МЕЖГОСУДАРСТВЕННЫЙ СОВЕТ ПО СТАНДАРТИЗАЦИИ, МЕТРОЛОГИИ И СЕРТИФИКАЦИИ
(МГС)

INTERSTATE COUNCIL FOR STANDARDIZATION, METROLOGY AND CERTIFICATION
(ISC)

МЕЖГОСУДАРСТВЕННЫЙ СТАНДАРТ

ГОСТ 34.13— 2018

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Режимы работы блочных шифров

Издание официальное

Москва
Стандартинформ
2018

Предисловие

Цели, основные принципы и основной порядок проведения работ по межгосударственной стандартизации установлены в ГОСТ 1.0—2015 «Межгосударственная система стандартизации. Основные положения» и ГОСТ 1.2—2015 «Межгосударственная система стандартизации. Стандарты межгосударственные, правила и рекомендации по межгосударственной стандартизации. Правила разработки, принятия, обновления и отмены»

Сведения о стандарте

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 ПРИНЯТ Межгосударственным советом по метрологии, стандартизации и сертификации (протокол от 29 ноября 2018 г. № 54)

За принятие проголосовали:

Краткое наименование страны по МК (ИСО 3166) 004—97	Код страны по МК (ИСО 3166) 004—97	Сокращенное наименование национального органа по стандартизации
Армения	AM	Минэкономики Республики Армения
Киргизия	KG	Кыргызстандарт
Россия	RU	Росстандарт
Таджикистан	TJ	Таджикстандарт

4 Приказом Федерального агентства по техническому регулированию и метрологии от 4 декабря 2018 г. № 1062-ст межгосударственный стандарт ГОСТ 34.13—2018 введен в действие в качестве национального стандарта Российской Федерации с 1 июня 2019 г.

5 Настоящий стандарт подготовлен на основе применения ГОСТ Р 34.13—2015

6 ВЗАМЕН ГОСТ 28147—89 в части раздела 2 «Режим простой замены»; раздела 3 «Режим гаммирования»; раздела 4 «Режим гаммирования с обратной связью»; раздела 5 «Режим выработки имитовставки»

Информация об изменениях к настоящему стандарту публикуется в ежегодном информационном указателе «Национальные стандарты», а текст изменений и поправок — в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ежемесячном информационном указателе «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

1 Область применения . . . 1
2 Термины, определения и обозначения . . . 1
2.1 Термины и определения . . . 1
2.2 Обозначения . . . 3
3 Общие положения . . . 3
4 Вспомогательные операции . . . 4
4.1 Дополнение сообщения . . . 4
4.2 Выработка начального значения . . . 4
4.3 Процедура усечения . . . 5
5 Режимы работы алгоритмов блочного шифрования . . . 5
5.1 Режим простой замены . . . 5
5.2 Режим гаммирования . . . 6
5.3 Режим гаммирования с обратной связью по выходу . . . 7
5.4 Режим простой замены с зацеплением . . . 9
5.5 Режим гаммирования с обратной связью по шифртексту . . . 11
5.6 Режим выработки имитовставки . . . 13
Приложение А (справочное) Контрольные примеры . . . 16
Библиография . . . 22

Введение

Настоящий стандарт содержит описание режимов работы блочных шифров. Данные режимы работы блочных шифров определяют правила криптографического преобразования данных и выработки имитовставки для сообщений произвольного размера.

Необходимость разработки настоящего стандарта вызвана потребностью в определении режимов работы блочных шифров, соответствующих современным требованиям к криптографической стойкости.

Настоящий стандарт терминологически и концептуально увязан с международными стандартами ИСО/МЭК 9797-1 [1], ИСО/МЭК 10116 [2], ИСО/МЭК 10118-1 [3], ИСО/МЭК 18033-1 [4], ИСО/МЭК 14888-1 [5].

Примечание — Основная часть стандарта дополнена приложением А «Контрольные примеры».

Поправка к ГОСТ 34.13—2018 Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров

В каком месте	Напечатано	Должно быть		
Предисловие. Таблица согласования	—	Туркмения	ТМ	Главгосслужба «Туркменстандартлары»

(ИУС № 1 2021 г.)

М Е Ж Г О С У Д А Р С Т В Е Н Н Ы Й С Т А Н Д А Р Т

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Режимы работы блочных шифров

Information technology. Cryptographic data security.
Modes of operation for block ciphers

Дата введения — 2019—06—01

1 Область применения

Настоящий стандарт распространяется на криптографическую защиту информации и определяет режимы работы блочных шифров.

Режимы работы блочных шифров, определенные в настоящем стандарте, рекомендуется использовать при разработке, производстве, эксплуатации и модернизации средств криптографической защиты информации в системах 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.

Примечание — Адаптировано из ИСО/МЭК 18033-1 [4].

2.1.2 **алгоритм расшифрования** (decryption algorithm): Алгоритм, реализующий расшифрование, т. е. преобразующий шифртекст в открытый текст.

Примечание — Адаптировано из ИСО/МЭК 18033-1 [4].

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.

Примечание — Адаптировано из ИСО/МЭК 18033-1 [4].

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.

Примечания

1 Адаптировано из ИСО/МЭК 18033-1 [4].

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

Издание официальное

2.1.6 **дополнение** (padding): Приписывание дополнительных бит к строке бит.

Примечание — Адаптировано из ИСО/МЭК 10118-1 [3].

2.1.7 **зацепление блоков** (block chaining): Шифрование информации таким образом, что каждый блок шифртекста криптографически зависит от предыдущего блока шифртекста.

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

Примечание — Адаптировано из ИСО/МЭК 18033-1 [4].

2.1.9 **имитовставка** (message authentication code): Строка бит фиксированной длины, полученная применением симметричного криптографического метода к сообщению, добавляемая к сообщению для обеспечения его целостности и аутентификации источника данных.

Примечание — Адаптировано из ИСО/МЭК 9797-1 [1].

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

Примечания

1 Адаптировано из ИСО/МЭК 18033-1 [4].

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

2.1.11 **начальное значение** (starting variable): Значение, возможно, полученное из синхропосылки и используемое для задания начальной точки режима работы блочного шифра.

Примечание — Адаптировано из ИСО/МЭК 10116 [2].

2.1.12 **открытый текст** (plaintext): Незашифрованная информация.

Примечание — Адаптировано из ИСО/МЭК 10116 [2].

2.1.13 **расшифрование** (decryption): Операция, обратная к зашифрованию.

Примечания

1 Адаптировано из ИСО/МЭК 18033-1 [4].

2 В настоящем стандарте в целях сохранения терминологической преемственности по отношению к нормативным документам, действующим на территории государства, принявшего настоящий стандарт, и опубликованным ранее на русском языке научно-техническим изданиям применяется термин «шифрование», объединяющий операции, определенные терминами «зашифрование» и «расшифрование». Конкретное значение термина «шифрование» определяется в зависимости от контекста упоминания.

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

Примечание — Адаптировано из ИСО/МЭК 18033-1 [4].

2.1.15 **синхропосылка** (initializing value): Комбинация знаков, передаваемая по каналу связи и предназначенная для инициализации алгоритма шифрования.

2.1.16 **сообщение** (message): Строка бит произвольной конечной длины.

Примечание — Адаптировано из ИСО/МЭК 14888-1 [5].

2.1.17 **счетчик** (counter): Строка бит длины, равной длине блока блочного шифра, используемая при шифровании в режиме гаммирования.

Примечание — Адаптировано из ИСО/МЭК 10116 [2].

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

Примечание — Адаптировано из ИСО/МЭК 18033-1 [4].

2.1.19 **шифртекст** (ciphertext): Данные, полученные в результате зашифрования открытого текста в целях скрытия его содержания.

Примечание — Адаптировано из ИСО/МЭК 10116 [2].

2.2 Обозначения

В настоящем стандарте применены 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;

$|A|$ — 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 бóльшими номерами компонент из $V_{|A|}$ совпадает со строкой A, а подстрока с меньшими номерами компонент из $V_{|B|}$ совпадает со строкой B;

0^r — строка, состоящая из r нулей;

$\oplus$ — 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 $\mathbb{Z}_{2^s}$;

$x \bmod l$ — операция вычисления остатка от деления целого числа x на целое положительное число l;

$\mathrm{MSB}_s: V^* \setminus \bigcup_{i=0}^{s-1} V_i \to V_s$ — отображение, ставящее в соответствие строке $z_{m-1}\|\ldots\|z_1\|z_0$, $m \geq s$, строку $z_{m-1}\|\ldots\|z_{m-s+1}\|z_{m-s}$, $z_i \in V_1$, $i = 0, 1, \ldots, m-1$;

$\mathrm{LSB}_s: V^* \setminus \bigcup_{i=0}^{s-1} V_i \to V_s$ — отображение, ставящее в соответствие строке $z_{m-1}\|\ldots\|z_1\|z_0$, $m \geq s$, строку $z_{s-1}\|\ldots\|z_1\|z_0$, $z_i \in V_1$, $i = 0, 1, \ldots, m-1$;

$A \ll r$ — операция логического сдвига строки A на r компонент в сторону компонент, имеющих бóльшие номера. Если $A \in V_s$, то $A \ll r \in V_s$, причем

$$A \ll r = \begin{cases} \mathrm{LSB}_{s-r}(A)\|0^r, & \text{если } r < s, \\ 0^s, & \text{если } r \geq s; \end{cases}$$

$\mathrm{Poly}_s: V_s \to \mathrm{GF}(2)[x]$ — отображение, ставящее в соответствие строке $z = (z_{s-1}\|\ldots\|z_0) \in V_s$ многочлен

$$\mathrm{Poly}_s(z) = \sum_{i=0}^{s-1} z_i x^i;$$

$\mathbf{Vec}_s: \mathbb{Z}_{2^s} \to V_s$ — 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 $z = z_0 + 2 \cdot z_1 + \ldots + 2^{s-1} \cdot z_{s-1}$, где $z_i \in \{0, 1\}$, $i = 0, 1, \ldots, s-1$, выполнено равенство $\mathrm{Vec}_s(z) = z_{s-1}\|\ldots\|z_1\|z_0$;

$\mathrm{Int}_s: V_s \to \mathbb{Z}_{2^s}$ — отображение, обратное к отображению Vec_s, т. е. $\mathrm{Int}_s = \mathrm{Vec}_s^{-1}$;

k — параметр алгоритма блочного шифрования, называемый длиной ключа;

n — параметр алгоритма блочного шифрования, называемый длиной блока;

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

$\mathrm{e}_K: V_n \to V_n$ — отображение, реализующее зашифрование с использованием ключа $K \in V_k$, т. е. $\mathrm{e}_K(P) = \mathrm{E}(P, K)$ для всех $P \in V_n$;

$\mathrm{d}_K: V_n \to V_n$ — отображение, реализующее расшифрование с использованием ключа $K \in V_k$, т. е. $\mathrm{d}_K = \mathrm{e}_K^{-1}$.

3 Общие положения

Настоящий стандарт определяет следующие режимы работы алгоритмов блочного шифрования:

- режим простой замены (ECB, англ. Electronic Codebook);
- режим гаммирования (CTR, англ. Counter);
- режим гаммирования с обратной связью по выходу (OFB, англ. Output Feedback);
- режим простой замены с зацеплением (CBC, англ. Cipher Block Chaining);
- режим гаммирования с обратной связью по шифртексту (CFB, англ. Cipher Feedback);
- режим выработки имитовставки (англ. Message Authentication Code algorithm).

Данные режимы могут использоваться в качестве режимов для блочных шифров с произвольной длиной блока n.

4 Вспомогательные операции

4.1 Дополнение сообщения

4.1.1 Общие положения

Отдельные из описанных ниже режимов работы (режим гаммирования, режим гаммирования с обратной связью по выходу, режим гаммирования с обратной связью по шифртексту) могут осуществлять криптографическое преобразование сообщений произвольной длины. Для других режимов (режим простой замены, режим простой замены с зацеплением) требуется, чтобы длина сообщения была кратна некоторой величине l. В последнем случае при работе с сообщениями произвольной длины необходимо применение процедуры дополнения сообщения до требуемой длины. Ниже приведены три процедуры дополнения.

Пусть $P \in V^*$ исходное сообщение, подлежащее зашифрованию.

4.1.2 Процедура 1

Пусть $r = |P| \bmod l$. Положим

$$P^* = \begin{cases} P, & \text{если } r = 0, \\ P \| 0^{l-r}, & \text{иначе.} \end{cases}$$

Примечание — Описанная процедура в некоторых случаях не обеспечивает однозначного восстановления исходного сообщения. Например, результаты дополнения сообщений P_1, такого что $|P_1| = l \cdot q - 1$ для некоторого q, и $P_2 = P_1 \| 0$ будут одинаковы. В этом случае для однозначного восстановления необходимо дополнительно знать длину исходного сообщения.

4.1.3 Процедура 2

Пусть $r = |P| \bmod l$. Положим

$$P^* = P \| 1 \| 0^{l-r-1}.$$

Примечание — Данная процедура обеспечивает однозначное восстановление исходного сообщения. При этом если длина исходного сообщения кратна l, то длина дополненного сообщения будет увеличена.

4.1.4 Процедура 3

Пусть $r = |P| \bmod l$.

В зависимости от значения r возможны случаи:

- если $r = l$, то последний блок не изменяется $P^* = P$;
- если $r < l$, то применяется процедура 2.

Примечания

1 Данная процедура обязательна для режима выработки имитовставки (5.6) и не рекомендуется для использования в других режимах (5.1—5.5).

2 Выбор конкретной процедуры дополнения предоставляется разработчику информационной системы и/или регламентируется другими нормативными документами.

4.2 Выработка начального значения

В некоторых режимах работы используются величины, начальное значение которых вычисляется на основании синхропосылки IV; обозначим через m суммарную длину указанных величин. Будем обозначать процедуру выработки начального значения через $I_m: V_{|IV|} \to V_m$ и называть процедурой инициализации. Будем называть процедуру инициализации тривиальной, если $I_{|IV|} = IV$. Если не оговорено иное, будем считать, что используется тривиальная процедура инициализации на основе синхропосылки необходимой длины.

Во всех описываемых в настоящем стандарте режимах работы не требуется обеспечение конфиденциальности синхропосылки. Вместе с тем процедура выработки синхропосылки должна удовлетворять одному из следующих требований:

- значения синхропосылки для режимов простой замены с зацеплением и гаммирования с обратной связью по шифртексту необходимо выбирать случайно, равновероятно и независимо друг от друга из множества всех допустимых значений. В этом случае значение каждой используемой синхропосылки IV должно быть непредсказуемым (случайным или псевдослучайным): зная значения всех других используемых синхропосылок, значение IV нельзя определить с вероятностью большей, чем $2^{-|IV|}$;

- все значения синхропосылок, выработанных для зашифрования на одном и том же ключе в режиме гаммирования, должны быть уникальными, т. е. попарно различными. Для выработки значений синхропосылок может быть использован детерминированный счетчик;

- значение синхропосылки для режима гаммирования с обратной связью по выходу должно быть либо непредсказуемым (случайным или псевдослучайным), либо уникальным.

Примечание — Режим простой замены не предусматривает использования синхропосылки.

