ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ

Р 1323565.1.026— 2019

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Режимы работы блочных шифров, реализующие аутентифицированное шифрование

Издание официальное

Москва
Стандартинформ
2019

gost.e-ecolog.ru

Предисловие

1 РАЗРАБОТАНЫ Центром защиты информации и специальной связи ФСБ России при участии Общества 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 6 сентября 2019 г. № 646-ст

4 ВВЕДЕНЫ ВПЕРВЫЕ

*Правила применения настоящих рекомендаций установлены в статье 26 Федерального закона от 29 июня 2015 г. № 162-ФЗ «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 (*gost.e-ecolog.ru

© Стандартинформ, оформление, 2019

Настоящие рекомендации не могут быть полностью или частично воспроизведены, тиражированы и распространены в качестве официального издания без разрешения Федерального агентства по техническому регулированию и метрологии

Содержание

1 Область применения 1
2 Нормативные ссылки 1
3 Обозначения и сокращения 1
3.1 Обозначения 1
3.2 Сокращения 3
4 Общие положения 3
5 Режим MGM 3
5.1 Зашифрование 3
5.2 Расшифрование 5
Приложение А (справочное) 7
Приложение Б (справочное) 8
Б.1 Пример для блочного шифра «Кузнечик» 8
Б.2 Пример для блочного шифра «Магма» 9

Введение

Настоящие рекомендации содержат описание режима работы блочных шифров. Данный режим определяет правила криптографического преобразования данных и выработки имитовставки для сообщений произвольной длины.

Необходимость разработки настоящих рекомендаций вызвана потребностью в определении режима работы блочных шифров, осуществляющего одновременно шифрование и выработку имитовставки, соответствующего современным требованиям к криптографической стойкости.

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

РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Режимы работы блочных шифров, реализующие аутентифицированное шифрование

Information technology. Cryptographic data security.
Authenticated encryption block cipher operation modes

Дата введения — 2019—12—01

1 Область применения

Режим работы блочных шифров, определенный в настоящих рекомендациях, рекомендуется использовать при разработке, производстве, эксплуатации и модернизации средств криптографической защиты информации в системах обработки информации различного назначения.

2 Нормативные ссылки

В настоящих рекомендациях использована нормативная ссылка на следующий стандарт:

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

Примечание — 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 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 и сокращения

3.1 Обозначения

В настоящих рекомендациях использованы следующие обозначения:

Издание официальное

V_s — множество битовых строк длины s, $s \geq 0$; нумерация подстрок и компонент строки осуществляется слева направо, начиная с единицы. При $s = 0$ множество V_s состоит из единственной пустой строки длины 0;

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

B_s — множество байтовых строк длины s, $s \geq 0$. Строка $a = (a_1,\ldots,a_s)$ принадлежит множеству B_s, если $a_1,\ldots,a_s \in \{0,\ldots,255\}$; при этом элементы $a_1,\ldots,a_s$ называются байтами строки a. При $s = 0$ множество B_s состоит из единственной пустой строки длины 0;

$|a|$ — длина битовой строки $a \in V^*$ (если a — пустая строка, то $|a| = 0$);

$\|$ — конкатенация битовых строк; если $a = (a_1,\ldots,a_{s1}) \in V_{s1}$, $b = (b_1,\ldots,b_{s2}) \in V_{s2}$, то $a \| b$ называется строка $(a_1,\ldots,a_{s1}, b_1,\ldots,b_{s2}) \in V_{s1+s2}$;

a^s — битовая строка длины s вида $a^s = (a, a,\ldots,a)$, $a \in V_1$, $a^s \in V_s$;

$\oplus$ — операция покомпонентного сложения по модулю 2 двух битовых строк одинаковой длины;

$\sum_{i=1}^{m} a_i$ — битовая строка, являющаяся результатом покомпонентного сложения по модулю 2 битовых строк одинаковой длины. Суммой строк $a_1,\ldots,a_m$ называется строка $\sum_{i=1}^{n} a_i = a_1 \oplus \ldots \oplus a_m$;

$\mathbb{Z}_2 s$ — кольцо вычетов по модулю 2^s;

$MSB_i : V_s \to V_i$ — отображение, ставящее в соответствие битовой строке $a = (a_1,\ldots,a_s) \in V_s$ строку $MSB_i(a) = (a_1,\ldots,a_i) \in V_i$, $1 \leq i \leq s$;

$Int_s : V_s \to \mathbb{Z}_2 s$ — отображение, ставящее в соответствие битовой строке $a = (a_1,\ldots,a_s) \in V_s$ число $Int_s(a) = 2^{s-1} a_1 + \ldots + 2^0 a_s$;

$Vec_s : \mathbb{Z}_2 s \to V_s$ — отображение, обратное к отображению Int_s;

