 44 55 66 77
Блок шифртекста C_3	C7 2C 67 AF 6C 2E 5B 6B
Обработка 4-го блока:	
Счетчик CTR_4	12 34 56 78 00 00 00 03
Блок гаммы	86 36 1C AC BC 1F 4C 24
Блок открытого текста P_4	88 99 AA BB CC EE FF 0A
Блок шифртекста C_4	0E AF B6 17 70 F1 B3 2E

Т а б л и ц а А.1.3 – Обработка секции M_3 в режиме CTR-ACPKM для шифра Магма

Секция M_3	11 22 33 44 55 66 77 88 99 AA BB CC EE FF 0A 00
Ключ K^3	49 A5 E2 67 7D E5 55 98 2B 8A D5 E8 26 65 2D 17 EE C8 47 BF 5B 39 97 A8 1C F7 FE 7F 11 87 BD 27
Обработка 5-го блока:	
Счетчик CTR_5	12 34 56 78 00 00 00 04
Блок гаммы	B0 8C 42 50 CB 8B 64 0A
Блок открытого текста P_5	11 22 33 44 55 66 77 88
Блок шифртекста C_5	A1 AE 71 14 9E ED 13 82
Обработка 6-го блока:	
Счетчик CTR_6	12 34 56 78 00 00 00 05
Блок гаммы	32 7E DC D4 E8 8D E6 6F
Блок открытого текста P_6	99 AA BB CC EE FF 0A 00
Блок шифртекста C_6	AB D4 67 18 06 72 EC 6F

Т а б л и ц а А.1.4 – Обработка секции M_4 в режиме CTR-ACPKM для шифра Магма

Секция M_4	22 33 44 55 66 77 88 99
Ключ K^4	32 56 BF 3F 97 B5 66 74 26 A9 FB 1C 5E AA BE 41 89 3C CD D5 A8 68 F9 B6 3B 0A A9 07 20 FA 43 C4
Обработка 7-го блока:	
Счетчик CTR_7	12 34 56 78 00 00 00 06
Блок гаммы	A6 91 B5 0E 59 BD FA 58
Блок открытого текста P_7	22 33 44 55 66 77 88 99
Блок шифртекста C_7	84 A2 F1 5B 3F CA 72 C1

Результатом зашифрования открытого текста M в режиме CTR-ACPKM в данном случае является строка $C_1 \| C_2 \| \dots \| C_7$:

2A B8 1D EE EB 1E 4C AB 68 E1 04 C4 BD 6B 94 EA
C7 2C 67 AF 6C 2E 5B 6B 0E AF B6 17 70 F1 B3 2E
A1 AE 71 14 9E ED 13 82 AB D4 67 18 06 72 EC 6F
84 A2 F1 5B 3F CA 72 C1.

А.2 Режим шифрования CTR-ACPKM для шифра Кузнечик

В настоящем разделе приведены тестовые примеры работы режима шифрования CTR-ACPKM для шифра Кузнечик со следующими входными данными:

- длина блока n: 128 бит;
- длина блока гаммы s: 128 бит;
- размер секции N: 256 бит;
- ключ K:

88 99 AA BB CC DD EE FF 00 11 22 33 44 55 66 77
FE DC BA 98 76 54 32 10 01 23 45 67 89 AB CD EF;

- вектор инициализации IV:

12 34 56 78 90 AB CE F0;

- открытый текст M:

11 22 33 44 55 66 77 00 FF EE DD CC BB AA 99 88
00 11 22 33 44 55 66 77 88 99 AA BB CC EE FF 0A
11 22 33 44 55 66 77 88 99 AA BB CC EE FF 0A 00
22 33 44 55 66 77 88 99 AA BB CC EE FF 0A 00 11
33 44 55 66 77 88 99 AA BB CC EE FF 0A 00 11 22
44 55 66 77 88 99 AA BB CC EE FF 0A 00 11 22 33
55 66 77 88 99 AA BB CC EE FF 0A 00 11 22 33 44.