4.3 Процедура усечения

В некоторых режимах используется усечение строк длины n до строк длины s, $s \le n$, с использованием функции $T_s = MSB_s$, т. е. в качестве операции усечения используется операция взятия бит с бóльшими номерами.

5 Режимы работы алгоритмов блочного шифрования

5.1 Режим простой замены

5.1.1 Общие положения

Длина сообщений, зашифровываемых в режиме простой замены, должна быть кратна длине блока базового алгоритма блочного шифрования n, поэтому при необходимости к исходному сообщению должна быть предварительно применена процедура дополнения.

Зашифрование (расшифрование) в режиме простой замены заключается в зашифровании (расшифровании) каждого блока текста с помощью базового алгоритма блочного шифрования.

5.1.2 Зашифрование

Открытый и при необходимости дополненный текст $P \in V^*$, $|P| = n \cdot q$, представляется в виде: $P = P_1 \| P_2 \| \ldots \| P_q$, $P_i \in V_n$, $i = 1, 2, \ldots, q$. Блоки шифртекста вычисляют по следующему правилу:

$$C_i = e_K(P_{-i}),\ i = 1, 2, \ldots, q. \qquad (1)$$

Результирующий шифртекст имеет вид:

$$C = C_1 \| C_2 \| \ldots \| C_q.$$

Зашифрование в режиме простой замены показано на рисунке 1.

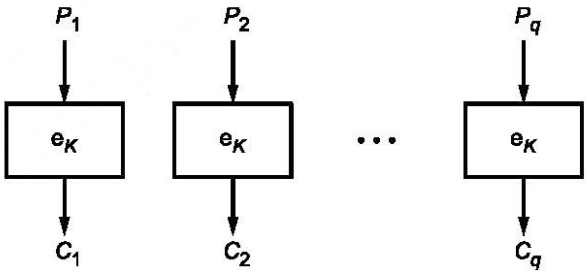

Рисунок 1 — Зашифрование в режиме простой замены

5.1.3 Расшифрование

Шифртекст представляется в виде: $C = C_1 || C_2 || \ldots || C_q$, $C_i \in V_n$, $i = 1, 2, \ldots q$. Блоки открытого текста вычисляются по следующему правилу:

$$P_i = d_K(C_i),\ i = 1, 2, \ldots, q. \qquad (2)$$

Исходный (дополненный) открытый текст имеет вид:

$$P = P_1 || P_2 || \ldots || P_q.$$

Примечание — Если к исходному открытому тексту была применена процедура дополнения, то после расшифрования следует провести обратную процедуру. Для однозначного восстановления сообщения может потребоваться знание длины исходного сообщения.

Расшифрование в режиме простой замены показано на рисунке 2.

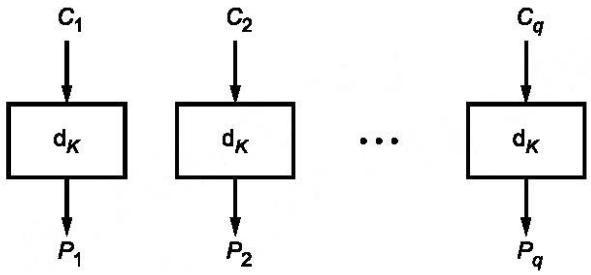

Рисунок 2 — Расшифрование в режиме простой замены

5.2 Режим гаммирования

5.2.1 Общие положения

Параметром режима гаммирования является целочисленная величина s, $0 < s \le n$. При использовании режима гаммирования не требуется применение процедуры дополнения сообщения.

Для зашифрования (расшифрования) каждого отдельного открытого текста на одном ключе используется значение уникальной синхропосылки $IV \in V_{\frac{n}{2}}$.

Зашифрование в режиме гаммирования заключается в покомпонентном сложении открытого текста с гаммой шифра, которая вырабатывается блоками длины s путем зашифрования последовательности значений счетчика $CTR_i \in V_n$, $i = 1, 2, \ldots$, базовым алгоритмом блочного шифрования с последующим усечением. Начальным значением счетчика является $CTR_1 = \mathrm{I}_n(IV) = IV \,||\, 0^{\frac{n}{2}}$. Последующие значения счетчика вырабатываются с помощью функции Add: $V_n \to V_n$ следующим образом:

$$CTR_{i+1} = \mathrm{Add}(CTR_i) = \mathrm{Vec}_n(\mathrm{Int}_n(CTR_i) \boxplus_n 1). \tag{3}$$

5.2.2 Зашифрование

Открытый текст $P \in V^*$ представляется в виде $P = P_1 \| P_2 \| \ldots \| P_q$, $P_i \in V_s$, $i = 1, 2, \ldots, q-1$, $P_q \in V_r$, $r \le s$. Блоки шифртекста вычисляются по следующему правилу:

$$\begin{cases} C_i = P_i \oplus \mathrm{T}_s(\mathrm{e}_K(CTR_i)), \ i = 1, 2, \ldots, q-1, \\ C_q = P_q \oplus \mathrm{T}_r(\mathrm{e}_K(CTR_q)). \end{cases} \tag{4}$$

Результирующий шифртекст имеет вид:

$$C = C_1 \| C_2 \| \ldots \| C_q.$$

Зашифрование в режиме гаммирования показано на рисунке 3.

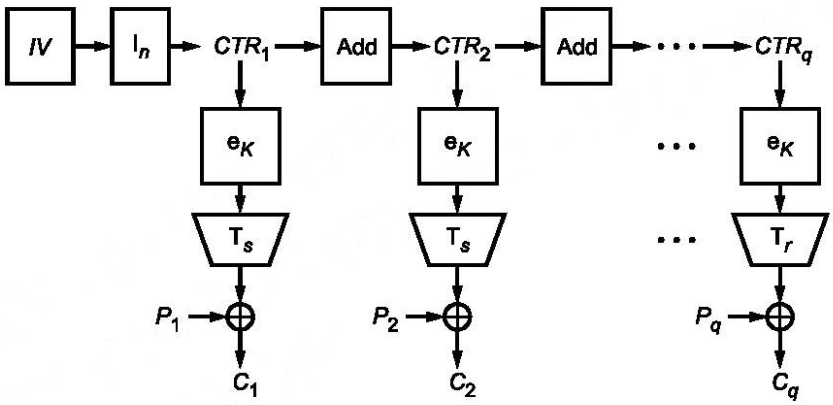

Рисунок 3 — Зашифрование в режиме гаммирования

5.2.3 Расшифрование

Шифртекст представляется в виде: $C = C_1 \| C_2 \| \ldots \| C_q$, $C_i \in V_s$, $i = 1, 2, \ldots, q-1$, $C_q \in V_r$, $r \le s$.

Блоки открытого текста вычисляются по следующему правилу:

$$\begin{cases} P_i = C_i \oplus \mathrm{T}_s(\mathrm{e}_K(CTR_i)), \ i = 1, 2, \ldots, q-1, \\ P_q = C_q \oplus \mathrm{T}_r(\mathrm{e}_K(CTR_q)). \end{cases} \quad (5)$$

Исходный открытый текст имеет вид:

$$P = P_1 \| P_2 \| \ldots \| P_q.$$

Расшифрование в режиме гаммирования показано на рисунке 4.

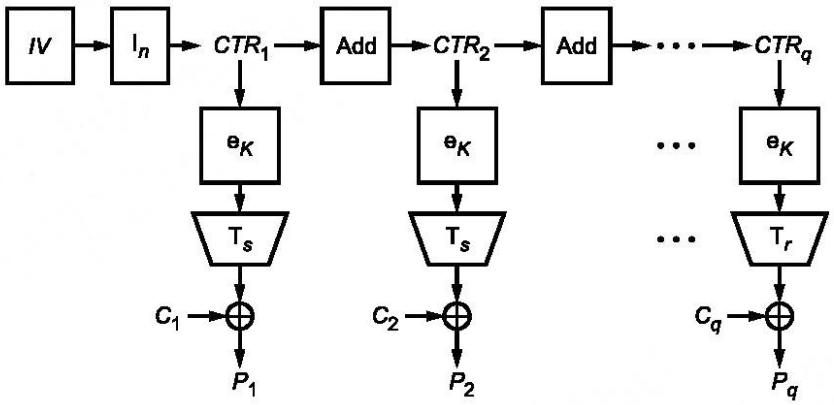

Рисунок 4 — Расшифрование в режиме гаммирования

5.3 Режим гаммирования с обратной связью по выходу

5.3.1 Общие положения

Параметрами режима гаммирования с обратной связью по выходу являются целочисленные величины s и m, $0 < s \le n$, $m = n \cdot z$, $z \ge 1$ — целое число.

При использовании режима гаммирования с обратной связью по выходу не требуется применение процедуры дополнения сообщения.

При шифровании на одном ключе для каждого отдельного открытого текста используется значение уникальной или непредсказуемой (случайной или псевдослучайной) синхропосылки $IV \in V_m$.

При шифровании в режиме гаммирования с обратной связью по выходу используется двоичный регистр сдвига R длины m. Начальным заполнением регистра является значение синхропосылки IV.

Зашифрование в режиме гаммирования с обратной связью по выходу заключается в покомпонентном сложении открытого текста с гаммой шифра, которая вырабатывается блоками длины s. При вычислении очередного блока гаммы выполняется зашифрование n разрядов регистра сдвига с бóльшими номерами базовым алгоритмом блочного шифрования. Затем заполнение регистра сдвигается на n бит в сторону разрядов с бóльшими номерами, при этом в разряды с меньшими номерами записывается полученный выход базового алгоритма блочного шифрования. Блок гаммы вычисляется путем усечения выхода базового алгоритма блочного шифрования.

5.3.2 Зашифрование

Открытый текст $P \in V^*$ представляется в виде $P = P_1 \| P_2 \| \ldots \| P_q$, $P_i \in V_s$, $i = 1, 2, \ldots, q-1$, $P_q \in V_r$, $r \le s$. Блоки шифртекста вычисляются по следующему правилу:

$$R_1 = IV,$$

$$\begin{cases} Y_i = \mathrm{e}_K(\mathrm{MSB}_n(R_i)), \\ C_i = P_i \oplus \mathrm{T}_s(Y_i), \qquad i = 1, 2, \ldots, q-1, \\ R_{i+1} = \mathrm{LSB}_{m-n}(R_i) \| Y_i, \end{cases} \quad (6)$$

$$Y_q = \mathrm{e}_K(\mathrm{MSB}_n(R_q)),$$

$$C_q = P_q \oplus \mathrm{T}_r(Y_q).$$

Результирующий шифртекст имеет вид:

$$C = C_1 \| C_2 \| \ldots \| C_q.$$

Зашифрование в режиме гаммирования с обратной связью по выходу показано на рисунке 5.

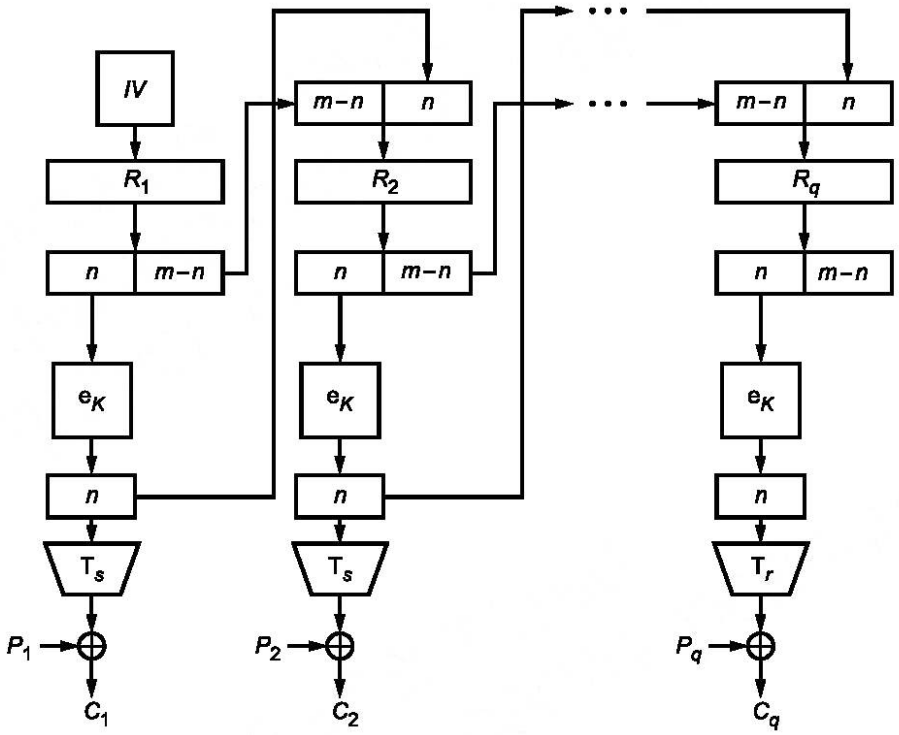

Рисунок 5 — Зашифрование в режиме гаммирования с обратной связью по выходу

5.3.3 Расшифрование

Шифртекст представляется в виде: $C = C_1 \| C_2 \| \ldots \| C_q$, $C_i \in V_s$, $i = 1, 2, \ldots, q-1$, $C_q \in V_r$, $r \le s$.

Блоки открытого текста вычисляются по следующему правилу:

$$R_1 = IV,$$

$$\begin{cases} Y_i = \mathrm{e}_K(\mathrm{MSB}_n(R_i)), \\ P_i = C_i \oplus \mathrm{T}_s(Y_i), \qquad i = 1, 2, \ldots, q-1, \\ R_{i+1} = \mathrm{LSB}_{m-n}(R_i) \| Y_i, \end{cases} \tag{7}$$

$$Y_q = \mathrm{e}_K(\mathrm{MSB}_n(R_q)),$$

$$P_q = C_q \oplus \mathrm{T}_r(Y_q).$$

Исходный открытый текст имеет вид:

$$P = P_1 \| P_2 \| \ldots \| P_q.$$

Расшифрование в режиме гаммирования с обратной связью по выходу показано на рисунке 6.