$E : V_n \times V_k \to V_n$ — отображение, реализующее базовый блочный шифр и осуществляющее преобразование блока открытого текста $P \in V_n$ с использованием ключа (шифрования) $K \in V_k$ в блок шифртекста $C \in V_n$: $E(P, K) = C$;

$E_K : V_n \to V_n$ — отображение, реализующее функцию зашифрования с использованием ключа $K \in V_k$, т. е. $E_K(P) = E(P, K)$ для всех $P \in V_n$;

k — параметр блочного шифра, называемый длиной ключа, в рамках настоящих рекомендаций измеряемый в битах;

n — параметр блочного шифра, называемый длиной блока, в рамках настоящих рекомендаций измеряемый в битах и соответствующий значению 64 или 128;

$len : V_s \to V_{n/2}$ — отображение, ставящее в соответствие строке $a \in V_s$ строку $len(a) = Vec_{n/2}(|a|) \in V_{n/2}$;

$\boxplus_{n/2}$ — операция сложения в кольце $\mathbb{Z}_{2n/2}$;

$\otimes : V_n \times V_n \to V_n$ — отображение, ставящее в соответствие двум строкам $a = (a_1, a_2,\ldots,a_n)$ и $b = (b_1, b_2,\ldots,b_n)$, $a, b \in V_n$, строку $c = a \otimes b = (c_1, c_2,\ldots,c_n)$, $c \in V_n$; строка c соответствует многочлену $c(x) = c_1 \cdot x^{n-1} + \ldots + c_{n-1} \cdot x + c_n$, который является результатом умножения двух многочленов $a(x) = a_1 \cdot x^{n-1} + \ldots + a_{n-1} \cdot x + a_n$ и $b(x) = b_1 \cdot x^{n-1} + \ldots + b_{n-1} \cdot x + b_n$ в поле $GF(2^n)$; для $n = 64$ задан порождающий многочлен $f(x) = x^{64} + x^4 + x^3 + x + 1$, для $n = 128$ задан порождающий многочлен $f(x) = x^{128} + x^7 + x^2 + x + 1$;

$incr_l : V_n \to V_n$ — отображение, сопоставляющее строке $L \| R$, где $L, R \in V_{n/2}$, строку $incr_l(L \| R) = Vec_{n/2}(Int_{n/2}(L) \boxplus_{n/2} 1) \| R$;

$incr_r : V_n \to V_n$ — отображение, сопоставляющее строке $L \| R$, где $L, R \in V_{n/2}$, строку $incr_r(L \| R) = L \| Vec_{n/2}(Int_{n/2}(R) \boxplus_{n/2} 1)$;

BitToByte:$V_{8s} \to B_s$ — биективное отображение, ставящее в соответствие битовой строке $a = (a_1, a_2,\ldots, a_{8s})$, $a \in V_{8s}$, байтовую строку $b = (b_1, b_2,\ldots,b_s)$, $b \in B_s$, где $b_i = a_{1+8(i-1)} \cdot 2^7 + a_{2+8(i-1)} \cdot 2^6 + \ldots + a_{8+8(i-1)} \cdot 2^0$, $i = 1, 2,\ldots,s$; при этом строка b называется байтовым представлением строки a;

ByteToBit:$B_s \to V_{8s}$ — биективное отображение, обратное к отображению *BitToByte*.

3.2 Сокращения

В настоящих рекомендациях применены следующие сокращения:

- AAD — (Additional Authenticated Data) — дополнительные имитозащищаемые данные;
- AEAD — (Authenticated Encryption with Associated Data) шифрование с имитозащитой и ассоциированными данными;
- nonce — (number used once) уникальный вектор.

4 Общие положения

Настоящие рекомендации определяют режим MGM (Multilinear Galois Mode) — режим работы блочного шифра. Данный режим можно использовать в качестве режима работы блочного шифра с длиной блока $n = 64$ или $n = 128$. Для определенных в ГОСТ Р 34.12—2015 блочных шифров «Магма» и «Кузнечик», используемых в режиме MGM, выделены идентификаторы 1.2.643.7.1.1.5.1.3 (id-tc26-cipher-gostr3412-2015-magma-mgm) и 1.2.643.7.1.1.5.2.3 (id-tc26-cipher-gostr3412-2015-kuznyechik-mgm) соответственно.

Данный режим является AEAD-режимом и обеспечивает конфиденциальность и имитозащиту сообщений. При этом сообщения могут состоять из одной или двух частей. Если сообщение состоит из двух частей, то первая часть содержит дополнительные имитозащищаемые данные AAD и обозначается через A, а вторая часть называется открытым текстом и обозначается через P. Если сообщение состоит из одной части, то пустой строке должны быть равны либо дополнительные имитозащищаемые данные, либо открытый текст. Дополнительные имитозащищаемые данные не подлежат шифрованию, но требуют имитозащиты. Для открытого текста обеспечены конфиденциальность и имитозащита.