Сообщение M разбивается на 4 секции M_1, M_2, M_3, M_4, каждая из которых разбивается на блоки. Обработка данных производится следующим образом:

Т а б л и ц а А.2.1 – Обработка секции M_1 в режиме CTR-ACPKM для шифра Кузнечик

Секция M_1	11 22 33 44 55 66 77 00 FF EE DD CC BB AA 99 88 00 11 22 33 44 55 66 77 88 99 AA BB CC EE FF 0A

Ключ K^1	88 99 AA BB CC DD EE FF 00 11 22 33 44 55 66 77 FE DC BA 98 76 54 32 10 01 23 45 67 89 AB CD EF
Обработка 1-го блока:	
Счетчик CTR_1	12 34 56 78 90 AB CE F0 00 00 00 00 00 00 00 00
Блок гаммы	E0 B7 EB FA 94 68 A6 DB 2A 95 82 6E FB 17 38 30
Блок открытого текста P_1	11 22 33 44 55 66 77 00 FF EE DD CC BB AA 99 88
Блок шифртекста C_1	F1 95 D8 BE C1 0E D1 DB D5 7B 5F A2 40 BD A1 B8
Обработка 2-го блока:	
Счетчик CTR_2	12 34 56 78 90 AB CE F0 00 00 00 00 00 00 00 01
Блок гаммы	85 FF C5 00 B2 F4 58 2A 7B A5 4E 08 F0 AB 21 EE
Блок открытого текста P_2	00 11 22 33 44 55 66 77 88 99 AA BB CC EE FF 0A
Блок шифртекста C_2	85 EE E7 33 F6 A1 3E 5D F3 3C E4 B3 3C 45 DE E4

Т а б л и ц а А.2.2 – Обработка секции M_2 в режиме CTR-ACPKM для шифра Кузнечик

Секция M_2	11 22 33 44 55 66 77 88 99 AA BB CC EE FF 0A 00 22 33 44 55 66 77 88 99 AA BB CC EE FF 0A 00 11
Ключ K^2	26 66 ED 40 AE 68 78 11 74 5C A0 B4 48 F5 7A 7B 39 0A DB 57 80 30 7E 8E 96 59 AC 40 3A E6 0C 60
Обработка 3-го блока:	
Счетчик CTR_3	12 34 56 78 90 AB CE F0 00 00 00 00 00 00 00 02
Блок гаммы	5A EC D8 CB 31 09 3B DD 99 BD BD EB B0 7A E2 00
Блок открытого текста P_3	11 22 33 44 55 66 77 88 99 AA BB CC EE FF 0A 00
Блок шифртекста C_3	4B CE EB 8F 64 6F 4C 55 00 17 06 27 5E 85 E8 00
Обработка 4-го блока:	
Счетчик CTR_4	12 34 56 78 90 AB CE F0 00 00 00 00 00 00 00 03
Блок гаммы	7A 4F 09 A0 0E A7 1C A0 94 F3 F8 41 2F 8A 50 57
Блок открытого текста P_4	22 33 44 55 66 77 88 99 AA BB CC EE FF 0A 00 11
Блок шифртекста C_4	58 7C 4D F5 68 D0 94 39 3E 48 34 AF D0 80 50 46

Т а б л и ц а А.2.3 – Обработка секции M_3 в режиме CTR-ACPKM для шифра Кузнечик

Секция M_3	33 44 55 66 77 88 99 AA BB CC EE FF 0A 00 11 22 44 55 66 77 88 99 AA BB CC EE FF 0A 00 11 22 33
Ключ K^3	BB 3D D5 40 2E 99 9B 7A 3D EB B0 DB 45 44 8E C5 30 F0 73 65 DF EE 3A BA 84 15 F7 7A C8 F3 4C E8
Обработка 5-го блока:	
Счетчик CTR_5	12 34 56 78 90 AB CE F0 00 00 00 00 00 00 00 04
Блок гаммы	FC 74 A0 10 F1 26 75 4B A7 30 82 CE 61 8A 98 4C
Блок открытого текста P_5	33 44 55 66 77 88 99 AA BB CC EE FF 0A 00 11 22
Блок шифртекста C_5	CF 30 F5 76 86 AE EC E1 1C FC 6C 31 6B 8A 89 6E

Обработка 6-го блока:	
Счетчик CTR_6	12 34 56 78 90 AB CE F0 00 00 00 00 00 00 00 05
Блок гаммы	9B A8 61 9B 09 AF 9C FD C0 A1 C4 7E 34 32 34 0D
Блок открытого текста P_6	44 55 66 77 88 99 AA BB CC EE FF 0A 00 11 22 33
Блок шифртекста C_6	DF FD 07 EC 81 36 36 46 0C 4F 3B 74 34 23 16 3E