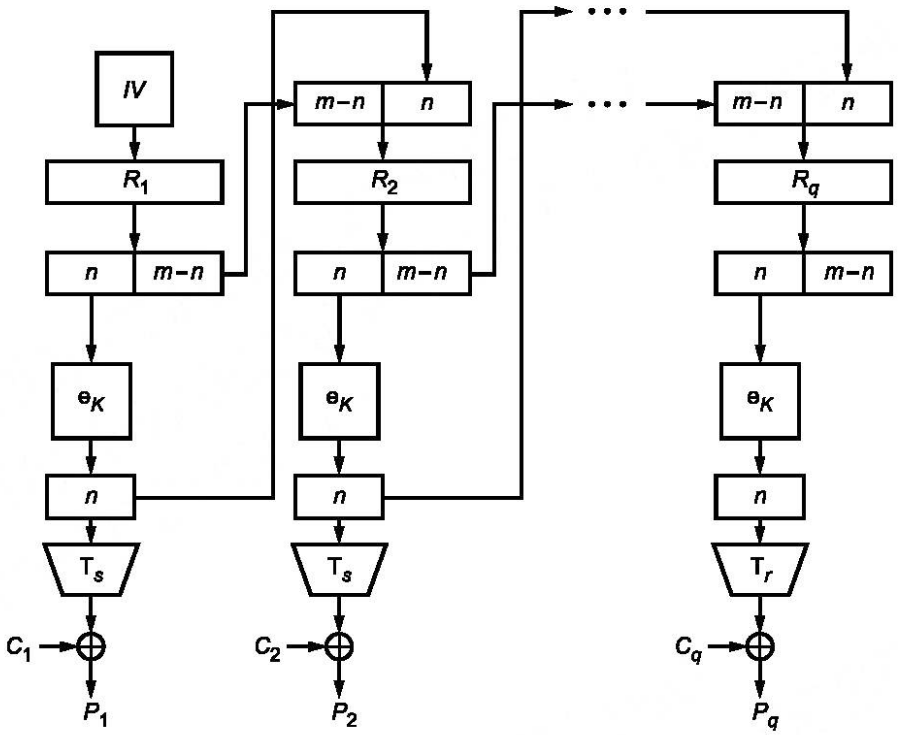

Рисунок 6 — Расшифрование в режиме гаммирования с обратной связью по выходу

5.4 Режим простой замены с зацеплением

5.4.1 Общие положения

Параметром режима простой замены с зацеплением является целочисленная величина m, $m = n \cdot z$, $z \geq 1$ — целое число.

Длина сообщений, зашифровываемых в режиме простой замены с зацеплением, должна быть кратна длине блока базового алгоритма блочного шифрования n, поэтому при необходимости к исходному сообщению должна быть предварительно применена процедура дополнения.

При шифровании на одном ключе для каждого отдельного открытого текста используется значение непредсказуемой (случайной или псевдослучайной) синхропосылки $IV \in V_m$.

При шифровании в режиме простой замены с зацеплением используется двоичный регистр сдвига R длины m. Начальным заполнением регистра является значение синхропосылки IV.

В режиме простой замены с зацеплением очередной блок шифртекста получается путем зашифрования результата покомпонентного сложения значения очередного блока открытого текста со значением n разрядов регистра сдвига с бóльшими номерами. Затем регистр сдвигается на один блок в сторону разрядов с бóльшими номерами. В разряды с меньшими номерами записывается значение блока шифртекста.

5.4.2 Зашифрование

Открытый и при необходимости дополненный текст $P \in V^*$, $|P| = n \cdot q$, представляется в виде: $P = P_1 \| P_2 \| \ldots \| P_q$, $P_i \in V_n$, $i = 1, 2, \ldots, q$. Блоки шифртекста вычисляются по следующему правилу:

$$
\begin{aligned}
&R_1 = IV,\\
&\begin{cases} C_i = \mathrm{e}_K(P_i \oplus \mathrm{MSB}_n(R_i)), \\ R_{i+1} = \mathrm{LSB}_{m-n}(R_i) \| C_i, \end{cases} \quad i = 1, 2, \ldots, q-1, \\
&C_q = \mathrm{e}_K(P_q \oplus \mathrm{MSB}_n(R_q)).
\end{aligned}
\tag{8}
$$

Результирующий шифртекст имеет вид:

$$C = C_1 \| C_2 \| \ldots \| C_q.$$

Зашифрование в режиме простой замены с зацеплением показано на рисунке 7.

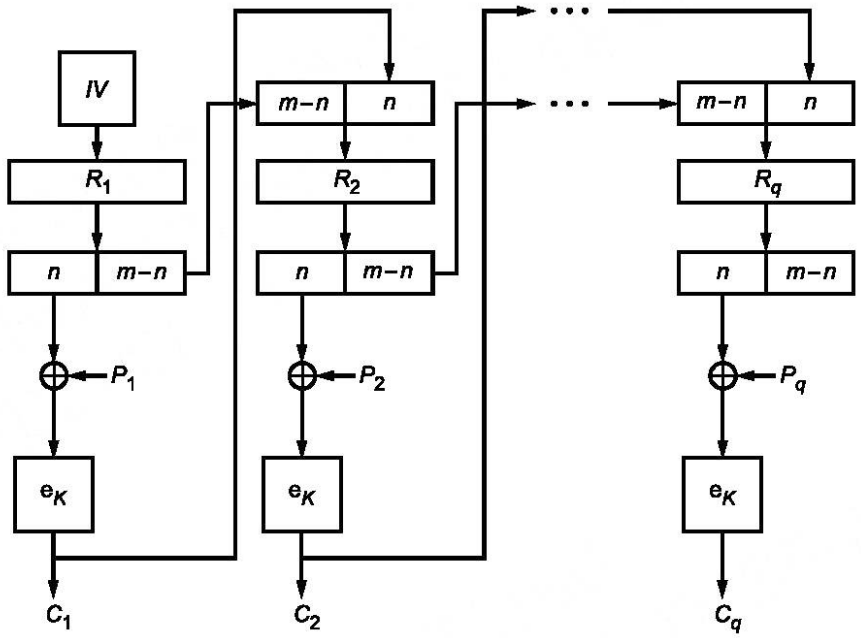

Рисунок 7 — Зашифрование в режиме простой замены с зацеплением

5.4.3 Расшифрование

Шифртекст представляется в виде $C = C_1 \| C_2 \| \ldots \| C_q$, $C_i \in V_n$, $i = 1, 2, \ldots, q$. Блоки открытого текста вычисляются по следующему правилу:

$$\begin{aligned} &R_1 = IV, \\ &\begin{cases} P_i = \mathrm{d}_K(C_i) \oplus \mathrm{MSB}_n(R_i), \\ R_{i+1} = \mathrm{LSB}_{m-n}(R_i) \| C_i, \end{cases} \quad i = 1, 2, \ldots, q-1, \\ &P_q = \mathrm{d}_K(C_q) \oplus \mathrm{MSB}_n(R_q). \end{aligned} \tag{9}$$

Исходный (дополненный) открытый текст имеет вид:

$$P = P_1 \| P_2 \| \ldots \| P_q.$$

Примечание — Если к исходному открытому тексту была применена процедура дополнения, то после расшифрования следует провести обратную процедуру. Для однозначного восстановления сообщения может потребоваться знание длины исходного сообщения.

Расшифрование в режиме простой замены с зацеплением показано на рисунке 8.

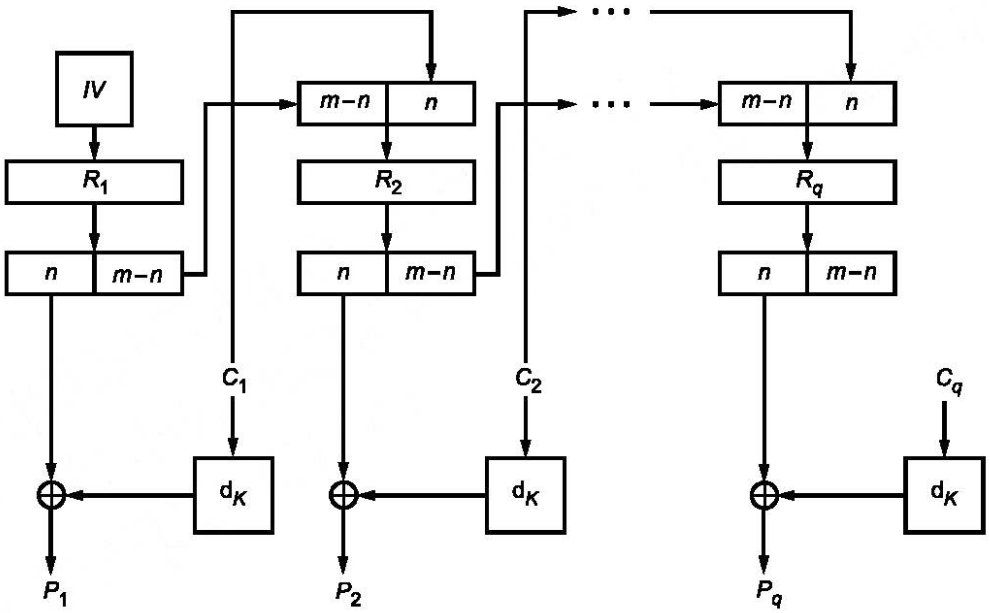

Рисунок 8 — Расшифрование в режиме простой замены с зацеплением

5.5 Режим гаммирования с обратной связью по шифртексту

5.5.1 Общие положения

Параметрами режима гаммирования с обратной связью по шифртексту являются целочисленные величины s и m, $0 < s \le n$, $n \le m$.

В конкретной системе обработки информации на длину сообщения P может как накладываться ограничение $|P| = s \cdot q$, так и не накладываться никаких ограничений. В случае если такое ограничение накладывается, к исходному сообщению при необходимости должна быть предварительно применена процедура дополнения.

При шифровании на одном ключе для каждого отдельного открытого текста используется значение непредсказуемой (случайной или псевдослучайной) синхропосылки $IV \in V_m$.

При шифровании в режиме гаммирования с обратной связью по шифртексту используется двоичный регистр сдвига R длины m. Начальным заполнением регистра является значение синхропосылки IV.

Зашифрование в режиме гаммирования с обратной связью по шифртексту заключается в покомпонентном сложении открытого текста с гаммой шифра, которая вырабатывается блоками длины s. При вычислении очередного блока гаммы выполняется зашифрование n разрядов регистра сдвига с бóльшими номерами базовым алгоритмом блочного шифрования с последующим усечением. Затем заполнение регистра сдвигается на s разрядов в сторону разрядов с бóльшими номерами, при этом в разряды с меньшими номерами записывается полученный блок шифртекста, являющийся результатом покомпонентного сложения гаммы шифра и блока открытого текста.

5.5.2 Зашифрование

Открытый текст $P \in V^*$ представляется в виде $P = P_1 \| P_2 \| \ldots \| p_q$, $P_i \in V_s$, $i = 1, 2, \ldots, q-1$, $P_q \in V_r$, $r \le s$. Блоки шифртекста вычисляются по следующему правилу:

$$\begin{aligned} &R_1 = IV, \\ &\begin{cases} C_i = P_i \oplus \mathrm{T}_s(\mathrm{e}_K(\mathrm{MSB}_n(R_i))), \\ R_{i+1} = \mathrm{LSB}_{m-n}(R_i) \| C_i, \end{cases} \quad i = 1, 2, \ldots, q-1, \\ &C_q = P_q \oplus \mathrm{T}_r(\mathrm{e}_K(\mathrm{MSB}_n(R_q))). \end{aligned} \tag{10}$$

Результирующий шифртекст имеет вид:

$$C = C_1 \| C_2 \| \ldots \| C_q.$$

Зашифрование в режиме гаммирования с обратной связью по шифртексту показано на рисунке 9.

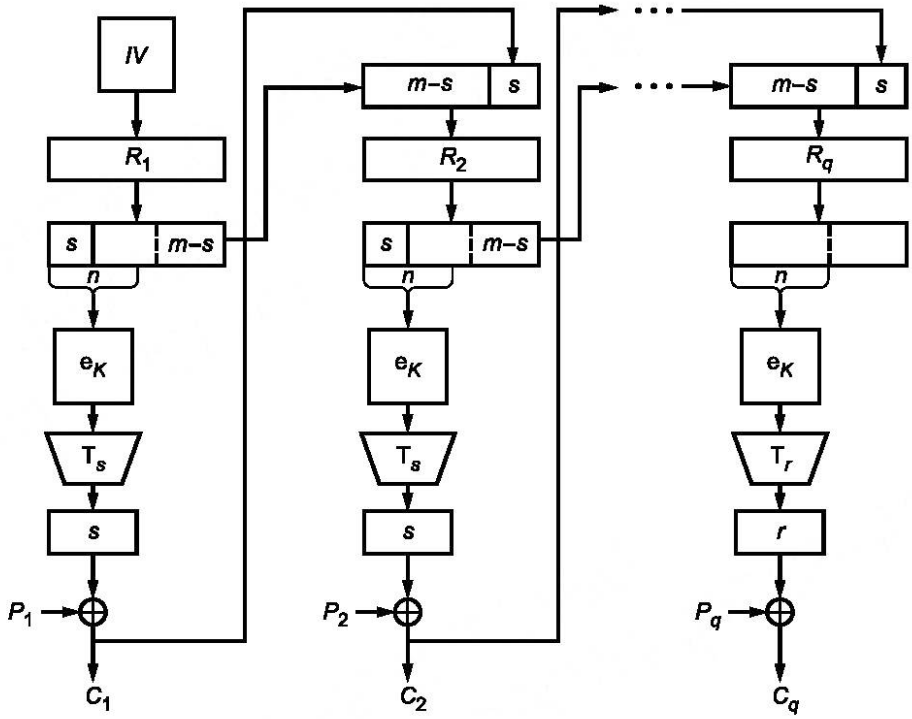

Рисунок 9 — Зашифрование в режиме гаммирования с обратной связью по шифртексту

5.5.3 Расшифрование

Шифртекст представляется в виде: $C = C_1 \| C_2 \| \ldots \| C_q$, $C_i \in V_s$, $i = 1, 2, \ldots, q-1$, $C_q \in V_r$, $r \le s$. Блоки открытого текста вычисляются по следующему правилу:

$$\begin{aligned} &R_1 = IV, \\ &\begin{cases} P_i = C_i \oplus \mathrm{T}_s(\mathrm{e}_K(\mathrm{MSB}_n(R_i))), \\ R_{i+1} = \mathrm{LSB}_{m-n}(R_i) \| C_i, \end{cases} \quad i = 1, 2, \ldots, q-1, \\ &P_q = C_q \oplus \mathrm{T}_r(\mathrm{e}_K(\mathrm{MSB}_n(R_q))). \end{aligned} \tag{11}$$

Исходный открытый текст имеет вид:

$$P = P_1 \| P_2 \| \ldots \| P_q.$$

Примечание — Если к исходному открытому тексту была применена процедура дополнения, то после расшифрования следует провести обратную процедуру. Для однозначного восстановления сообщения может потребоваться знание длины исходного сообщения.

Расшифрование в режиме гаммирования с обратной связью по шифртексту показано на рисунке 10.

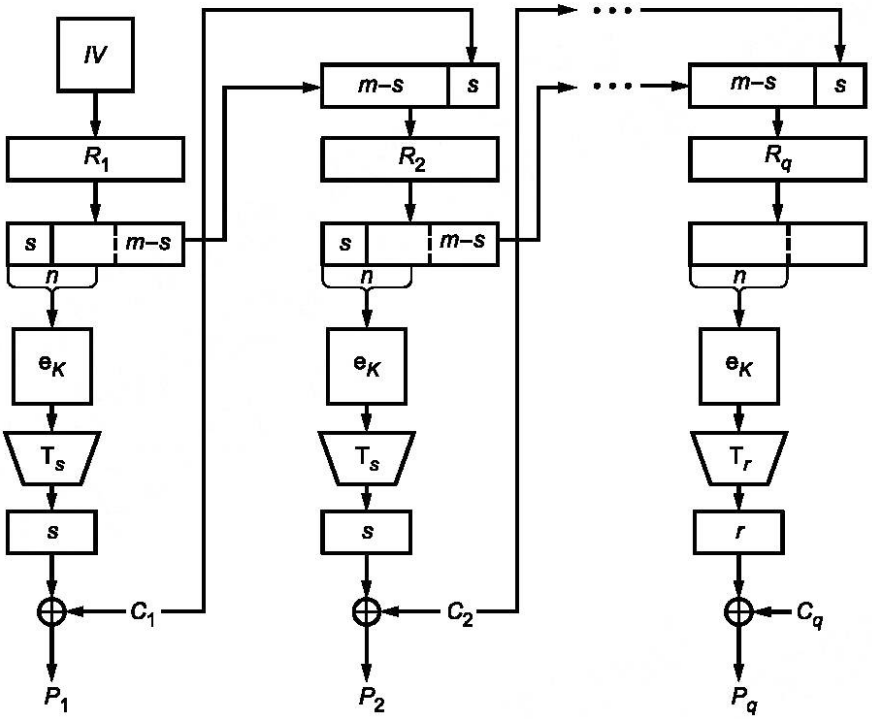

Рисунок 10 — Расшифрование в режиме гаммирования с обратной связью по шифртексту

5.6 Режим выработки имитовставки

5.6.1 Общие положения

Режим выработки имитовставки, описание которого представлено ниже, реализует конструкцию OMAC1 (стандартизован в ISO под названием CMAC [1]).