Параметром режима MGM является длина имитовставки S, выраженная в битах, $32 \le S \le n$. Значение S должно быть зафиксировано в рамках каждого конкретного протокола исходя из требований к производительности системы и требований к стойкости режима относительно угрозы нарушения имитозащиты.

5 Режим MGM

5.1 Зашифрование

Процесс зашифрования сообщения, изображенный на рисунке 1, осуществляется при помощи функции *MGM-Encrypt*.

Функция *MGM-Encrypt* принимает на вход следующие значения:

- ключ шифрования $K \in V_k$;
- уникальный вектор *nonce* $\in V_{n-1}$. Значение вектора *nonce* должно быть уникальным для каждого сообщения при фиксированном ключе K. Выработка уникальных векторов может быть реализована с использованием счетчика;
- дополнительные имитозащищаемые данные A, $0 \le |A| < 2^{n/2}$. Дополнительные имитозащищаемые данные разбивают на h блоков и представляют в виде $A = A_1 \,||\ldots||\, A_h^*$, где $A_j \in V_n$, $j = 1,2,\ldots, h-1$, $A_h^* \in V_t$, $1 \le t \le n$. Если длина дополнительных имитозащищаемых данных нулевая, то последний блок A_h^* равен пустой строке, а значения параметров h и t устанавливаются следующим образом: $h = 0$, $t = n$;
- открытый текст P, $0 \le |P| < 2^{n/2}$. Открытый текст разбивают на q блоков и представляют в виде $P = P_1 \,||\ldots||\, P_q^*$, где $P_i \in V_n$, $i = 1,2,\ldots, q-1$, $P_q^* \in V_u$, $1 \le u \le n$. Если длина открытого текста нулевая, то последний блок открытого текста P_q^* равен пустой строке, а значения параметров q и u устанавливаются следующим образом: $q = 0$, $u = n$.

При этом длины $|A|$ и $|P|$ должны удовлетворять следующему ограничению: $0 < |A| + |P| < 2^{n/2}$.

Функция *MGM-Encrypt* в результате своей работы возвращает следующие значения:

- уникальный вектор *nonce* $\in V_{n-1}$;

- дополнительные имитозащищаемые данные A;
- шифртекст $C \in V_{|P|}$;
- имитовставка $T \in V_S$.

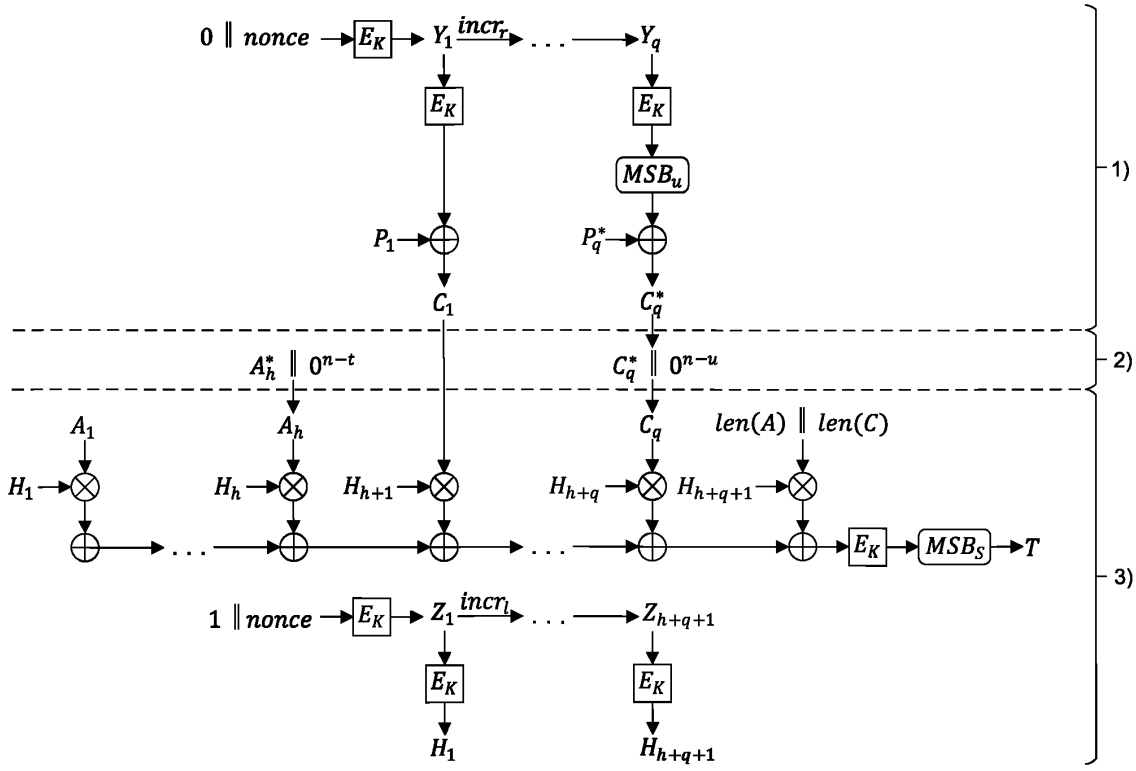


Рисунок 1 — Зашифрование сообщения в режиме MGM

Процесс зашифрования сообщения с помощью функции *MGM-Encrypt* состоит из следующих этапов.