Т а б л и ц а А.2.4 – Обработка секции M_4 в режиме CTR-ACPKM для шифра Кузнечик

Секция M_4	55 66 77 88 99 AA BB CC EE FF 0A 00 11 22 33 44
Ключ K^4	23 36 2F D5 53 CA D2 17 82 99 A5 B5 A2 D4 72 2E 3B B8 3C 73 0A 8B F5 7C E2 DD 00 40 17 F8 C5 65
Обработка 7-го блока:	
Счетчик CTR_7	12 34 56 78 90 AB CE F0 00 00 00 00 00 00 00 06
Блок гаммы	31 6F DE 4A 1B 50 73 18 87 2D 2B E7 EA F4 ED 19
Блок открытого текста P_7	55 66 77 88 99 AA BB CC EE FF 0A 00 11 22 33 44
Блок шифртекста C_7	64 09 A9 C2 82 FA C8 D4 69 D2 21 E7 FB D6 DE 5D

Результатом зашифрования открытого текста M в режиме CTR-ACPKM в данном случае является строка $C_1 \mid C_2 \mid \ldots \mid C_7$:

```
F1 95 D8 BE C1 0E D1 DB D5 7B 5F A2 40 BD A1 B8
85 EE E7 33 F6 A1 3E 5D F3 3C E4 B3 3C 45 DE E4
4B CE EB 8F 64 6F 4C 55 00 17 06 27 5E 85 E8 00
58 7C 4D F5 68 D0 94 39 3E 48 34 AF D0 80 50 46
CF 30 F5 76 86 AE EC E1 1C FC 6C 31 6B 8A 89 6E
DF FD 07 EC 81 36 36 46 0C 4F 3B 74 34 23 16 3E
64 09 A9 C2 82 FA C8 D4 69 D2 21 E7 FB D6 DE 5D.
```

А.3 Режим вычисления имитовставки сообщения OMAC-ACPKM для шифра Магма

В настоящем разделе приведены тестовые примеры работы режима шифрования OMAC-ACPKM для шифра Магма со следующими входными данными:

- длина блока n: 64 бита;
- длина блока гаммы s: 64 бита;
- размер секции N: 128 бит;
- частота смены ключа T^*: 640 бит;
- ключ K:

```
88 99 AA BB CC DD EE FF 00 11 22 33 44 55 66 77
FE DC BA 98 76 54 32 10 01 23 45 67 89 AB CD EF.
```

А.3.1. Пример работы режима OMAC-ACPKM для шифра Магма с открытым текстом длины 1,5 блока

Открытый текст M длины 1,5 блока:

```
11 22 33 44 55 66 77 00 FF EE DD CC
```

Сообщение M состоит из одной секции M_1, которая разбивается на блоки.

При формировании ключевого материала вырабатывается строка $K^1 \,|\, K_1^1 = ACPKM\text{-}Master(K, T^*, 1)$:

```
0D F2 F5 27 3D A3 28 93 2A C4 9D 81 D3 6B 25 58
A5 0D BF 9B BC AC 74 A6 14 B2 CC B2 F1 CB CD 8A
70 63 8E 3D E8 B3 57 1E.
```

Обработка данных производится следующим образом:

Т а б л и ц а А.3.1.1 – Обработка секции M_1 в режиме OMAC-ACPKM для шифра Магма

Секция M_1	11 22 33 44 55 66 77 00 FF EE DD CC
Ключ K^1	0D F2 F5 27 3D A3 28 93 2A C4 9D 81 D3 6B 25 58 A5 0D BF 9B BC AC 74 A6 14 B2 CC B2 F1 CB CD 8A
Ключ K_1^1	70 63 8E 3D E8 B3 57 1E
Обработка 1-го блока:	
Блок открытого текста P_1	11 22 33 44 55 66 77 00
Входной блок ($P_1 \oplus C_0$)	11 22 33 44 55 66 77 00
Выходной блок C_1	A0 2B D0 1D 04 5A 9E 45
Обработка 2-го блока:	
Ключ K'	E0 C7 1C 7B D1 66 AE 3C
Блок открытого текста P_2^*	FF EE DD CC 80 00 00 00
Вх. блок ($P_2^* \oplus C_1 \oplus K'$)	BF 02 11 AA 55 3C 30 79
Выходной блок C_2	A0 54 0E 37 30 AC BC F3