Параметром режима является длина имитовставки (в битах) $0 < s \le n$.

5.6.2 Выработка вспомогательных ключей

При вычислении значения имитовставки используются вспомогательные ключи, которые вычисляются с использованием ключа K. Длины вспомогательных ключей равны длине блока n базового алгоритма блочного шифрования.

Процедура выработки вспомогательных ключей может быть представлена в следующем виде:

$$R = \mathrm{e}_K(0^n);$$

$$K_1 = \begin{cases} R \ll 1, & \text{если } \mathrm{MSB}_1(R) = 0, \\ (R \ll 1) \oplus B_n, & \text{иначе;} \end{cases}$$

$$K_2 = \begin{cases} K_1 \ll 1, & \text{если } \mathrm{MSB}_1(K_1) = 0, \\ (K_1 \ll 1) \oplus B_n, & \text{иначе,} \end{cases}$$

где $B_{64} = 0^{59} \| 11011$, $B_{128} = 0^{120} \| 10000111$.

Если значение n отлично от 64 и 128, необходимо использовать следующую процедуру определения значения константы B_n. Рассмотрим множество примитивных многочленов степени n над полем GF(2) с наименьшим количеством ненулевых коэффициентов. Упорядочим это множество лексикографически по возрастанию векторов коэффициентов и обозначим через $f_n(x)$ первый многочлен в этом упорядоченном множестве.

Рассмотрим поле $GF(2^n)[x]/(f_n(x))$, зафиксируем в нем степенной базис и будем обозначать операцию умножения в этом поле символом $\otimes$. Вспомогательные ключи K_1 и K_2 вычисляются следующим образом:

$$\begin{cases} R = e_K(0^n), \\ K_1 = \mathrm{Poly}_n^{-1}(\mathrm{Poly}_n(R) \otimes x), \\ K_2 = \mathrm{Poly}_n^{-1}(\mathrm{Poly}_n(R) \otimes x^2). \end{cases} \quad (12)$$

Примечание — Вспомогательные ключи K_1 и K_2 и промежуточное значение R наряду с ключом K являются секретными параметрами. Компрометация какого-либо из этих значений приводит к возможности построения эффективных методов анализа всего алгоритма.

5.6.3 Вычисление значения имитовставки

Процедура вычисления значения имитовставки похожа на процедуру зашифрования в режиме простой замены с зацеплением при $m = n$ и инициализации начального заполнения регистра сдвига значением 0^n: на вход алгоритму шифрования подается результат покомпонентного сложения очередного блока текста и результата зашифрования на предыдущем шаге. Основное отличие заключается в процедуре обработки последнего блока: на вход базовому алгоритму блочного шифрования подается результат покомпонентного сложения последнего блока, результата зашифрования на предыдущем шаге и одного из вспомогательных ключей. Конкретный вспомогательный ключ выбирается в зависимости от того, является ли последний блок исходного сообщения полным или нет. Значением имитовставки MAC является результат применения процедуры усечения к выходу алгоритма шифрования при обработке последнего блока.

Исходное сообщение $P \in V^*$, для которого требуется вычислить имитовставку, представляется в виде:

$$P = P_1 \| P_2 \| \ldots \| P_q,$$

где $P_i \in V_n$, $i = 1, 2, \ldots, q-1$, $P_q \in V_r$, $r \le n$.

Процедура вычисления имитовставки описывается следующим образом:

$$\begin{aligned} &C_0 = 0^n, \\ &C_i = \mathrm{e}_K(P_i \oplus C_{i-1}),\ i = 1, 2, \ldots, q-1, \\ &\mathrm{MAC} = \mathrm{T}_s(\mathrm{e}_K(P_q^* \oplus C_{q-1} \oplus K^*)), \end{aligned} \quad (13)$$

где

$$K^* = \begin{cases} K_1, \text{ если } |P_q| = n, \\ K_2, \text{ иначе,} \end{cases}$$

P_q^* — последний блок сообщения, полученного в результате дополнения исходного сообщения с помощью процедуры 3.

Примечание — Настоятельно рекомендуется не использовать ключ режима выработки имитовставки в других криптографических алгоритмах, в том числе в режимах, обеспечивающих конфиденциальность, описанных в 5.1—5.5.

Процедура вычисления имитовставки показана на рисунках 11—13.

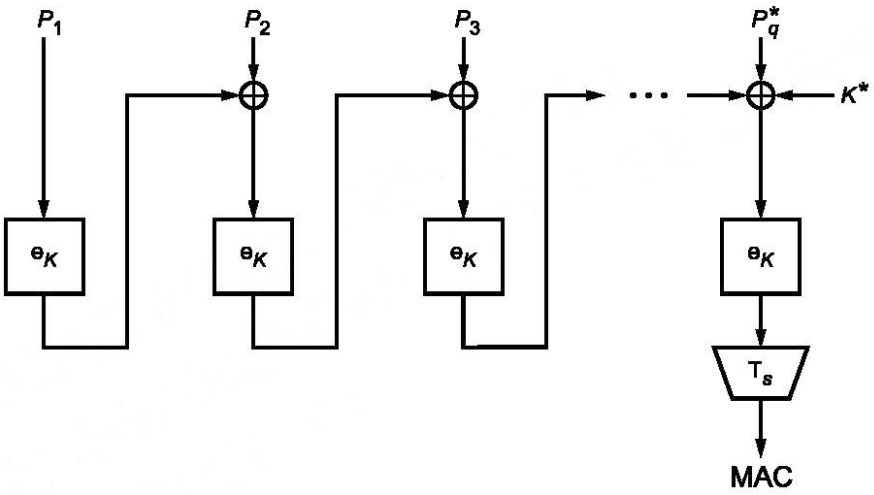

Рисунок 11 — Вычисление значения имитовставки — общий вид

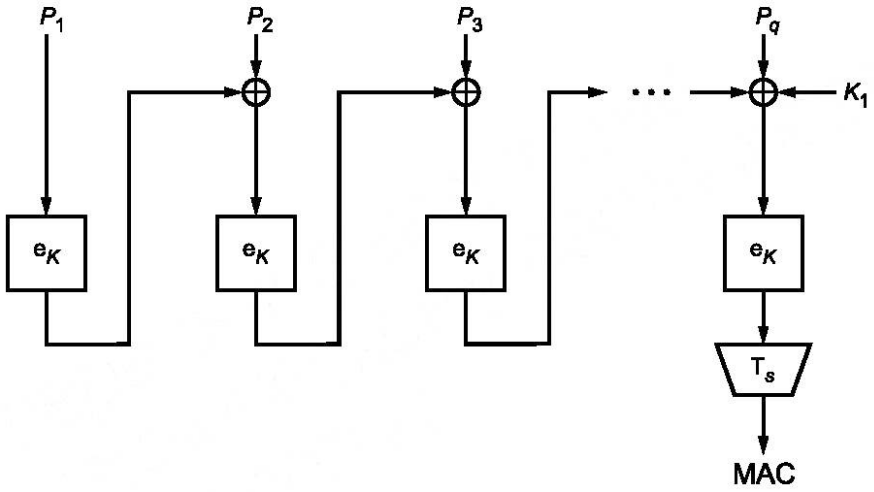

Рисунок 12 — Вычисление значения имитовставки — случай полного последнего блока

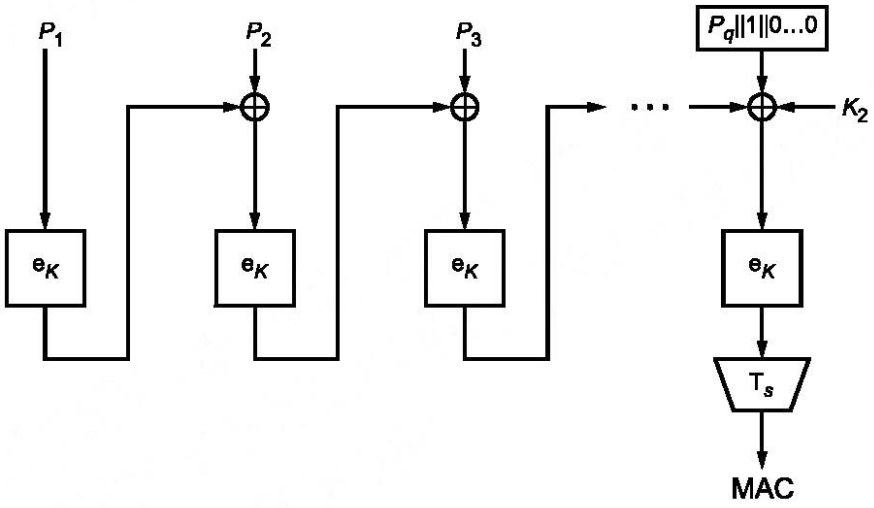

Рисунок 13 — Вычисление значения имитовставки — случай с дополнением последнего блока

Приложение А
(справочное)

Контрольные примеры

А.1 Общие положения

Настоящее приложение носит справочный характер и не является частью нормативных положений настоящего стандарта.

В настоящем приложении содержатся примеры для зашифрования и расшифрования сообщений, а также выработки имитовставки с использованием режимов работы шифра, определенных в настоящем стандарте. Параметр s выбран равным n в целях упрощения проводимых вычислений, а параметр m выбирался из соображений демонстрации особенностей каждого режима шифрования. Двоичные строки из V^*, длина которых кратна 4, записываются в шестнадцатеричном виде, а символ конкатенации ("||") опускается. Таким образом, строка $a \in V_{4r}$ будет представлена в виде $a_{r-1}a_{r-2}\dots a_0$, где $a_i \in \{0, 1, \dots, 9, a, b, c, d, e, f\}$, $i = 0, 1, \dots, r-1$.

В А.2 приведены примеры для блочного шифра с длиной блока n = 128 бит («Кузнечик»). В А.3 приведены примеры для блочного шифра с длиной блока n = 64 бит («Магма»).

А.2 Блочный шифр с длиной блока n = 128 бит

А.2.1 Параметры процессов

Примеры используют следующие параметры:

Ключ

K = 8899aabbccddeeff0011223344556677fedcba98765432100123456789abcdef.

Открытый текст — четыре 128-битных блока:

P_1 = 1122334455667700ffeeddccbbaa9988,

P_2 = 00112233445566778899aabbcceeff0a,

P_3 = 11223344556677889aabbcceeff0a00,

P_4 = 2233445566778899aabbcceeff0a0011.

А.2.2 Режим простой замены

Таблица А.1 — Зашифрование в режиме простой замены

Открытый текст	Шифртекст
1122334455667700ffeeddccbbaa9988	7f679d90bebc24305a468d42b9d4edcd
00112233445566778899aabbcceeff0a	b429912c6e0032f9285452d76718d08b
11223344556677889aabbcceeff0a00	f0ca33549d247ceef3f5a5313bd4b157
2233445566778899aabbcceeff0a0011	d0b09ccde830b9eb3a02c4c5aa8ada98

А.2.3 Режим гаммирования

А.2.3.1 Зашифрование

$s = n$ = 128,

IV = 1234567890abcef.

Таблица А.2 — Зашифрование в режиме гаммирования

i	1	2
P_i	1122334455667700ffeeddccbbaa9988	00112233445566778899aabbcceeff0a
Входной блок	1234567890abcef00000000000000000	1234567890abcef00000000000000001
Выходной блок	e0b7ebfa9468a6db2a95826efb173830	85ffc500b2f4582a7ba54e08f0ab21ee
C_i	f195d8bec10ed1dbd57b5fa240bda1b8	85eee733f6a13e5df33ce4b33c45dee4

Окончание таблицы А.2

i	3	4
P_i	112233445566778899aabbcceeff0a00	2233445566778899aabbcceeff0a0011
Входной блок	1234567890abcef00000000000000002	1234567890abcef00000000000000003
Выходной блок	b4c8dbcfb353195b4c42cc3ddb9ba9a5	e9a2bee4947b322f7b7d1db6dfb7ba62
C_i	a5eae88be6356ed3d5e877f13564a3a5	cb91fab1f20cbab6d1c6d15820bdba73

А.2.3.2 Расшифрование

С использованием приведенных значений K, IV и C с помощью операции расшифрования воспроизводятся исходные значения P_1, P_2, P_3, P_4.

А.2.4 Режим гаммирования с обратной связью по выходу

А.2.4.1 Зашифрование

$s = n = 128$, $m = 2n = 256$,

IV = 1234567890abcef0a1b2c3d4e5f00112233445566778899012131415161718 19.

Таблица А.3 — Зашифрование в режиме гаммирования с обратной связью по выходу

i	1	2
P_i	1122334455667700ffeeddccbbaa9988	00112233445566778899aabbcceeff0a
Входной блок	1234567890abcef0a1b2c3d4e5f00112	23344556677889901213141516171819
Выходной блок	90a2391de4e25c2400f1a49232d0241d	ed4a659440d99cc3072c8b8d517dd9b5
C_i	81800a59b1842b24ff1f795e897abd95	ed5b47a7048cfab48fb521369d9326bf

Окончание таблицы А.3

i	3	4
P_i	112233445566778899aabbcceeff0a00	2233445566778899aabbcceeff0a0011
Входной блок	90a2391de4e25c2400f1a49232d0241d	ed4a659440d99cc3072c8b8d517dd9b5
Выходной блок	778064e869c6cf3951a55c30fed78013	020dff9500640ef90a92eead099a3141
C_i	66a257ac3ca0b8b1c80fe7fc10288a13	203ebbc066138660a0292243f6903150

А.2.4.2 Расшифрование

С использованием приведенных значений K, IV и C с помощью операции расшифрования воспроизводятся исходные значения P_1, P_2, P_3, P_4.

А.2.5 Режим простой замены с зацеплением

А.2.5.1 Зашифрование

$m = 2n = 256$,

IV = 1234567890abcef0a1b2c3d4e5f00112233445566778899012131415161718 19.