5.1.1 Зашифрование открытого текста P:

$$Y_1 = E_K(0 \,||\, nonce);$$

$$Y_i = incr_r\,(Y_{i-1}),\ i = 2,3,\ldots,\ q; \tag{1}$$

$$C_i = P_i \oplus E_K\,(Y_i),\ i = 1,2,\ldots,\ q-1;$$

$$C_q^* = P_q^* \oplus MSB_u\,(E_K(Y_q)).$$

Результатом данного этапа является шифртекст $C = C_1 \,\|\ldots\|\, C_q^*$.

В случае если открытый текст P равен пустой строке, то шифртекст C также полагается равным пустой строке.

5.1.2 Дополнение последнего блока дополнительных имитозащищаемых данных $A_h^* \in V_t$ и последнего блока шифртекста $C_q^* \in V_u$ до длины n:

$$A_h = A_h^* \,\|\, 0^{n-t};$$

$$C_q = C_q^* \,\|\, 0^{n-u}. \tag{2}$$

5.1.3 Выработка значения имитовставки T от дополнительных имитозащищаемых данных A и шифртекста C:

$$Z_1 = E_K(1 \parallel nonce);$$

$$Z_i = incr_l(Z_{i-1}),\ i = 2,3,\ldots,h+q+1;$$

$$H_i = E_K(Z_i),\ i = 1,2,\ldots,h+q+1; \tag{3}$$

$$T = MSB_s\left(E_K\left(\sum_{i=1}^{h}(H_i \otimes A_i) \oplus \sum_{j=1}^{q}(H_{h+j} \otimes C_j) \oplus H_{h+q+1} \otimes \left(len(A)\|len(C)\right)\right)\right).$$

Результатом данного этапа является значение имитовставки T.

5.2 Расшифрование

Процесс расшифрования сообщения, изображенный на рисунке 2, осуществляется при помощи функции *MGM-Decrypt*.

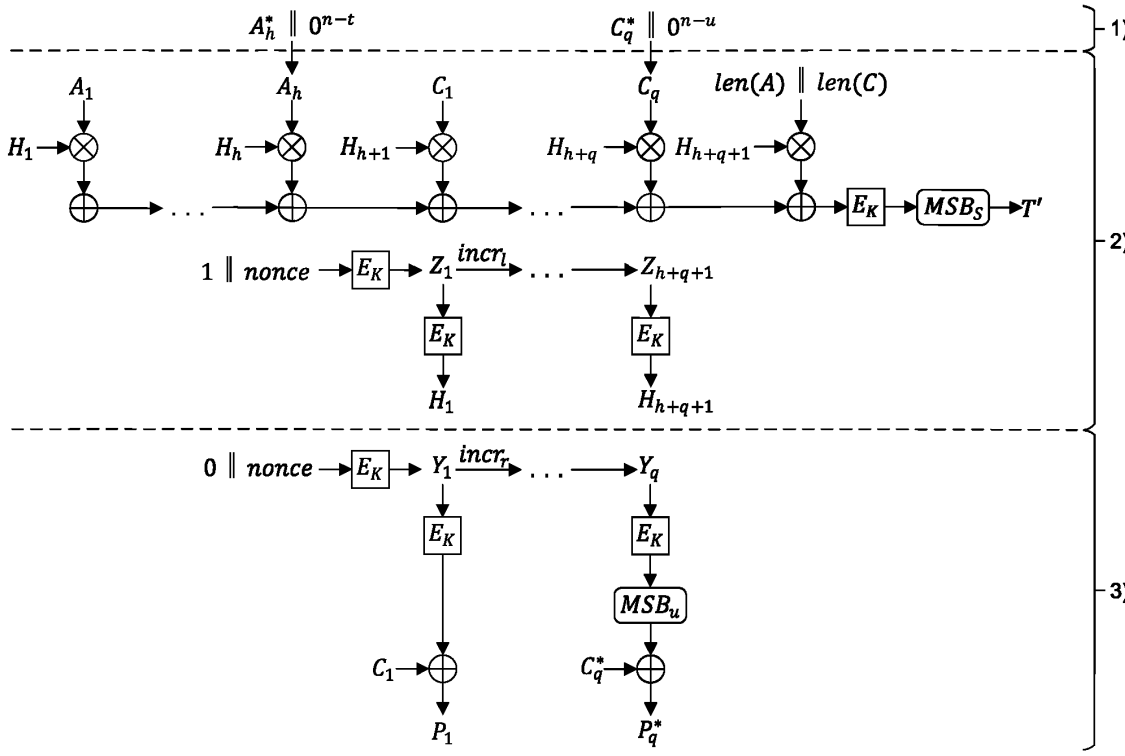


Рисунок 2 — Расшифрование сообщения в режиме MGM

Функция *MGM-Decrypt* принимает на вход следующие значения:

- ключ шифрования $K \in K_k$;
- уникальный вектор $nonce \in V_{n-1}$;
- дополнительные имитозащищаемые данные A, $0 \le |A| < 2^{n/2}$. Дополнительные имитозащищаемые данные разбивают на h блоков и представляют в виде $A = A_1 \parallel \ldots \parallel A_h^*$, где $A_j \in V_n$, $j = 1,2,\ldots, h-1$,

$A_h^* \in V_t$, $1 \le t \le n$. Если длина дополнительных имитозащищаемых данных нулевая, то последний блок A_h^* равен пустой строке, а значения параметров h и t устанавливаются следующим образом: $h = 0$, $t = n$.

- шифртекст C, $0 \le |C| < 2^{n/2}$. Шифртекст разбивают на q блоков и представляют в виде $C = C_1 \| \ldots \| C_q^*$, где $C_i \in V_n$, $i = 1,2,\ldots,q-1$, $C_q^* \in V_u$, $1 \le u \le n$. Если длина шифртекста нулевая, то последний блок шифртекста C_q^* равен пустой строке, а значения параметров q и u устанавливаются следующим образом: $q = 0$, $u = n$;
- имитовставка $T \in V_S$.

Функция *MGM-Decrypt* в результате своей работы возвращает либо ошибку, либо следующие значения:

- дополнительные имитозащищаемые данные A;
- открытый текст $P \in V_{|C|}$.

Процесс расшифрования сообщения с помощью функции *MGM-Decrypt* состоит из следующих этапов.

5.2.1 Дополнение последнего блока дополнительных имитозащищаемых данных $A_h^* \in V_t$ и последнего блока шифртекста $C_q^* \in V_u$ до длины n:

$$A_h = A_h^* \| 0^{n-t};$$

$$C_q = C_q^* \| 0^{n-u}. \tag{4}$$

5.2.2 Выработка значения T' от дополнительных имитозащищаемых данных A и шифртекста C:

$$Z_1 = E_K(1 \| nonce);$$

$$Z_i = incr_l(Z_{i-1}),\ i = 2,3,\ldots,h+q+1;$$

$$H_i = E_K(Z_i),\ i = 1,2,\ldots,h+q+1; \tag{5}$$

$$T' = MSB_S\left(E_K\left(\sum_{i=1}^{h}(H_i \otimes A_i) \oplus \sum_{j=1}^{q}(H_{h+j} \otimes C_j) \oplus H_{h+q+1} \otimes \left(len(A) \| len(C)\right)\right)\right).$$

Если выработанное значение T' отлично от значения T, то возвращается ошибка. Если значения T' и T совпали, то осуществляется переход к следующему этапу.

5.2.3 Расшифрование шифртекста C:

$$Y_1 = E_K(0 \| nonce);$$

$$Y_i = incr_r(Y_{i-1}),\ i = 2,3,\ldots,q;$$

$$P_i = C_i \oplus E_K(Y_i),\ i = 1,2,\ldots,q-1; \tag{6}$$

$$P_q^* = C_q^* \oplus MSB_u(E_K(Y_q)).$$

Результатом данного этапа является открытый текст $P = P_1 \| \ldots \| P_q^*$.

В том случае если шифртекст C равен пустой строке, то открытый текст P также полагается равным пустой строке.

В результате своей успешной работы функция *MGM-Decrypt* возвращает набор данных (A, P). В противном случае функция возвращает сообщение об ошибке.

Приложение А
(справочное)

Работа с байтовыми строками

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

В данном приложении приведены примеры перевода битовой строки в байтовую и наоборот. Для перевода битовой строки в байтовую используется функция *BitToByte*; для перевода байтовой строки в битовую — функция *ByteToBit*.

При записи байтовой строки каждый байт представляется в шестнадцатеричном виде и отделяется от соседних пробелами. Каждой битовой строке $a \in V_{8s}$ соответствует байтовая строка $b = BitToByte(a)$ и наоборот. Например, битовая строка 1100101100011000 соответствует байтовой строке CB 18.

При записи битовой строки она разделяется на подстроки длины не более 8. Каждая подстрока отделяется от соседних пробелами.

Для формирования строки с длиной, кратной 8, битовый вектор *nonce* $\in V_{n-1}$ дополняется нулем слева. Таким образом, байтовым представлением вектора *nonce* является строка *BitToByte* (0 || *nonce*).