Результатом вычисления имитовставки сообщения M в режиме OMAC-ACPKM в данном случае является строка C_2:

```
A0 54 0E 37 30 AC BC F3.
```

А.3.2. Пример работы режима OMAC-ACPKM для шифра Магма с открытым текстом длины 5 блоков

Открытый текст M длины 5 блоков:

```
11 22 33 44 55 66 77 00 FF EE DD CC BB AA 99 88
00 11 22 33 44 55 66 77 88 99 AA BB CC EE FF 0A
11 22 33 44 55 66 77 88
```

Сообщение M разбивается на 3 секции M_1, M_2, M_3, каждая из которых разбивается на блоки.

При формировании ключевого материала вырабатывается строка $K^1 \,|\, K_1^1 \,|\, K^2 \,|\, K_1^2 \,|\, K^3 \,|\, K_1^3 = ACPKM\text{-}Master(K, T^*, 3)$:

```
0D F2 F5 27 3D A3 28 93 2A C4 9D 81 D3 6B 25 58
A5 0D BF 9B BC AC 74 A6 14 B2 CC B2 F1 CB CD 8A
70 63 8E 3D E8 B3 57 1E 8D 38 26 D5 5E 63 A1 67
E2 40 66 40 54 7B 9F 1F 5F 2B 43 61 2A AE AF DA
18 0B AC 86 04 DF A6 FE 53 C2 CE 27 0E 9C 9F 52
```

68 D0 FD BF E1 A3 BD D9 BE 5B 96 D0 A1 20 23 48
6E F1 71 0F 92 4A E0 31 30 52 CB 5F CA 0B 79 1E
1B AB E8 57 6D 0F E3 A8.

Обработка данных производится следующим образом:

Т а б л и ц а А.3.2.1 – Обработка секции M_1 в режиме OMAC-ACPKM для шифра Магма

Секция M_1	11 22 33 44 55 66 77 00 FF EE DD CC BB AA 99 88
Ключ K^1	0D F2 F5 27 3D A3 28 93 2A C4 9D 81 D3 6B 25 58 A5 0D BF 9B BC AC 74 A6 14 B2 CC B2 F1 CB CD 8A
Обработка 1-го блока:	
Блок открытого текста P_1	11 22 33 44 55 66 77 00
Входной блок ($P_1 \oplus C_0$)	11 22 33 44 55 66 77 00
Выходной блок C_1	A0 2B D0 1D 04 5A 9E 45
Обработка 2-го блока:	
Блок открытого текста P_2	FF EE DD CC BB AA 99 88
Входной блок ($P_2 \oplus C_1$)	5F C5 0D D1 BF F0 07 CD
Выходной блок C_2	1D 61 FD 38 6F E5 8E 2F

Т а б л и ц а А.3.2.2 – Обработка секции M_2 в режиме OMAC-ACPKM для шифра Магма

Секция M_2	00 11 22 33 44 55 66 77 88 99 AA BB CC EE FF 0A
Ключ K^2	8D 38 26 D5 5E 63 A1 67 E2 40 66 40 54 7B 9F 1F 5F 2B 43 61 2A AE AF DA 18 0B AC 86 04 DF A6 FE
Обработка 3-го блока:	
Блок открытого текста P_3	00 11 22 33 44 55 66 77
Входной блок ($P_3 \oplus C_2$)	1D 70 DF 0B 2B B0 E8 58
Выходной блок C_3	E7 9A E5 A1 8F 11 24 6B
Обработка 4-го блока:	
Блок открытого текста P_4	88 99 AA BB CC EE FF 0A
Входной блок ($P_4 \oplus C_3$)	6F 03 4F 1A 43 FF DB 61
Выходной блок C_4	A3 1E 9B 72 1F 64 88 E8

Т а б л и ц а А.3.2.3 – Обработка секции M_3 в режиме OMAC-ACPKM для шифра Магма

Секция M_3	11 22 33 44 55 66 77 88
Ключ K^3	68 D0 FD BF E1 A3 BD D9 BE 5B 96 D0 A1 20 23 48 6E F1 71 0F 92 4A E0 31 30 52 CB 5F CA 0B 79 1E
Ключ K_1^3	1B AB E8 57 6D 0F E3 A8
Обработка 5-го блока:	
Ключ K'	1B AB E8 57 6D 0F E3 A8
Блок открытого текста P_5	11 22 33 44 55 66 77 88
Вх. блок ($P_5^* \oplus C_4 \oplus K'$)	A9 97 40 61 27 0D 1C C8

Выходной блок C_5	34 00 8D AD 54 96 BB 8E

Результатом вычисления имитовставки сообщения M в режиме OMAC-ACPKM в данном случае является строка C_5:

34 00 8D AD 54 96 BB 8E.