Таблица А.4 — Зашифрование в режиме простой замены с зацеплением

i	1	2
P_i	1122334455667700ffeeddccbbaa9988	00112233445566778899aabbcceeff0a
Входной блок	0316653cc5cdb9f05e5c1e185e5a989a	23256765232defe79a8abeaedaf9e713
Выходной блок	689972d4a085fa4d90e52e3d6d7dcc27	2826e661b478eca6af1e8e448d5ea5ac
C_i	689972d4a085fa4d90e52e3d6d7dcc27	2826e661b478eca6af1e8e448d5ea5ac

Окончание таблицы А.4

i	3	4
P_i	112233445566778899aabbcceeff0a00	2233445566778899aabbcceeff0a0011
Входной блок	79bb4190f5e38dc5 094f95f18382c627	0a15a234d20f643f05a542aa7254a5bd
Выходной блок	fe7babf1e91999e85640e8b0f49d90d0	167688065a895c631a2d9a1560b63970
C_i	fe7babf1e91999e85640e8b0f49d90d0	167688065a895c631a2d9a1560b63970

А.2.5.2 Расшифрование

С использованием приведенных значений K, IV и C с помощью операции расшифрования воспроизводятся исходные значения P_1, P_2, P_3, P_4.

А.2.6 Режим гаммирования с обратной связью по шифртексту

А.2.6.1 Зашифрование

$s = n = 128$, $m = 2n = 256$,

IV = 1234567890abcef0a1b2c3d4e5f00112233445566778899012131415161718 19.

Таблица А.5 — Зашифрование в режиме гаммирования с обратной связью по шифртексту

i	1	2
P_i	1122334455667700ffeeddccbbaa9988	00112233445566778899aabbcceeff0a
Входной блок	1234567890abcef0a1b2c3d4e5f00112	23344556677889901213141516171819
Выходной блок	90a2391de4e25c2400f1a49232d0241d	ed4a659440d99cc3072c8b8d517dd9b5
C_i	81800a59b1842b24ff1f795e897abd95	ed5b47a7048cfab48fb521369d9326bf

Окончание таблицы А.5

i	3	4
P_i	112233445566778899aabbcceeff0a00	2233445566778899aabbcceeff0a0011
Входной блок	81800a59b1842b24ff1f795e897abd95	ed5b47a7048cfab48fb521369d9326bf
Выходной блок	68d09baf09a0fab01d879d82795d32b5	6dcdfa9828e5a57f6de01533bbf1f4c0
C_i	79f2a8eb5cc68d38842d264e97a238b5	4ffebecd4e922de6c75bd9dd44fbf4d1

А.2.6.2 Расшифрование

С использованием приведенных значений K, IV и C с помощью операции расшифрования воспроизводятся исходные значения P_1, P_2, P_3, P_4.

А.2.7 Режим выработки имитовставки

А.2.7.1 Выработка вспомогательных ключей

R = 94bec15e269cf1e506f02b994c0a8ea0,

$\mathrm{MSB}_1(R) = 1$,

$K_1 = R \ll 1 \oplus B_n$ = 297d82bc4d39e3ca0de0573298151d40 $\oplus$ 87 = 297d82bc4d39e3ca0de0573298151dc7,

$\mathrm{MSB}_1(K_1) = 0$,

$K_2 = K_1 \ll 1 = 297d82bc4d39e3ca0de0573298151dc \ll 1$ = 52fb05789a73c7941bc0ae65302a3b8e,

$|P_4| = n$, $K^* = K_1$.

А.2.7.2 Вычисление имитовставки

s = 64.

Таблица А.6 — Вычисление имитовставки

i	1	2
P_i	1122334455667700ffeeddccbbaa9988	00112233445566778899aabbcceeff0a
Входной блок	1122334455667700ffeeddccbbaa9988	7f76bfa3fae94247d2df27f9753a12c7
Выходной блок	7f679d90bebc24305a468d42b9d4edcd	1ac9d976f83636f55ae9ef305e7c90d2

Окончание таблицы А.6

i	3	4
P_i	112233445566778899aabbcceeff0a00	2233445566778899aabbcceeff0a0011
Входной блок	0beba32ad50417dc34354fcb0839ad2	1e2a9c1d8cc03bfa0cb340971252fe24
Выходной блок	15645af4a78e50a9abe8db4b754de3f2	336f4d296059fbe34ddeb35b37749c67

MAC = 336f4d296059fbe3.

А.3 Блочный шифр с длиной блока n = 64 бит

А.3.1 Используемые параметры

Примеры используют следующие параметры:

Ключ

K = ffeeddccbbaa99887766554433221100f0f1f2f3f4f5f6f7f8f9fafbfcfdfeff.

Открытый текст — четыре 64-битных блока:

P_1 = 92def06b3c130a59,

P_2 = db54c704f8189d20,

P_3 = 4a98fb2e67a8024c,

P_4 = 8912409b17b57e41.

А.3.2 Режим простой замены

Таблица А.7 — Зашифрование в режиме простой замены

Открытый текст	Шифртекст
92def06b3c130a59	2b073f0494f372a0
db54c704f8189d20	de70e715d3556e48
4a98fb2e67a8024c	11d8d9e9eacfbc1e
8912409b17b57e41	7c68260996c67efb

А.3.3 Режим гаммирования

А.3.3.1 Зашифрование

$s = n$ = 64,

IV = 12345678.

Таблица А.8 — Зашифрование в режиме гаммирования

i	1	2
P_i	92def06b3c130a59	db54c704f8189d20
Входной блок	1234567800000000	1234567800000001
Выходной блок	dc46e167aba4b365	e571ca972ef0c049
C_i	4e98110c 97b7b93c	3e250d93d6e85d69

Окончание таблицы А.8

i	3	4
P_i	4a98fb2e67a8024c	8912409b17b57e41
Входной блок	1234567800000002	1234567800000003
Выходной блок	59f57da6601ad9a3	df9cf61bbce7df6c
C_i	136d868807b2dbef	568eb680ab52a12d

А.3.3.2 Расшифрование

С использованием приведенных значений *K*, *IV* и *C* с помощью операции расшифрования воспроизводятся исходные значения P_1, P_2, P_3, P_4.

А.3.4 Режим гаммирования с обратной связью по выходу

А.3.4.1 Зашифрование

$s = n = 64$, $m = 2n = 128$,

IV = 1234567890abcdef234567890abcdef1.

Таблица А.9 — Зашифрование в режиме гаммирования с обратной связью

i	1	2
P_i	92def06b3c130a59	db54c704f8189d20
Входной блок	1234567890abcdef	234567890abcdef1
Выходной блок	49e910895a8336da	d612a348e78295bc
C_i	db37e0e266903c83	0d46644c1f9a089c

Окончание таблицы А.9

i	3	4
P_i	4a98fb2e67a8024c	8912409b17b57e41
Входной блок	49e910895a8336da	d612a348e78295bc
Выходной блок	ea60cb4c24a63032	4136af23aafaa544
C_i	a0f83062430e327e	c824efb8bd4fdb05

А.3.4.2 Расшифрование

С использованием приведенных значений *K*, *IV* и *C* с помощью операции расшифрования воспроизводятся исходные значения P_1, P_2, P_3, P_4.

А.3.5 Режим простой замены с зацеплением

А.3.5.1 Зашифрование

$m = 3n = 192$,

IV = 1234567890abcdef234567890abcdef134567890abcdef12.

Таблица А.10 — Зашифрование в режиме простой замены с зацеплением

i	1	2
P_i	92def06b3c130a59	db54c704f8189d20
Входной блок	80eaa613acb8c7b6	f811a08df2a443d1
Выходной блок	96d1b05eea683919	aff76129abb937b9
C_i	96d1b05eea683919	aff76129abb937b9

Окончание таблицы А.10

i	3	4
P_i	4a98fb2e67a8024c	8912409b17b57e41
Входной блок	7ece83becc65ed5e	1fc3f0c5fddd4758
Выходной блок	5058b4a1c4bc0019	20b78b1a7cd7e667
C_i	5058b4a1c4bc0019	20b78b1a7cd7e667

А.3.5.2 Расшифрование

С использованием приведенных значений K, IV и C с помощью операции расшифрования воспроизводятся исходные значения P_1, P_2, P_3, P_4.

А.3.6 Режим гаммирования с обратной связью по шифртексту

А.3.6.1 Зашифрование

$s = n = 64$, $m = 2n = 128$,

IV = 1234567890abcdef234567890abcdef1.

Таблица А.11 — Зашифрование в режиме гаммирования с обратной связью по шифртексту

i	1	2
P_i	92def06b3c130a59	db54c704f8189d20
Входной блок	1234567890abcdef	234567890abcdef1
Выходной блок	49e910895a8336da	d612a348e78295bc
C_i	db37e0e266903c83	0d46644c1f9a089c

Окончание таблицы А.11

i	3	4
P_i	4a98fb2e67a8024c	8912409b17b57e41
Входной блок	db37e0e266903c83	0d46644c1f9a089c
Выходной блок	6e25292d34bdd1c7	35d2728f36b22b44
C_i	24bdd2035315d38b	bcc0321421075505

А.3.6.2 Расшифрование

С использованием приведенных значений K, IV и C с помощью операции расшифрования воспроизводятся исходные значения P_1, P_2, P_3, P_4.

А.3.7 Режим выработки имитовставки

А.3.7.1 Выработка вспомогательных ключей

R = 2fa2cd99a1290a12,

$\mathrm{MSB}_1(R) = 0$, $K_1 = R \ll 1 = 5f459b3342521424$,

$\mathrm{MSB}_1(K_1) = 0$, следовательно $K_2 = K_1 \ll 1 = be8b366684a42848$,

$|P_4| = n$, $K^* = K_1$.

А.3.7.2 Вычисление имитовставки

s = 32.

Таблица А.12 — Вычисление имитовставки

i	1	2
P_i	92def06b3c130a59	db54c704f8189d20
Входной блок	92def06b3c130a59	f053f8006cebef80
Выходной блок	2b073f0494f372a0	c89ed814fd5e18e9

Окончание таблицы А.12

i	3	4
P_i	4a98fb2e67a8024c	8912409b17b57e41
Входной блок	8206233a9af61aa5	216e6a2561cff165
Выходной блок	f739b18d34289b00	154e72102030c5bb

MAC = 154e7210.

Библиография

Примечание — Оригиналы международных стандартов ИСО/МЭК находятся в национальных (государственных) органах по стандартизации* государств, принявших настоящий стандарт.

[1] ИСО/МЭК 9797-1:2011 (ISO/IEC 9797-1:2011) Информационные технологии. Методы защиты. Коды аутентификации сообщений (MAC). Часть 1. Механизмы, использующие блочный шифр (Information technology — Security techniques — Message Authentication Codes (MACs) — Part 1: Mechanisms using a block cipher)

[2] ИСО/МЭК 10116:2017 (ISO/IEC 10116:2017) Информационная технология. Методы и средства обеспечения безопасности. Режимы работы для алгорита *n*-разрядного блочного шифрования (Information technology — Security techniques — Modes of operation for an *n*-bit block cipher)

[3] ИСО/МЭК 10118-1:2016 (ISO/IEC 10118-1:2016) Информационная технология. Методы защиты информации. Хэш-функции. Часть 1. Общие положения (Information technology — Security techniques — Hash-functions — Part 1: General)

[4] ИСО/МЭК 18033-1:2015 (ISO/IEC 18033-1:2005) Информационная технология. Технология обеспечения защиты. Алгоритмы кодирования. Часть 1. Общие положения (Information technology — Security techniques — Encryption algorithms — Part 1: General)

[5] ИСО/МЭК 14888-1:2008 (ISO/IEC 14888-1:2008) Информационные технологии. Методы защиты. Цифровые подписи с приложением. Часть 1. Общие положения (Information technology — Security techniques — Digital signatures with appendix — Part 1: General)

* В Российской Федерации оригиналы международных стандартов ИСО/МЭК находятся в Федеральном информационном фонде стандартов.

УДК 681.3.06:006.354 МКС 35.040

Ключевые слова: информационная технология, криптографическая защита информации, блочный шифр, режимы работы блочного шифра, конфиденциальность, целостность, имитовставка, гаммирование, зацепление

БЗ 1—2019/64

Редактор *Л.В. Коретникова*
Технический редактор *В.Н. Прусакова*
Корректор *Е.Р. Ароян*
Компьютерная верстка *Ю.В. Поповой*

Сдано в набор 05.12.2018. Подписано в печать 09.01.2019. Формат 60 × 84 1/8. Гарнитура Ариал.
Усл. печ. л. 3,26. Уч.-изд. л. 2,95.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

ИД «Юриспруденция», 115419, Москва, ул. Орджоникидзе, 11.
www.jurisizdat.ru y-book@mail.ru

Создано в единичном исполнении ФГУП «СТАНДАРТИНФОРМ»
для комплектования Федерального информационного фонда стандартов,
117418 Москва, Нахимовский пр-т, д. 31, к. 2.
www.gostinfo.ru info@gostinfo.ru

МКС 35.040

Изменение № 1 ГОСТ 34.13—2018 Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров

Принято Межгосударственным советом по стандартизации, метрологии и сертификации (протокол № 165-П от 25.09.2023)

Зарегистрировано Бюро по стандартам МГС № 17003

За принятие изменения проголосовали национальные органы по стандартизации следующих государств: AM, KG, RU, TJ, UZ [коды альфа-2 по МК (ИСО 3166) 004]

Дату введения в действие настоящего изменения устанавливают указанные национальные органы по стандартизации*

Предисловие. Пункт 1 дополнить словами: «и Общества с ограниченной ответственностью «КРИПТО-ПРО» (ООО «КРИПТО-ПРО»)».

Пункт 5 изложить в новой редакции:

«5 Настоящий стандарт подготовлен на основе применения ГОСТ Р 34.13—2015, Р 1323565.1.017—2018, Р 1323565.1.026—2019».

Содержание дополнить словами:

«4.4 Процедура преобразования ключа»;

«5.7 Режим гаммирования с преобразованием ключа

5.8 Режим аутентифицированного шифрования с ассоциированными данными».

Подраздел 2.1 дополнить пунктами 2.1.20, 2.1.21, 2.1.22:

«2.1.20 **ассоциированные данные** (associated data): Данные, для которых обеспечивается целостность, но не обеспечивается конфиденциальность.

2.1.21 **зашифрование с выработкой имитовставки** (authenticated encryption): Операция, состоящая из зашифрования открытого текста и вычисления имитовставки от открытого текста и ассоциированных данных, с использованием одного ключа в обоих преобразованиях.

2.1.22 **расшифрование с проверкой имитовставки** (authenticated decryption): Операция, обратная к зашифрованию с выработкой имитовставки, состоящая из проверки имитовставки и последующего расшифрования шифртекста в случае успешного завершения проверки».

Подраздел 2.2 дополнить обозначениями:

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

$\otimes: F \times F \to F$ — отображение, определенное для $F = V_n$ и $F = GF(2)[x]/f_n(x)$, где под многочленом $f_n(x)$ понимается примитивный многочлен степени n над полем $GF(2)$ с наименьшим количеством ненулевых коэффициентов, который является первым в списке таких многочленов, упорядоченных лексикографически по возрастанию векторов коэффициентов. Для $n = 64$ порождающим многочленом является $f_{64}(x) = x^{64} + x^4 + x^3 + x + 1$, для $n = 128$ порождающим многочленом является $f_{128}(x) = x^{128} + x^7 + x^2 + x + 1$.