Ниже приведен пример перевода битового представления *nonce* в байтовое для случая $n = 128$.

nonce $\in V_{n-1}$:

0010001 00100010 00110011 01000100 01010101 01100110 01110111 10001000 10011001 00000000 10101010 10111011 11001100 11011101 11101110 11111111.

0 || *nonce*:

00010001 00100010 00110011 01000100 01010101 01100110 01110111 10001000 10011001 00000000 10101010 10111011 11001100 11011101 11101110 11111111.

BitToByte (0 || *nonce*):

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

Ниже приведен пример перевода байтового представления *nonce* в битовое для случая $n = 128$.

Байтовое представление *nonce*:

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

0 || *nonce*:

00010001 00100010 00110011 01000100 01010101 01100110 01110111 10001000 10011001 00000000 10101010 10111011 11001100 11011101 11101110 11111111.

nonce $\in V_{n-1}$:

0010001 00100010 00110011 01000100 01010101 01100110 01110111 10001000 10011001 00000000 10101010 10111011 11001100 11011101 11101110 11111111.

Приложение Б
(справочное)

Контрольные примеры

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

В данном приложении содержатся примеры работы блочного шифра «Кузнечик» и «Магма» в режиме MGM, определенном в настоящих рекомендациях. Параметр S выбран равным n.

Б.1 Пример для блочного шифра «Кузнечик»

На вход функции *MGM-Encrypt* подается набор аргументов (K, *nonce*, A, P), принимающих следующие значения:

- 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;
- *nonce*:
11 22 33 44 55 66 77 00 FF EE DD CC BB AA 99 88;
- A:
02 02 02 02 02 02 02 02 01 01 01 01 01 01 01 01
04 04 04 04 04 04 04 04 03 03 03 03 03 03 03 03
EA 05 05 05 05 05 05 05 05;
- P:
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
AA BB CC.

Б.1.1 Зашифрование открытого текста P

$0 \| nonce$:
11 22 33 44 55 66 77 00 FF EE DD CC BB AA 99 88.
Y_1:
7F 67 9D 90 BE BC 24 30 5A 46 8D 42 B9 D4 ED CD.
$E_K(Y_1)$:
B8 57 48 C5 12 F3 19 90 AA 56 7E F1 53 35 DB 74.
Y_2:
7F 67 9D 90 BE BC 24 30 5A 46 8D 42 B9 D4 ED CE.
$E_K(Y_2)$:
80 64 F0 12 6F AC 9B 2C 5B 6E AC 21 61 2F 94 33.
Y_3:
7F 67 9D 90 BE BC 24 30 5A 46 8D 42 B9 D4 ED CF.
$E_K(Y_3)$:
58 58 82 1D 40 C0 CD 0D 0A C1 E6 C2 47 09 8F 1C.
Y_4:
7F 67 9D 90 BE BC 24 30 5A 46 8D 42 B9 D4 ED D0.
$E_K(Y_4)$:
E4 3F 50 81 B5 8F 0B 49 01 2F 8E E8 6A CD 6D FA.
Y_5:
7F 67 9D 90 BE BC 24 30 5A 46 8D 42 B9 D4 ED D1.
$E_K(Y_5)$:
86 CE 9E 2A 0A 12 25 E3 33 56 91 B2 0D 5A 33 48.
C:
A9 75 7B 81 47 95 6E 90 55 B8 A3 3D E8 9F 42 FC
80 75 D2 21 2B F9 FD 5B D3 F7 06 9A AD C1 6B 39
49 7A B1 59 15 A6 BA 85 93 6B 5D 0E A9 F6 85 1C
C6 0C 14 D4 D3 F8 83 D0 AB 94 42 06 95 C7 6D EB
2C 75 52.

Б.1.2 Дополнение последнего блока дополнительных имитозащищаемых данных и последнего блока шифртекста до длины n.

$A = A_1 \| \ldots \| A_h$:
02 02 02 02 02 02 02 02 01 01 01 01 01 01 01 01
04 04 04 04 04 04 04 04 03 03 03 03 03 03 03 03
EA 05 05 05 05 05 05 05 05 00 00 00 00 00 00 00 00.

$C = C_1 \| \ldots \| C_q$:
A9 75 7B 81 47 95 6E 90 55 B8 A3 3D E8 9F 42 FC
80 75 D2 21 2B F9 FD 5B D3 F7 06 9A AD C1 6B 39
49 7A B1 59 15 A6 BA 85 93 6B 5D 0E A9 F6 85 1C
C6 0C 14 D4 D3 F8 83 D0 AB 94 42 06 95 C7 6D EB
2C 75 52 00 00 00 00 00 00 00 00 00 00 00 00 00.

Б.1.3 Выработка значения имитовставки T от дополнительных имитозащищаемых данных A и шифртекста C происходит следующим образом:

$1 \| nonce$:
91 22 33 44 55 66 77 00 FF EE DD CC BB AA 99 88.