А.4 Режим вычисления имитовставки сообщения OMAC-ACPKM для шифра Кузнечик

В настоящем разделе приведены тестовые примеры работы режима шифрования OMAC-ACPKM для шифра Кузнечик со следующими входными данными:

- длина блока n: 128 бит;
- длина блока гаммы s: 128 бит;
- размер секции N: 256 бит;
- частота смены ключа T^*: 768 бит;
- ключ K:

88 99 AA BB CC DD EE FF 00 11 22 33 44 55 66 77
FE DC BA 98 76 54 32 10 01 23 45 67 89 AB CD EF.

А.4.1. Пример работы режима OMAC-ACPKM для шифра Кузнечик с открытым текстом длины 1,5 блока

Открытый текст M длины 1,5 блока:

11 22 33 44 55 66 77 00 FF EE DD CC BB AA 99 88
00 11 22 33 44 55 66 77.

Сообщение M состоит из одной секции M_1, которая разбивается на блоки.

При формировании ключевого материала вырабатывается строка $K^1 \,|\, K_1^1 = ACPKM\text{-}Master(K, T^*, 1)$:

0C AB F1 F2 EF BC 4A C1 60 48 DF 1A 24 C6 05 B2
C0 D1 67 3D 75 86 A8 EC 0D D4 2C 45 A4 F9 5B AE
0F 2E 26 17 E4 71 48 68 0F C3 E6 17 8D F2 C1 37.

Обработка данных производится следующим образом:

Т а б л и ц а А.4.1.1 – Обработка секции M_1 в режиме OMAC-ACPKM для шифра Кузнечик

Секция M_1	11 22 33 44 55 66 77 00 FF EE DD CC BB AA 99 88
Ключ K^1	0C AB F1 F2 EF BC 4A C1 60 48 DF 1A 24 C6 05 B2 C0 D1 67 3D 75 86 A8 EC 0D D4 2C 45 A4 F9 5B AE
Ключ K_1^1	0F 2E 26 17 E4 71 48 68 0F C3 E6 17 8D F2 C1 37
Обработка 1-го блока:	
Блок открытого текста P_1	11 22 33 44 55 66 77 00 FF EE DD CC BB AA 99 88
Входной блок ($P_1 \oplus C_0$)	11 22 33 44 55 66 77 00 FF EE DD CC BB AA 99 88
Выходной блок C_1	DD 01 38 F4 86 C7 07 DA F7 F4 57 76 6D A4 78 B0
Обработка 2-го блока:	

Ключ K'	1E 5C 4C 2F C8 E2 90 D0 1F 87 CC 2F 1B E5 82 6E
Блок открытого текста P_2^*	00 11 22 33 44 55 66 77 80 00 00 00 00 00 00 00
Вх. блок ($P_2^* \oplus C_1 \oplus K'$)	C3 4C 56 E8 0A 70 F1 7D 68 73 9B 59 76 41 FA DE
Выходной блок C_2	B5 36 7F 47 B6 2B 99 5E EB 2A 64 8C 58 43 14 5E

Результатом вычисления имитовставки сообщения M в режиме OMAC-ACPKM в данном случае является строка C_2:

B5 36 7F 47 B6 2B 99 5E EB 2A 64 8C 58 43 14 5E.