В случае $F = GF(2)[x]/f_n(x)$ отображение ставит в соответствие двум элементам поля $a(x) \in GF(2)[x]/f_n(x)$ и $b(x) \in GF(2)/f_n(x)$ элемент поля $c(x) \in GF(2)/f_n(x)$, который является результатом умножения элементов $a(x)$ и $b(x)$ в поле $GF(2)[x]/f_n(x)$.

В случае $F = V_n$ отображение ставит в соответствие двум строкам $a = (a_{n-1} \| \cdots \| a_0)$ и $b = (b_{n-1} \| \cdots \| b_0)$, $a, b \in V_n$, строку $c = a \otimes b = (c_{n-1} \| \cdots \| c_0)$, $c \in V_n$; строка c является результатом применения функции Poly_n^{-1} к произведению двух многочленов $\mathrm{Poly}_n(a)$ и $\mathrm{Poly}_n(b)$ в поле $GF(2)[x]/f_n(x)$;

$\mathrm{incr}_l: V_n \to V_n$, n кратно 2 — отображение, ставящее в соответствие строке $L \| R$, где $L, R \in V_{n/2}$, строку $\mathrm{incr}_l(L \| R) = \mathrm{Vec}_{n/2}(\mathrm{Int}_{n/2}(L) \boxplus_{n/2} 1) \| R$;

* Дата введения в действие на территории Российской Федерации — 2023—11—01.

incr_r: $V_n \to V_n$, n кратно 2 — отображение, ставящее в соответствие строке $L \| R$, где $L, R \in V_{n/2}$, строку $\mathrm{incr}_r(L \| R) = L \| \mathrm{Vec}_{n/2}(\mathrm{Int}_{n/2}(R) \boxplus_{n/2} 1)$;

len: $V_s \to V_{n/2}$, n кратно 2 — отображение, ставящее в соответствие строке $a \in V_s$, $s < 2^{n/2}$, строку $\mathrm{len}(a) = \mathrm{Vec}_{n/2}(|a|) \in V_{n/2}$;

I_m — процедура инициализации, определенная в 4.2;

T_s — процедура усечения, определенная в 4.3».

Раздел 3. Первый абзац дополнить перечислениями (перед первым перечислением):

«- режим гаммирования с преобразованием ключа (CTR-ACPKM, англ. Counter Advanced Cryptographic Prolongation of Key Material);

- режим аутентифицированного шифрования с ассоциированными данными (AEAD, англ. Authenticated Encryption with Associated Data)»;

второй абзац изложить в новой редакции:

«Режим гаммирования может использоваться в качестве режима для блочных шифров с длиной блока n, кратной 2, режим гаммирования с преобразованием ключа может использоваться в качестве режима для блочных шифров с длиной блока n, кратной 8, режим аутентифицированного шифрования с ассоциированными данными может использоваться в качестве режима для блочных шифров с длиной блока $n = 64$ и $n = 128$, остальные режимы могут использоваться в качестве режимов для блочных шифров с произвольной длиной блока n».

Подраздел 4.2. Второй абзац. Второе перечисление. Заменить слова: «в режиме гаммирования,» на «в режимах гаммирования, гаммирования с преобразованием ключа, аутентифицированного шифрования с ассоциированными данными».

Раздел 4 дополнить подразделом 4.4:

«**4.4 Процедура преобразования ключа**

Для преобразования ключа используется функция ACPKM, которая принимает на вход ключ K длины $k \le 256$ бит и преобразует его в ключ K' той же длины.

Функция ACPKM использует базовый алгоритм блочного шифрования и определяется следующим образом:

$$K' = \mathrm{ACPKM}(K) = \mathrm{LSB}_k(\mathrm{e}_K(D_1) \| \cdots \| \mathrm{e}_K(D_J)),$$

где $J = \lceil k/n \rceil$, $D_1 \| \cdots \| D_J = \mathrm{LSB}_{J \cdot n}(D)$, $D_1, \ldots, D_J \in V_n$.

Константа $D \in V_{256}$ в шестнадцатеричной системе счисления задана следующим образом:

D = 8081828384858687888898a8b8c8d8e8f909192939495969798999a9b9c9d9e9f».

Раздел 5 дополнить подразделами 5.7, 5.8:

«**5.7 Режим гаммирования с преобразованием ключа**

5.7.1 Общие положения

Параметром, определяющим порядок функционирования режима гаммирования с преобразованием ключа, является длина секции N. Значение N выражено в битах и фиксировано в рамках каждого конкретного протокола, исходя из требований к производительности системы и суммарной длине данных, обработанных на одном ключе. Длина секции N должна быть кратна длине блока n используемого базового алгоритма блочного шифрования. Дополнительный параметр режима гаммирования с преобразованием ключа — это длина блока гаммы s, $0 < s \le n$, выраженная в битах. Величина s должна быть кратна 8 и делить длину блока n.

Режим гаммирования с преобразованием ключа использует функцию ACPKM, определенную в 4.4.

Пусть $P^j \in V^*$, $j = 1, 2, \ldots$, — множество сообщений, подлежащих зашифрованию. При обработке каждого сообщения $P = P^j$, $j = 1, 2, \ldots$, в режиме гаммирования с преобразованием ключа сообщение разбивается на $l = \lceil |P|/N \rceil$ секций и представляется в виде $P = M^1 \| M^2 \| \ldots \| M^l$, где $M^i \in V_N$, $i = 1, 2, \ldots, l-1$, $M^l \in V_w$, $w \le N$. Первая секция каждого сообщения обрабатывается на секционном ключе K^1, который равен начальному ключу K. Для обработки i-й секции каждого сообщения, $i = 2, \ldots, l$, используется секционный ключ K^i, который вычисляется из ключа K^{i-1} с помощью функции ACPKM.

Преобразование ключа в процессе обработки сообщений в режиме гаммирования с преобразованием ключа показано на рисунке 14.

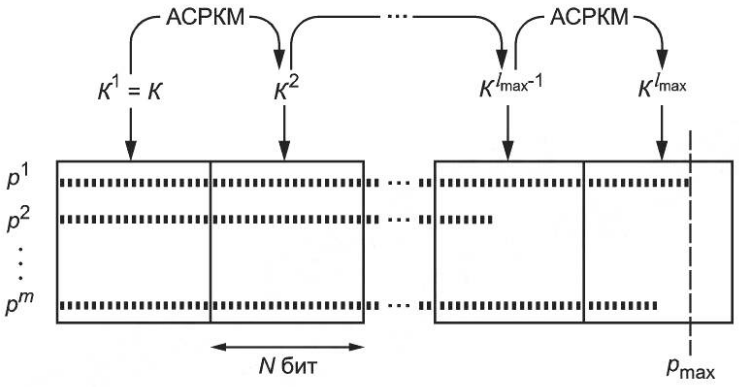

Рисунок 14 — Преобразование ключа в процессе обработки сообщений в режиме гаммирования с преобразованием ключа

Примечание — На рисунке 14 через p_{max} обозначена максимальная длина сообщения, выраженная в битах, $l_{max} = \lceil p_{max}/N \rceil$, m — количество обрабатываемых сообщений.

Для зашифрования (расшифрования) каждого отдельного открытого текста (шифртекста) на одном ключе используется уникальное значение синхропосылки $IV \in V_{n-c}$, где $0 < c < n$, величина c кратна 8.

При использовании режима гаммирования с преобразованием ключа не требуется применение процедуры дополнения сообщения.

Длина p сообщения, обрабатываемого в режиме гаммирования с преобразованием ключа, не должна превышать значения $2^{c-1} \cdot s$ бит.

Зашифрование (расшифрование) открытого текста (шифртекста) в режиме гаммирования с преобразованием ключа заключается в покомпонентном сложении открытого текста с гаммой шифра, которая вырабатывается блоками длины s путем зашифрования последовательности значений счетчика $CTR_i \in V_n$, $i = 1, 2, \ldots$, базовым алгоритмом блочного шифрования с использованием соответствующего секционного ключа с последующим усечением выходного значения. Начальным значением счетчика является $CTR_1 = \mathrm{I}_n(IV) = IV \| 0^c$. Последующие значения счетчика вырабатываются с помощью функции Add: $V_n \to V_n$ следующим образом:

$$CTR_{i+1} = \mathrm{Add}(CTR_i) = \mathrm{Vec}_n(\mathrm{Int}_n(CTR_i) \boxplus_n 1),\ i = 1, 2 \ldots \tag{14}$$

5.7.2 Зашифрование

Открытый текст $P \in V^*$ представляется в виде $P = P_1 \| P_2 \| \cdots \| P_q$, где $P_i \in V_s$, $i = 1, 2, \ldots, q-1$, $P_q \in V_r$, $1 \le r \le s$.

Блоки шифртекста вычисляются по следующему правилу:

$$\begin{gathered} q = \lceil |P|/s \rceil,\ l = \lceil |P|/N \rceil; \\ CTR_1 = IV \| 0^c; \\ CTR_{i+1} = \mathrm{Add}(CTR_i),\ i = 1, 2, 3, \ldots, q-1; \\ K^1 = K; \\ K^j = \mathrm{ACPKM}(K^{j-1}),\ j = 2, 3, \ldots, l; \\ C_i = P_i \oplus \mathrm{T}_s\,(\mathrm{e}_{K^j}\,(CTR_i)),\ i = 1, 2, \ldots, q-1,\ j = \lceil i \cdot s/N \rceil; \\ C_q = P_q \oplus \mathrm{T}_r\,(\mathrm{e}_{K^l}\,(CTR_q)). \end{gathered} \tag{15}$$

Результирующий шифртекст имеет вид:

$$C = C_1 \| C_2 \| \cdots \| C_q.$$

Зашифрование в режиме гаммирования с преобразованием ключа показано на рисунке 15.

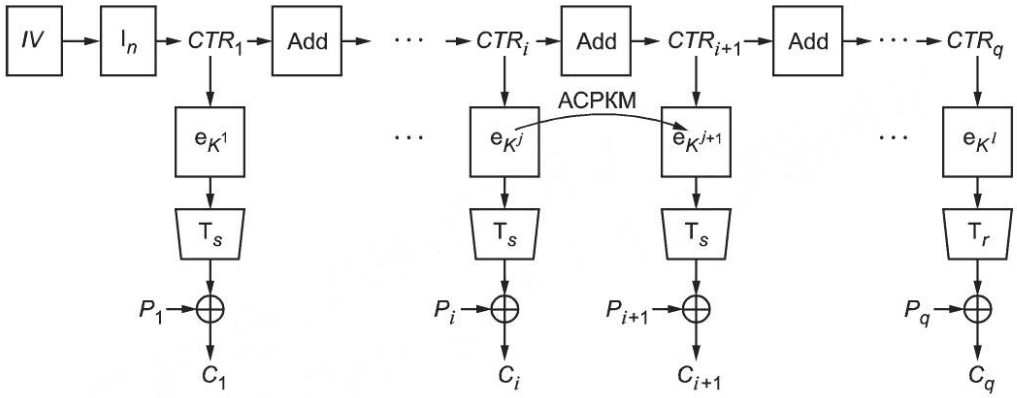

Рисунок 15 — Зашифрование в режиме гаммирования с преобразованием ключа

5.7.3 Расшифрование

Шифртекст представляется в виде: $C = C_1 \| C_2 \| \cdots \| C_q$, где $C_i \in V_s$, $i = 1, 2, \ldots, q-1$, $C_q \in V_r$, $1 \le r \le s$.

Блоки открытого текста вычисляются по следующему правилу:

$$q = \lceil |C|/s \rceil,\ l = \lceil |C|/N \rceil;$$

$$CTR_1 = IV \| 0^c;$$

$$CTR_{i+1} = \mathrm{Add}(CTR_i),\ i = 1, 2, 3, \ldots, q-1;$$

$$K^1 = K;$$

$$K^j = \mathrm{ACPKM}(K^{j-1}),\ j = 2, 3, \ldots, l; \qquad (16)$$

$$P_i = C_i \oplus \mathrm{T}_s(\mathrm{e}_{K^j}(CTR_i)),\ i = 1, 2, \ldots, q-1,\ j = \lceil i \cdot s/N \rceil;$$

$$P_q = C_q \oplus \mathrm{T}_r(\mathrm{e}_{K^l}(CTR_q)).$$

Исходный открытый текст имеет вид:

$$P = P_1 \| P_2 \| \cdots \| P_q.$$

Расшифрование в режиме гаммирования с преобразованием ключа показано на рисунке 16.

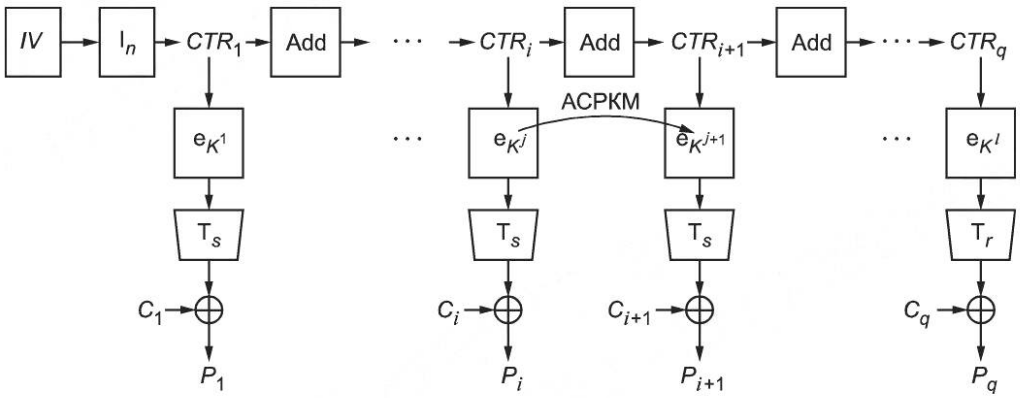

Рисунок 16 — Расшифрование в режиме гаммирования с преобразованием ключа

5.8 Режим аутентифицированного шифрования с ассоциированными данными

В данном подразделе описан режим аутентифицированного шифрования с ассоциированными данными MGM (Multilinear Galois Mode).

5.8.1 Общие положения

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 к стойкости режима относительно угрозы нарушения целостности.

Сообщения состоят из двух частей. Первая часть содержит ассоциированные данные A, а вторая часть — открытый текст P. Одна из двух частей может быть равна пустой строке. Данный режим подразумевает шифрование открытого текста и вычисление имитовставки от шифртекста и ассоциированных данных.

На длину ассоциированных данных и длину открытого текста накладываются следующие ограничения: $0 < |A| + |P| < 2^{n/2}$.

Режим MGM использует синхропосылку $IV \in V_{n-1}$. Значение синхропосылки должно быть уникальным для каждого сообщения при фиксированном ключе K. Выработка уникальных значений синхропосылки может быть реализована с использованием счетчика.

Шифрование в режиме MGM осуществляется путем побитового сложения открытого текста с секретной гаммой, получаемой в результате зашифрования последовательных значений счетчика базовым алгоритмом блочного шифрования. В качестве начального значения счетчика используется значение синхропосылки, дополненное до размера блока нулевым битом слева и зашифрованное базовым алгоритмом блочного шифрования. Вычисление имитовставки от шифртекста и ассоциированных данных в режиме MGM выполняется с помощью мультилинейной функции с секретными коэффициентами, получаемыми в результате зашифрования последовательных значений счетчика базовым алгоритмом блочного шифрования. В качестве начального значения счетчика используется значение синхропосылки, дополненное до размера блока единичным битом слева и базовым алгоритмом блочного шифрования.