Z_1:
7F C2 45 A8 58 6E 66 02 A7 BB DB 27 86 BD C6 6F.

H_1:
8D B1 87 D6 53 83 0E A4 BC 44 64 76 95 2C 30 0B.

Z_2:
7F C2 45 A8 58 6E 66 03 A7 BB DB 27 86 BD C6 6F.

H_2:
7A 24 F7 26 30 E3 76 37 21 C8 F3 CD B1 DA 0E 31.

Z_3:
7F C2 45 A8 58 6E 66 04 A7 BB DB 27 86 BD C6 6F.

H_3:
44 11 96 21 17 D2 06 35 C5 25 E0 A2 4D B4 B9 0A.

Z_4:
7F C2 45 A8 58 6E 66 05 A7 BB DB 27 86 BD C6 6F.

H_4:
D8 C9 62 3C 4D BF E8 14 CE 7C 1C 0C EA A9 59 DB.

Z_5:
7F C2 45 A8 58 6E 66 06 A7 BB DB 27 86 BD C6 6F.

H_5:
A5 E1 F1 95 33 3E 14 82 96 99 31 BF BE 6D FD 43.

Z_6:
7F C2 45 A8 58 6E 66 07 A7 BB DB 27 86 BD C6 6F.

H_6:
B4 CA 80 8C AC CF B3 F9 17 24 E4 8A 2C 7E E9 D2.

Z_7:
7F C2 45 A8 58 6E 66 08 A7 BB DB 27 86 BD C6 6F.

H_7:
72 90 8F C0 74 E4 69 E8 90 1B D1 88 EA 91 C3 31.

Z_8:
7F C2 45 A8 58 6E 66 09 A7 BB DB 27 86 BD C6 6F.

H_8:
23 CA 27 15 B0 2C 68 31 3B FD AC B3 9E 4D 0F B8.

Z_9:
7F C2 45 A8 58 6E 66 0A A7 BB DB 27 86 BD C6 6F.

H_9:
BC BC E6 C4 1A A3 55 A4 14 88 62 BF 64 BD 83 0D.

$len(A) \| len(C)$:
00 00 00 00 00 00 01 48 00 00 00 00 00 00 02 18.

T:
CF 5D 65 6F 40 C3 4F 5C 46 E8 BB 0E 29 FC DB 4C.

Б.2 Пример для блочного шифра «Магма»

На вход функции *MGM-Encrypt* подается набор аргументов (K, *nonce*, A, P), принимающих следующие значения:

- *K*:
FF EE DD CC BB AA 99 88 77 66 55 44 33 22 11 00
F0 F1 F2 F3 F4 F5 F6 F7 F8 F9 FA FB FC FD FE FF;
- *nonce*:
12 DE F0 6B 3C 13 0A 59;
- *A*:
01 01 01 01 01 01 01 02 02 02 02 02 02 02 02
03 03 03 03 03 03 03 04 04 04 04 04 04 04 04
05 05 05 05 05 05 05 EA;
- *P*:
FF EE DD CC BB AA 99 88 11 22 33 44 55 66 77 00
88 99 AA BB CC EE FF 0A 00 11 22 33 44 55 66 77
99 AA BB CC EE FF 0A 00 11 22 33 44 55 66 77 88
AA BB CC EE FF 0A 00 11 22 33 44 55 66 77 88 99
AA BB CC.

Б.2.1 Зашифрование открытого текста *P*

0 ‖ *nonce*:
12 DE F0 6B 3C 13 0A 59.
Y_1:
56 23 89 01 62 DE 31 BF.
$E_K(Y_1)$:
38 7B DB A0 E4 34 39 B3.
Y_2:
56 23 89 01 62 DE 31 C0.
$E_K(Y_2)$:
94 33 00 06 10 F7 F2 AE.
Y_3:
56 23 89 01 62 DE 31 C1.
$E_K(Y_3)$:
97 B7 AA 6D 73 C5 87 57.
Y_4:
56 23 89 01 62 DE 31 C2.
$E_K(Y_4)$:
94 15 52 8B FF C9 E8 0A.
Y_5:
56 23 89 01 62 DE 31 C3.
$E_K(Y_5)$:
03 F7 68 BF F1 82 D6 70.
Y_6:
56 23 89 01 62 DE 31 C4.
$E_K(Y_6)$:
FD 05 F8 4E 9B 09 D2 FE.
Y_7:
56 23 89 01 62 DE 31 C5.
$E_K(Y_7)$:
DA 4D 90 8A 95 B1 75 C4.
Y_8:
56 23 89 01 62 DE 31 C6.
$E_K(Y_8)$:
65 99 73 96 DA C2 4B D7.
Y_9:
56 23 89 01 62 DE 31 C7.
$E_K(Y_9)$:
A9 00 50 4A 14 8D EE 26.
C:
C7 95 06 6C 5F 9E A0 3B 85 11 33 42 45 91 85 AE
1F 2E 00 D6 BF 2B 78 5D 94 04 70 B8 BB 9C 8E 7D
9A 5D D3 73 1F 7D DC 70 EC 27 CB 0A CE 6F A5 76