А.4.2. Пример работы режима OMAC-ACPKM для шифра Кузнечик с открытым текстом длины 5 блоков

Открытый текст M длины 5 блоков:

11 22 33 44 55 66 77 00 FF EE DD CC BB AA 99 88
00 11 22 33 44 55 66 77 88 99 AA BB CC EE FF 0A
11 22 33 44 55 66 77 88 99 AA BB CC EE FF 0A 00
22 33 44 55 66 77 88 99 AA BB CC EE FF 0A 00 11
33 44 55 66 77 88 99 AA BB CC EE FF 0A 00 11 22

Сообщение M разбивается на 3 секции M_1, M_2, M_3, каждая из которых разбивается на блоки. При формировании ключевого материала вырабатывается строка $K^1 \,|\, K_1^1 \,|\, K^2 \,|\, K_1^2 \,|\, K^3 \,|\, K_1^3 = ACPKM\text{-}Master(K, T^*, 3)$:

0C AB F1 F2 EF BC 4A C1 60 48 DF 1A 24 C6 05 B2
C0 D1 67 3D 75 86 A8 EC 0D D4 2C 45 A4 F9 5B AE
0F 2E 26 17 E4 71 48 68 0F C3 E6 17 8D F2 C1 37
C9 DD A8 9C FF A4 91 FE AD D9 B3 EA B7 03 BB 31
BC 7E 92 7F 04 94 72 9F 51 B4 9D 3D F9 C9 46 08
00 FB BC F5 ED EE 61 0E A0 2F 01 09 3C 7B C7 42
D7 D6 27 15 01 B1 77 77 52 63 C2 A3 49 5A 83 18
A8 1C 79 A0 4F 29 66 0E A3 FD A8 74 C6 30 79 9E
14 2C 57 79 14 FE A9 0D 3B C2 50 2E 83 36 85 D9.

Обработка данных производится следующим образом:

Т а б л и ц а А.4.2.1 – Обработка секции M_1 в режиме OMAC-ACPKM для шифра Кузнечик

Секция M_1	11 22 33 44 55 66 77 00 FF EE DD CC BB AA 99 88 00 11 22 33 44 55 66 77 88 99 AA BB CC EE FF 0A
Ключ K^1	0C AB F1 F2 EF BC 4A C1 60 48 DF 1A 24 C6 05 B2 C0 D1 67 3D 75 86 A8 EC 0D D4 2C 45 A4 F9 5B AE
Обработка 1-го блока:	
Блок открытого текста P_1	11 22 33 44 55 66 77 00 FF EE DD CC BB AA 99 88
Входной блок ($P_1 \oplus C_0$)	11 22 33 44 55 66 77 00 FF EE DD CC BB AA 99 88
Выходной блок C_1	DD 01 38 F4 86 C7 07 DA F7 F4 57 76 6D A4 78 B0
Обработка 2-го блока:	
Блок открытого текста P_2	00 11 22 33 44 55 66 77 88 99 AA BB CC EE FF 0A

Входной блок ($P_2 \oplus C_1$)	DD 10 1A C7 C2 92 61 AD 7F 6D FD CD A1 4A 87 BA
Выходной блок C_2	9C 23 7F 18 85 F8 07 64 0B 32 5B 50 16 AB EC AF

Т а б л и ц а А.4.2.2 – Обработка секции M_2 в режиме OMAC-ACPKM для шифра Кузнечик

Секция M_2	11 22 33 44 55 66 77 88 99 AA BB CC EE FF 0A 00 22 33 44 55 66 77 88 99 AA BB CC EE FF 0A 00 11
Ключ K^2	C9 DD A8 9C FF A4 91 FE AD D9 B3 EA B7 03 BB 31 BC 7E 92 7F 04 94 72 9F 51 B4 9D 3D F9 C9 46 08
Обработка 3-го блока:	
Блок открытого текста P_3	11 22 33 44 55 66 77 88 99 AA BB CC EE FF 0A 00
Входной блок ($P_3 \oplus C_2$)	8D 01 4C 5C D0 9E 70 EC 92 98 E0 9C F8 54 E6 AF
Выходной блок C_3	2F 08 DE 89 F1 34 1B F9 1F 24 2F 88 94 E5 4E 6F
Обработка 4-го блока:	
Блок открытого текста P_4	22 33 44 55 66 77 88 99 AA BB CC EE FF 0A 00 11
Входной блок ($P_4 \oplus C_3$)	0D 3B 9A DC 97 43 93 60 B5 9F E3 66 6B EF 4E 7E
Выходной блок C_4	80 2C DF AC 40 FA 27 C2 FB 9B 2E 70 22 39 1D 84

Т а б л и ц а А.4.2.3 – Обработка секции M_3 в режиме OMAC-ACPKM для шифра Кузнечик