5.8.2 Зашифрование с выработкой имитовставки

Открытый текст $P \in V^*$ представляется в виде $P = P_1 \| P_2 \| \cdots \| P_q^*$, где $P_i \in V_n$, $i = 1, 2, \ldots, q-1$, $P_q^* \in V_r$, $1 \le r \le n$. Если длина открытого текста равна нулю, то последний блок открытого текста P_q^* равен пустой строке, а значения параметров q и r установлены следующим образом: $q = 0$, $r = n$. Ассоциированные данные представляются в виде $A = A_1 \| A_2 \| \cdots \| A_h^*$, где $A_j \in V_n$, $j = 1, 2, \ldots, h-1$, $A_h^* \in V_t$, $1 \le t \le n$. Если длина ассоциированных данных равна нулю, то последний блок ассоциированных данных A_h^* равен пустой строке, а значения параметров h и t установлены следующим образом: $h = 0$, $t = n$.

Если длина открытого текста не равна нулю, то блоки шифртекста вычисляются по следующему правилу:

$$\begin{gathered} Y_1 = \mathrm{e}_K(0 \| IV), \\ Y_i = \mathrm{incr}_r(Y_{i-1}),\ i = 2, 3, \ldots, q, \\ C_i = P_i \oplus \mathrm{e}_K(Y_i),\ i = 1, 2, \ldots, q-1, \\ C_q^* = P_q^* \oplus \mathrm{T}_r(\mathrm{e}_K(Y_q)). \end{gathered} \tag{17}$$

Результирующий шифртекст имеет вид:

$$C = C_1 \| C_2 \| \cdots \| C_q^*.$$

Если открытый текст P равен пустой строке, то шифртекст C также принимается равным пустой строке.

К ассоциированным данным A и шифртексту C применяется процедура 1 дополнения сообщения до длины блока n. После применения процедуры дополнения последний блок ассоциированных данных A_h и последний блок шифртекста C_q принимают следующий вид:

$$\begin{aligned} A_h &= A_h^* \| 0^{n-t}, \\ C_q &= C_q^* \| 0^{n-r}. \end{aligned} \tag{18}$$

Значение имитовставки вычисляется по следующему правилу:

$$\begin{gathered} Z_1 = \mathrm{e}_K(1 \| IV), \\ Z_i = \mathrm{incr}_l(Z_{i-1}),\ i = 2, 3, \ldots, h+q+1, \\ H_i = \mathrm{e}_K(Z_i),\ i = 1, 2, \ldots, h+q+1, \end{gathered} \tag{19}$$

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

Результатом вычисления имитовставки является значение MAC.

Зашифрование с выработкой имитовставки в режиме MGM показано на рисунке 17.

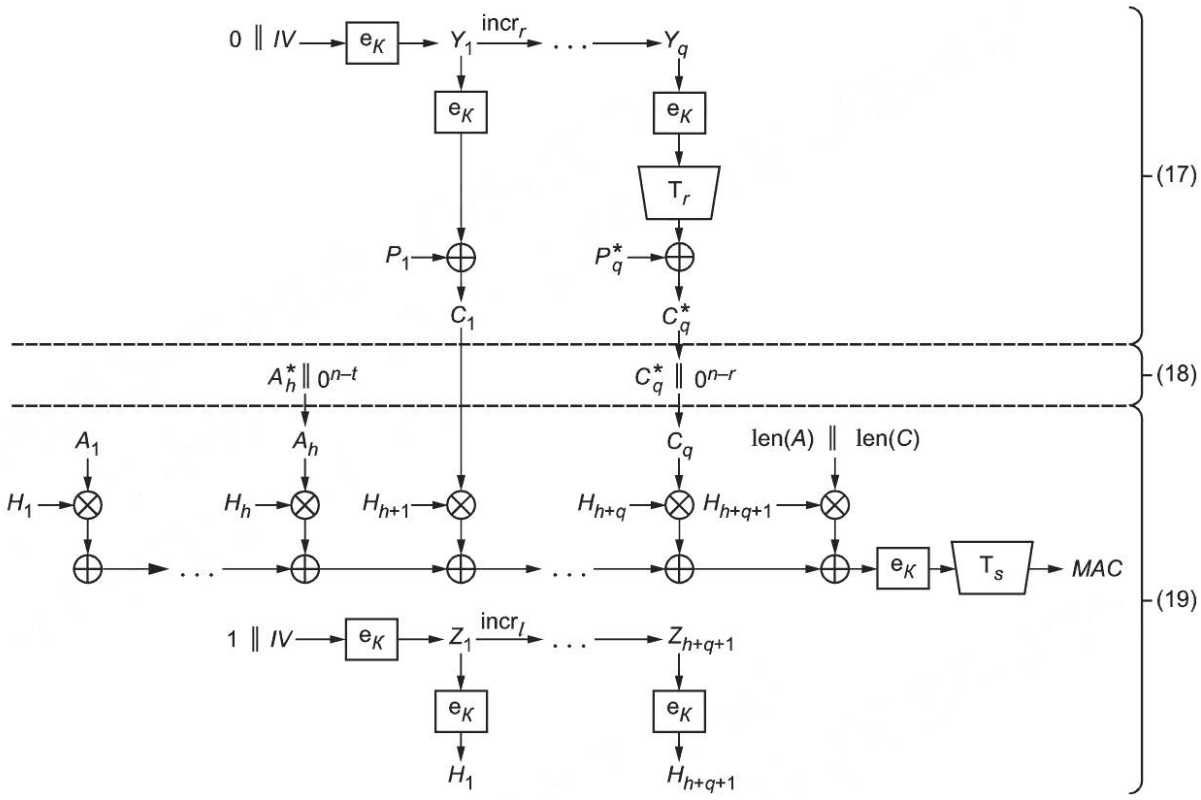

Рисунок 17 — Зашифрование с выработкой имитовставки в режиме MGM

5.8.3 Расшифрование с проверкой имитовставки

Шифртекст представляется в виде: $C = C_1 \| C_2 \| \cdots \| C_q^*$, где $C_j \in V_n$, $i = 1, 2, \ldots, q-1$, $C_q^* \in V_r$, $1 \le r \le n$. Если длина шифртекста равна нулю, то последний блок шифртекста P_q^* равен пустой строке, а значения параметров q и r установлены следующим образом: $q = 0$, $r = n$. Ассоциированные данные представляются в виде: $A = A_1 \| A_2 \| \cdots \| A_h^*$, где $A_j \in V_n$, $j = 1, 2, \ldots, h-1$, $A_h^* \in V_t$, $1 \le t \le n$. Если длина ассоциированных данных равна нулю, то последний блок ассоциированных данных A_h^* равен пустой строке, а значения параметров h и t установлены следующим образом: $h = 0$, $t = n$.

К ассоциированным данным A и шифртексту C применяется процедура 1 дополнения сообщения до длины блока n. После применения процедуры дополнения последний блок ассоциированных данных A_h и последний блок шифртекста C_q принимают следующий вид:

$$A_h = A_h^* \| 0^{n-t},$$
$$C_q = C_q^* \| 0^{n-r}. \qquad (20)$$

Проверка корректности имитовставки выполняется по следующему правилу:

$$Z_1 = \mathrm{e}_K(1 \| IV),$$
$$Z_i = \mathrm{incr}_l(Z_{i-1}),\ i = 2, 3, \ldots, h+q+1,$$
$$H_i = \mathrm{e}_K(Z_i),\ i = 1, 2, \ldots, h+q+1, \qquad (21)$$

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

Если $MAC' \ne MAC$, то в качестве результата расшифрования возвращается ошибка. Если $MAC' = MAC$, то выполняется расшифрование.

Если длина шифртекста не равна нулю, то блоки открытого текста вычисляются по следующему правилу:

$$Y_1 = e_K(0 \| IV),$$
$$Y_i = \mathrm{incr}_r(Y_{i-1}),\ i = 2, 3, \ldots, q,$$
$$P_i = C_i \oplus e_K(Y_i),\ i = 1, 2, \ldots, q-1, \qquad (22)$$
$$P_q^* = C_q^* \oplus T_r(e_K(Y_q)).$$

Исходный открытый текст имеет вид:

$$P = P_1 \| P_2 \| \cdots \| P_q^*.$$

Если шифртекст C равен пустой строке, то открытый текст P также принимается равным пустой строке.

Расшифрование с проверкой имитовставки в режиме MGM показано на рисунке 18.

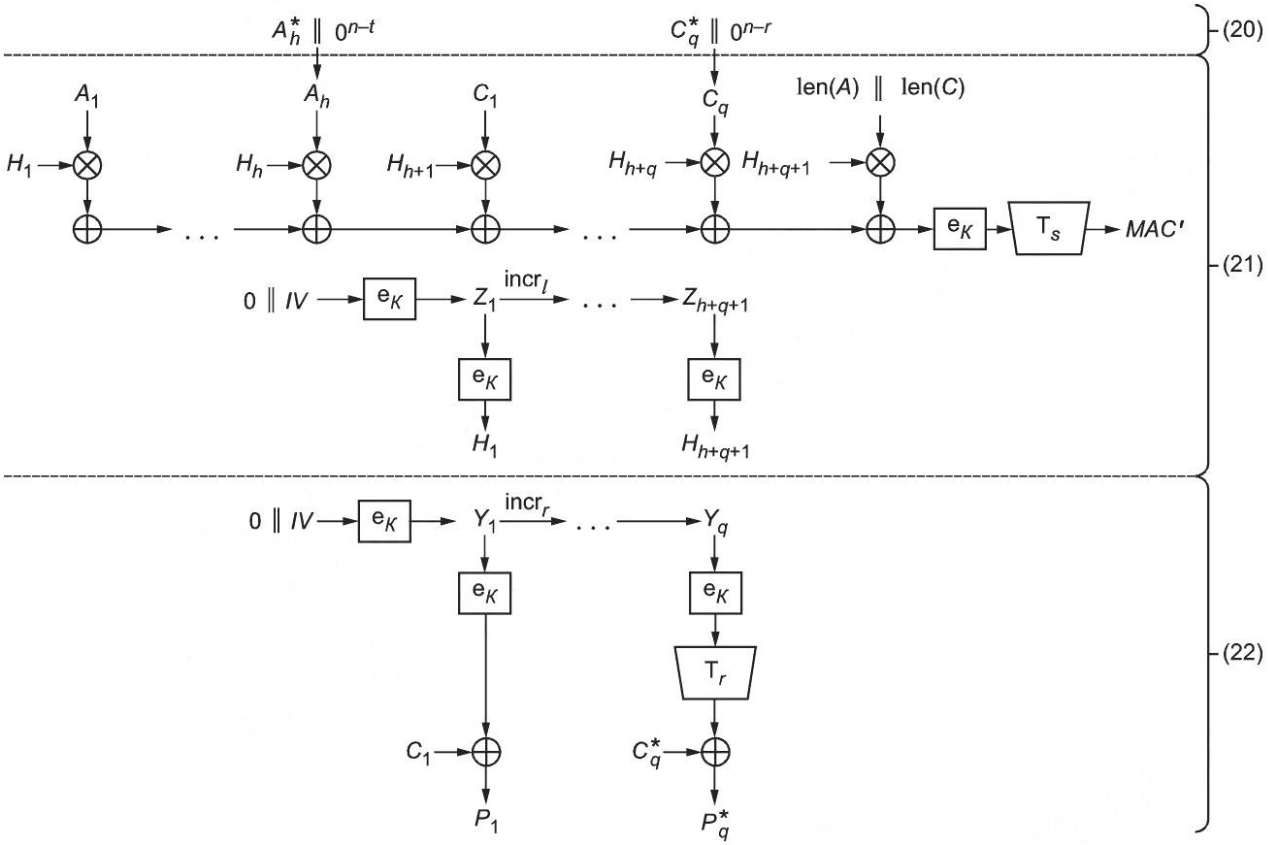

Рисунок 18 — Расшифрование с проверкой имитовставки в режиме MGM».

Приложение А. Пункт А.2.1 исключить.

Пункты А.2.2, А.2.3.1, А.2.4.1, А.2.5.1, А.2.6.1, А.2.7 (после наименования) дополнить абзацем:

«Пример использует следующие параметры:

Ключ

K = 8899aabbccddeeff0011223344556677fedcba98765432100123456789abcdef.

Открытый текст — четыре 128-битных блока:

P_1 = 1122334455667700ffeeddccbbaa9988,

P_2 = 00112233445566778899aabbcceeff0a,

P_3 = 112233445566778899aabbcceeff0a00,

P_4 = 2233445566778899aabbcceeff0a0011».

Подраздел А.2 дополнить пунктами А.2.8, А.2.9:

«**А.2.8 Режим гаммирования с преобразованием ключа**

А.2.8.1 Зашифрование

Пример использует следующие параметры:

Ключ

K = 8899aabbccddeeff0011223344556677fedcba98765432100123456789abcdef.

Открытый текст — семь 128-битных блоков:

P_1 = 1122334455667700ffeeddccbbaa9988,

P_2 = 00112233445566778899aabbcceeff0a,

P_3 = 11223344556677889aabbcceeff0a00,

P_4 = 2233445566778899aabbcceeff0a0011,

P_5 = 33445566778899aabbcceeff0a001122,

P_6 = 445566778899aabbcceeff0a00112233,

P_7 = 5566778899aabbcceeff0a0011223344.

n = 128, s = n = 128,

N = 256,

IV = 1234567890abcef0.

Таблица А.6а — Выработка секционных ключей с помощью функции преобразования ключа ACPKM

Номер секции i	Секционный ключ K^i
1	8899aabbccddeeff0011223344556677fedcba98765432100123456789abcdef
2	2666ed40ae687811745ca0b448f57a7b390adb5780307e8e9659ac403ae60c60
3	bb3dd5402e999b7a3debb0db45448ec530f07365dfee3aba8415f77ac8f34ce8
4	23362fd553cad2178299a5b5a2d4722e3bb83c730a8bf57ce2dd004017f8c565

Таблица А.6б — Зашифрование секции M^1 в режиме гаммирования с преобразованием ключа

i	1	2
P_i	1122334455667700ffeeddccbbaa9988	00112233445566778899aabbcceeff0a
Входной блок (CTR_i)	1234567890abcef00000000000000000	1234567890abcef00000000000000001
Выходной блок (e_{K^1} (CTR_i))	e0b7ebfa9468a6db2a95826efb173830	85ffc500b2f4582a7ba54e08f0ab21ee
C_i	f195d8bec10ed1dbd57b5fa240bda1b8	85eee733f6a13e5df33ce4b33c45dee4

Таблица А.6в — Зашифрование секции M^2 в режиме гаммирования с преобразованием ключа

i	3	4
P_i	11223344556677889aabbcceeff0a00	2233445566778899aabbcceeff0a0011
Входной блок (CTR_i)	1234567890abcef00000000000000002	1234567890abcef00000000000000003
Выходной блок (e_{K^2} (CTR_i))	5aecd8cb31093bdd99bdbdebb07ae200	7a4f09a00ea71ca094f3f8412f8a5057
C_i	4bceeb8f646f4c55001706275e85e800	587c4df568d094393e4834afd0805046

Таблица А.6г — Зашифрование секции M^3 в режиме гаммирования с преобразованием ключа

i	5	6
P_i	33445566778899aabbcceeff0a001122	445566778899aabbcceeff0a00112233
Входной блок (CTR_i)	1234567890abcef00000000000000004	1234567890abcef00000000000000005
Выходной блок (e_{K^3} (CTR_i))	fc74a010f126754ba73082ce618a984c	9ba8619b09af9cfdc0a1c47e3432340d
C_i	cf30f57686aeece11cfc6c316b8a896e	dffd07ec813636460c4f3b743423163e

Таблица А.6д — Зашифрование секции M^4 в режиме гаммирования с преобразованием ключа

i	7
P_i	5566778899aabbcceeff0a0011223344
Входной блок (CTR_i)	1234567890abcef00000000000000006
Выходной блок (e_{K^4} (CTR_i))	316fde4a1b507318872d2be7eaf4ed19
C_i	6409a9c282fac8d469d221e7fbd6de5d

А.2.8.2 Расшифрование

С использованием приведенных значений K, IV и C с помощью операции расшифрования воспроизводятся значения P_1, P_2, P_3, P_4, P_5, P_6, P_7.