70 F6 5C 64 6A BB 75 D5 47 AA 37 C3 BC B5 C3 4E
03 BB 9C.

Б.2.2 Дополнение последнего блока дополнительных имитозащищаемых данных и последнего блока шифртекста до длины *n*

$A = A_1 \| \ldots \| A_h$:
01 01 01 01 01 01 01 01 02 02 02 02 02 02 02 02
03 03 03 03 03 03 03 03 04 04 04 04 04 04 04 04
05 05 05 05 05 05 05 05 EA 00 00 00 00 00 00 00.
$C = C_1 \| \ldots \| C_q$:
C7 95 06 6C 5F 9E A0 3B 85 11 33 42 45 91 85 AE
1F 2E 00 D6 BF 2B 78 5D 94 04 70 B8 BB 9C 8E 7D
9A 5D D3 73 1F 7D DC 70 EC 27 CB 0A CE 6F A5 76
70 F6 5C 64 6A BB 75 D5 47 AA 37 C3 BC B5 C3 4E
03 BB 9C 00 00 00 00 00.

Б.2.3 Выработка значения имитовставки *T* от дополнительных имитозащищаемых данных *A* и шифртекста *C* происходит следующим образом:

$1 \| nonce$:
92 DE F0 6B 3C 13 0A 59.
Z_1:
2B 07 3F 04 94 F3 72 A0.
H_1:
70 8A 78 19 1C DD 22 AA.
Z_2:
2B 07 3F 05 94 F3 72 A0.
H_2:
6F 02 CC 46 4B 2F A0 A3.
Z_3:
2B 07 3F 06 94 F3 72 A0.
H_3:
9F 81 F2 26 FD 19 6F 05.
Z_4:
2B 07 3F 07 94 F3 72 A0.
H_4:
B9 C2 AC 9B E5 B5 DF F9.
Z_5:
2B 07 3F 08 94 F3 72 A0.
H_5:
74 B5 EC 96 55 1B F8 88.
Z_6:
2B 07 3F 09 94 F3 72 A0.
H_6:
7E B0 21 A4 03 5B 04 C3.
Z_7:
2B 07 3F 0A 94 F3 72 A0.
H_7:
C2 A9 C3 A8 70 4D 9B B0.
Z_8:
2B 07 3F 0B 94 F3 72 A0.
H_8:
F5 D5 05 A8 7B 83 83 B5.
Z_9:
2B 07 3F 0C 94 F3 72 A0.
H_9:
F7 95 E7 5F DE B8 93 3C.
Z_{10}:
2B 07 3F 0D 94 F3 72 A0.
H_{10}:

65 A1 A3 E6 80 F0 81 45.
Z_{11}:
2B 07 3F 0E 94 F3 72 A0.
H_{11}:
1C 74 A5 76 4C B0 D5 95.
Z_{12}:
2B 07 3F 0F 94 F3 72 A0.
H_{12}:
DC 84 47 A5 14 E7 83 E7.
Z_{13}:
2B 07 3F 10 94 F3 72 A0.
H_{13}:
A7 E3 AF E0 04 EE 16 E3.
Z_{14}:
2B 07 3F 11 94 F3 72 A0.
H_{14}:
A5 AA BB 0B 79 80 D0 71.
Z_{15}:
2B 07 3F 12 94 F3 72 A0.
H_{15}:
6E 10 4C C9 33 52 5C 5D.
Z_{16}:
2B 07 3F 13 94 F3 72 A0.
H_{16}:
83 11 B6 02 4A A9 66 C1.
len (*A*) || *len* (*C*):
00 00 01 48 00 00 02 18.
T:
A7 92 80 69 AA 10 FD 10.

УДК 681.3.06:006.354 ОКС 35. 040 ОКСТУ 5002 П85

Ключевые слова: зашифрование, расшифрование, имитозащита, режим работы блочного шифра, ключ

БЗ 10—2019/64

Редактор *Л.С. Зимилова*
Технический редактор *И.Е. Черепкова*
Корректор *Е.Д. Дульнева*
Компьютерная верстка *А.Н. Золотаревой*

Сдано в набор 10.09.2019. Подписано в печать 25.11.2019. Формат 60 × 84 1/8. Гарнитура Ариал.
Усл. печ. л. 1,86. Уч.-изд. л. 1,49.
Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Создано в единичном исполнении во ФГУП «СТАНДАРТИНФОРМ»
для комплектования Федерального информационного фонда стандартов,
117418 Москва, Нахимовский пр-т, д. 31, к. 2.
gost.e-ecolog.ru gost.e-ecolog.ru

gost.e-ecolog.ru