Секция M_3	33 44 55 66 77 88 99 AA BB CC EE FF 0A 00 11 22
Ключ K^3	D7 D6 27 15 01 B1 77 77 52 63 C2 A3 49 5A 83 18 A8 1C 79 A0 4F 29 66 0E A3 FD A8 74 C6 30 79 9E
Ключ K_1^3	14 2C 57 79 14 FE A9 0D 3B C2 50 2E 83 36 85 D9
Обработка 5-го блока:	
Ключ K'	14 2C 57 79 14 FE A9 0D 3B C2 50 2E 83 36 85 D9
Блок открытого текста P_5	33 44 55 66 77 88 99 AA BB CC EE FF 0A 00 11 22
Вх. блок ($P_5^* \oplus C_4 \oplus K'$)	A7 44 DD B3 23 8C 17 65 7B 95 90 A1 AB 0F 89 7F
Выходной блок C_5	FB B8 DC EE 45 BE A6 7C 35 F5 8C 57 00 89 8E 5D

Результатом вычисления имитовставки сообщения M в режиме OMAC-ACPKM в данном случае является строка C_5:

FB B8 DC EE 45 BE A6 7C 35 F5 8C 57 00 89 8E 5D.

Приложение В
(справочное)

Контрольные примеры работы алгоритмов экспорта и импорта ключа

Данное приложение носит справочный характер и не является частью настоящих рекомендаций.

В данном приложении содержатся контрольные примеры работы алгоритмов экспорта и импорта ключей, описанных в 5, со следующими входными данными:

- ключ K:
88 99 AA BB CC DD EE FF 00 11 22 33 44 55 66 77
FE DC BA 98 76 54 32 10 01 23 45 67 89 AB CD EF;

- ключ K_{MAC}^{Exp}:
08 09 0A 0B 0C 0D 0E 0F 00 01 02 03 04 05 06 07
10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F;

- ключ K_{ENC}^{Exp}:
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F
38 39 3A 3B 3C 3D 3E 3F 30 31 32 33 34 35 36 37.

В.1 Алгоритмы экспорта и импорта ключа для шифра Магма

Вектор инициализации IV:
67 BE D6 54.

$KEYMAC$:
75 A7 66 18 E9 0F 49 73.

$KEXP = KExp15(K, K_{MAC}^{Exp}, K_{ENC}^{Exp}, IV)$:
CF D5 A1 2D 5B 81 B6 E1 E9 9C 91 6D 07 90 0C 6A
C1 27 03 FB 3A BD ED 55 56 7B F3 74 2C 89 9C 75
5D AF E7 B4 2E 3A 8B D9.

В.2 Алгоритмы экспорта и импорта ключа для шифра Кузнечик

Вектор инициализации IV:
09 09 47 2D D9 F2 6B E8.

$KEYMAC$:
10 02 2A DE 94 EE 55 B4 34 D2 07 7F 5A 13 AF F4.

$KEXP = KExp15(K, K_{MAC}^{Exp}, K_{ENC}^{Exp}, IV)$:
E3 61 84 E8 4E 8D 73 6F F3 6C C2 E5 AE 06 5D C6

56 B2 3C 20 F5 49 B0 2F DF F8 8E 1F 3F 30 D8 C2
9A 53 F3 CA 55 4D BA D8 0D E1 52 B9 A4 62 5B 32.

УДК 681.3.06:006.354 ОКС 35. 040 ОКСТУ 5002 П85

Ключевые слова: криптографические протоколы, режимы, шифрование, имитовставка, ключ, экспорт ключа

Авторы документа

Директор по научной работе
ООО «КРИПТО-ПРО»,
Попов В.О.
vpopov@cryptopro.ru

Начальник отдела защиты информации
ООО «КРИПТО-ПРО»,
Смышляев С.В.
svs@cryptopro.ru

Заместитель начальника отдела защиты информации
ООО «КРИПТО-ПРО»,
Ошкин И.Б.
oshkin@cryptopro.ru

Ведущий инженер-аналитик
ООО «КРИПТО-ПРО»,
Алексеев Е.К.
alekseev@cryptopro.ru

Инженер-программист
ООО «КРИПТО-ПРО»,
Смышляева Е.С.
ess@cryptopro.ru

Инженер-аналитик
ООО «КРИПТО-ПРО»,
Ахметзянова Л.Р.
lah@cryptopro.ru

Инженер-аналитик
ООО «КРИПТО-ПРО»,
Шарапова А.Д.
shadshad@cryptopro.ru