А.2.9 Режим аутентифицированного шифрования с ассоциированными данными

А.2.9.1 Зашифрование с выработкой имитовставки

Пример использует следующие параметры:

Ключ

K = 8899aabbccddeeff0011223344556677fedcba98765432100123456789abcdef.

Открытый текст — четыре 128-битных блока и один 24-битный блок:

P_1 = 1122334455667700ffeeddccbbaa9988,

P_2 = 00112233445566778899aabbcceeff0a,

P_3 = 11223344556677889aabbcceeff0a00,

P_4 = 2233445566778899aabbcceeff0a0011,

P_5^* = aabbcc.

Ассоциированные данные — два 128-битных блока и один 72-битный блок:

A_1 = 02020202020202020101010101010101,

A_2 = 04040404040404040303030303030303,

A_3^* = ea0505050505050505.

n = 128, s = n = 128,

IV = 1122334455667700ffeeddccbbaa9988,

$Y_1 = e_K(0 \| IV)$ = 7f679d90bebc24305a468d42b9d4edcd,

$Z_1 = e_K(1 \| IV)$ = 7fc245a8586e6602a7bbdb2786bdc66f.

Таблица А.6е — Зашифрование в режиме аутентифицированного шифрования с ассоциированными данными

i	1	2
P_i	1122334455667700ffeeddccbbaa9988	00112233445566778899aabbcceeff0a
Входной блок (Y_i)	7f679d90bebc24305a468d42b9d4edcd	7f679d90bebc24305a468d42b9d4edce
Выходной блок ($e_K(Y_i)$)	b85748c512f31990aa567ef15335db74	8064f0126fac9b2c5b6eac21612f9433
C_i	a9757b8147956e9055b8a33de89f42fc	8075d2212bf9fd5bd3f7069aadc16b39

Продолжение таблицы А.6е

i	3	4
P_i	11223344556677889aabbcceeff0a00	2233445566778899aabbcceeff0a0011
Входной блок (Y_i)	7f679d90bebc24305a468d42b9d4edcf	7f679d90bebc24305a468d42b9d4edd0
Выходной блок ($e_K(Y_i)$)	5858821d40c0cd0d0ac1e6c247098f1c	e43f5081b58f0b49012f8ee86acd6dfa
C_i	497ab15915a6ba85936b5d0ea9f6851c	c60c14d4d3f883d0ab94420695c76deb

Окончание таблицы А.6е

i	5
P_i	aabbcc
Входной блок (Y_i)	7f679d90bebc24305a468d42b9d4edd1
Выходной блок ($e_K(Y_i)$)	86ce9e2a0a1225e3335691b20d5a3348
C_i^*	2c7552

Дополнение последнего блока шифртекста и последнего блока ассоциированных данных:
C_5 = 2c7552000000000000000000000000,
A_3 = ea05050505050505050000000000000.

Таблица А.6ж — Вычисление имитовставки в режиме аутентифицированного шифрования с ассоциированными данными

i	1	2
Входной блок (Z_i)	7fc245a8586e6602a7bbdb2786bdc66f	7fc245a8586e6603a7bbdb2786bdc66f
Выходной блок (H_i)	8db187d653830ea4bc446476952c300b	7a24f72630e3763721c8f3cdb1da0e31

Продолжение таблицы А.6ж

i	3	4
Входной блок (Z_i)	7fc245a8586e6604a7bbdb2786bdc66f	7fc245a8586e6605a7bbdb2786bdc66f
Выходной блок (H_i)	4411962117d20635c525e0a24db4b90a	d8c9623c4dbfe814ce7c1c0ceaa959db

Продолжение таблицы А.6ж

i	5	6
Входной блок (Z_i)	7fc245a8586e6606a7bbdb2786bdc66f	7fc245a8586e6607a7bbdb2786bdc66f
Выходной блок (H_i)	a5e1f195333e1482969931bfbe6dfd43	b4ca808caccfb3f91724e48a2c7ee9d2

Продолжение таблицы А.6ж

i	7	8
Входной блок (Z_i)	7fc245a8586e6608a7bbdb2786bdc66f	7fc245a8586e6609a7bbdb2786bdc66f
Выходной блок (H_i)	72908fc074e469e8901bd188ea91c331	23ca2715b02c68313bfdacb39e4d0fb8

Окончание таблицы А.6ж

i	9
Входной блок (Z_i)	7fc245a8586e660aa7bbdb2786bdc66f
Выходной блок (H_i)	bcbce6c41aa355a4148862bf64bd830d

$\text{len}(A) \| \text{len}(C)$ = 00000000000001480000000000000218.
MAC = cf5d656f40c34f5c46e8bb0e29fcdb4c.

А.2.9.2 Расшифрование

С использованием приведенных значений K, IV, A, C и MAC с помощью операции расшифрования с проверкой имитовставки выполняется проверка имитовставки MAC и воспроизводятся значения P_1, P_2, P_3, P_4, P_5^*».

Пункт А.3.1 исключить.

Пункты А.3.2, А.3.3.1, А.3.4.1, А.3.5.1, А.3.6.1, А.3.7 (после наименования) дополнить абзацем:
«Пример использует следующие параметры:
Ключ
K = ffeeddccbbaa99887766554433221100f0f1f2f3f4f5f6f7f8f9fafbfcfdfeff.
Открытый текст — четыре 64-битных блока:
P_1 = 92def06b3c130a59,
P_2 = db54c704f8189d20,
P_3 = 4a98fb2e67a8024c,
P_4 = 8912409b17b57e41».
Подраздел А.3 дополнить пунктами А.3.8, А.3.9:
«**А.3.8 Режим гаммирования с преобразованием ключа**
А.3.8.1 Зашифрование
Пример использует следующие параметры:
Ключ
K = 8899aabbccddeeff0011223344556677fedcba98765432100123456789abcdef.
Открытый текст — семь 64-битных блоков:
P_1 = 1122334455667700,
P_2 = feeddccbbaa9988,
P_3 = 0011223344556677,
P_4 = 8899aabbcceeff0a,
P_5 = 1122334455667788,
P_6 = 99aabbcceeff0a00,
P_7 = 2233445566778899.
n = 64, s = n = 64,
N = 128,
IV = 12345678.

Таблица А.13 — Выработка секционных ключей с помощью функции преобразования ключа ACPKM

Номер секции i	Секционный ключ K^i
1	8899aabbccddeeff0011223344556677fedcba98765432100123456789abcdef
2	863ea017842c3d372b18a85a28e2317d74befc107720de0c9e8ab974abd00ca0
3	49a5e2677de555982b8ad5e826652d17eec847bf5b3997a81cf7fe7f1187bd27
4	3256bf3f97b5667426a9fb1c5eaabe41893ccdd5a868f9b63b0aa90720fa43c4

Таблица А.14 — Зашифрование секции M^1 в режиме гаммирования с преобразованием ключа

i	1	2
P_i	1122334455667700	ffeeddccbbaa9988
Входной блок (CTR_i)	1234567800000000	1234567800000001
Выходной блок (e_{K^1} (CTR_i))	3b9a2eaabe783bab	970fd90806c10d62
C_i	2ab81deeeb1e4cab	68e104c4bd6b94ea

Таблица А.15 — Зашифрование секции M^2 в режиме гаммирования с преобразованием ключа

i	3	4
P_i	0011223344556677	8899aabbcceeff0a
Входной блок (CTR_i)	1234567800000002	1234567800000003
Выходной блок (e_{K^2} (CTR_i))	c73d459c287b3d1c	86361cacbc1f4c24
C_i	c72c67af6c2e5b6b	0eafb61770f1b32e

Таблица А.16 — Зашифрование секции M^3 в режиме гаммирования с преобразованием ключа

i	5	6
P_i	1122334455667788	99aabbcceeff0a00
Входной блок (CTR_i)	1234567800000004	1234567800000005
Выходной блок ($e_{K^3}(CTR_i)$)	b08c4250cb8b640a	327edcd4e88de66f
C_i	a1ae71149eed1382	abd467180672ec6f

Таблица А.17 — Зашифрование секции M^4 в режиме гаммирования с преобразованием ключа

i	7
P_i	2233445566778899
Входной блок (CTR_i)	1234567800000006
Выходной блок ($e_{K^4}(CTR_i)$)	a691b50e59bdfa58
C_i	84a2f15b3fca72c1

А.3.8.2 Расшифрование

С использованием приведенных значений K, IV и C с помощью операции расшифрования воспроизводятся значения P_1, P_2, P_3, P_4, P_5, P_6, P_7.

А.3.9 Режим аутентифицированного шифрования с ассоциированными данными

А.3.9.1 Зашифрование с выработкой имитовставки

Пример использует следующие параметры:

Ключ

K = ffeeddccbbaa99887766554433221100f0f1f2f3f4f5f6f7f8f9fafbfcfdfeff.

Открытый текст — восемь 64-битных блоков и один 24-битный блок:

P_1 = ffeeddccbbaa9988,

P_2 = 1122334455667700,

P_3 = 8899aabbcceeff0a,

P_4 = 0011223344556677,

P_5 = 99aabbcceeff0a00,

P_6 = 1122334455667788,

P_7 = aabbcceeff0a0011,

P_8 = 2233445566778899,

P_9 = aabbcc.

Ассоциированные данные — пять 64-битных блоков и один 8-битный блок:

A_1 = 0101010101010101,

A_2 = 0202020202020202,

A_3 = 0303030303030303,

A_4 = 0404040404040404,

A_5 = 0505050505050505,

A_6 = ea.

n = 64, $s = n$ = 64,

IV = 12def06b3c130a59,

$Y_1 = e_K(0 \| IV)$ = 5623890162de31bf,

$Z_1 = e_K(1 \| IV)$ = 2b073f0494f372a0.

Таблица А.18 — Зашифрование в режиме аутентифицированного шифрования с ассоциированными данными

i	1	2
P_i	ffeeddccbbaa9988	1122334455667700
Входной блок (Y_i)	5623890162de31bf	5623890162de31C0
Выходной блок ($e_K(Y_i)$)	387bdba0e43439b3	9433000610f7f2ae
C_i	c795066c5f9ea03b	85113342459185ae

Продолжение таблицы А.18

i	3	4
P_i	8899aabbcceeff0a	0011223344556677
Входной блок (Y_i)	5623890162de31c1	5623890162de31c2
Выходной блок ($e_K(Y_i)$)	97b7aa6d73c58757	9415528bffc9e80a
C_i	1f2e00d6bf2b785d	940470b8bb9c8e7d

Продолжение таблицы А.18

i	5	6
P_i	99aabbcceeff0a00	1122334455667788
Входной блок (Y_i)	5623890162de31c3	5623890162de31c4
Выходной блок ($e_K(Y_i)$)	03f768bff182d670	fd05f84e9b09d2fe
C_i	9a5dd3731f7ddc70	ec27cb0ace6fa576

Продолжение таблицы А.18

i	7	8
P_i	aabbcceeff0a0011	2233445566778899
Входной блок (Y_i)	5623890162de31c5	5623890162de31c6
Выходной блок ($e_K(Y_i)$)	da4d908a95b175c4	65997396dac24bd7
C_i	70f65c646abb75d5	47aa37c3bcb5c34e

Окончание таблицы А.18

i	9
P_i	aabbcc
Входной блок (Y_i)	5623890162de31c7
Выходной блок ($e_K(Y_i)$)	a900504a148dee26
C_i^*	03bb9c

Дополнение последнего блока шифртекста и последнего блока ассоциированных данных:

C_5 = 03bb9c0000000000,

A_3 = ea00000000000000.

Таблица А.19 — Вычисление имитовставки в режиме аутентифицированного шифрования с ассоциированными данными

i	1	2
Входной блок (Z_i)	2b073f0494f372a0	2b073f0594f372a0
Выходной блок (H_i)	708a78191cdd22aa	6f02cc464b2fa0a3

Продолжение таблицы А.19

i	3	4
Входной блок (Z_i)	2b073f0694f372a0	2b073f0794f372a0
Выходной блок (H_i)	9f81f226fd196f05	b9c2ac9be5b5dff9

Продолжение таблицы А.19

i	5	6
Входной блок (Z_i)	2b073f0894f372a0	2b073f0994f372a0
Выходной блок (H_i)	74b5ec96551bf888	7eb021a4035b04c3

Продолжение таблицы А.19

i	7	8
Входной блок (Z_i)	2b073f0a94f372a0	2b073f0b94f372a0
Выходной блок (H_i)	c2a9c3a8704d9bb0	f5d505a87b8383b5

Продолжение таблицы А.19

i	9	10
Входной блок (Z_i)	2b073f0c94f372a0	2b073f0d94f372a0
Выходной блок (H_i)	f795e75fdeb8933c	65a1a3e680f08145

Продолжение таблицы А.19

i	11	12
Входной блок (Z_i)	2b073f0e94f372a0	2b073f0f94f372a0
Выходной блок (H_i)	1c74a5764cb0d595	dc8447a514e783e7

Продолжение таблицы А.19

i	13	14
Входной блок (Z_i)	2b073f1094f372a0	2b073f1194f372a0
Выходной блок (H_i)	a7e3afe004ee16e3	a5aabb0b7980d071

Окончание таблицы А.19

i	15	16
Входной блок (Z_i)	2b073f1294f372a0	2b073f1394f372a0
Выходной блок (H_i)	6e104cc933525c5d	8311b6024aa966c1

len(A) ‖ len(C) = 0000014800000218.

MAC = a7928069aa10fd10.

А.3.9.2 Расшифрование

С использованием приведенных значений K, IV, A, C и MAC с помощью операции расшифрования с проверкой имитовставки выполняется проверка имитовставки MAC и воспроизводятся значения P_1, P_2, P_3, P_4, P_5^*».

Заменить код МКС: «35.040» на «35.030».

(ИУС № 2 2024 г.)