ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ

Р 1323565.1.022— 2018

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Функции выработки производного ключа

Издание официальное

Москва
Стандартинформ
2018

gost.e-ecolog.ru

Предисловие

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

2 ВНЕСЕНЫ Техническим комитетом по стандартизации ТК 026 «Криптографическая защита информации»

3 УТВЕРЖДЕНЫ И ВВЕДЕНЫ В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 14 декабря 2018 г. № 1103-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, 2018

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 Термины, определения и обозначения 2
3.1 Термины и определения 2
3.2 Обозначения 2
4 Общие положения 3
5 Описание функций 3
5.1 Вспомогательные преобразования 3
5.2 Выработка промежуточного ключа 3
5.3 Выработка производного ключевого материала 4
6 Форматирование данных 4
Приложение А (справочное) Пример процедуры форматирования данных 5
Библиография 6

Введение

Задача выработки производных ключей для различных криптографических механизмов на основании некоторой исходной ключевой информации, полученной, например, в результате выполнения протоколов выработки общего ключа, часто возникает в средствах криптографической защиты информации. В настоящее время в национальной системе стандартов и рекомендаций по стандартизации есть отдельные преобразования (см. [1]), реализующие функции выработки производных ключей.

Необходимость разработки настоящих рекомендаций вызвана потребностью в создании общей конструкции выработки производных ключей на основании национальных стандартов, использующей различные криптографические преобразования и обладающей большой гибкостью в эксплуатации.

Настоящие рекомендации определяют функции выработки производных криптографических ключей и используют в качестве базового преобразования криптографические алгоритмы хэширования, определенные в ГОСТ Р 34.11—2012, и алгоритмы шифрования, определенные ГОСТ Р 34.12—2015, в режиме выработки имитовставки согласно ГОСТ Р 34.13—2015.

РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Функции выработки производного ключа

Information technology. Cryptographic data security.
Key derivation functions

Дата введения — 2019—05—01

1 Область применения

При реализации средствами криптографической защиты информации (СКЗИ) нескольких криптографических функций возникает необходимость использования для механизмов, реализующих каждую из функций, различных ключей, выработанных из исходной ключевой информации. Исходной ключевой информацией может являться, например, заранее распределенный ключ или ключ, полученный в результате выполнения протоколов выработки общего ключа.

Функции выработки производных ключей осуществляют криптографическое преобразование исходной ключевой информации с использованием дополнительных открытых данных с целью получения ключей для дальнейшего использования в различных функциях. Функции, описываемые настоящим документом, дополняют существующую систему национальных стандартов и методических рекомендаций в области криптографической защиты информации в части реализации криптографических функций по выработке производных ключей.

2 Нормативные ссылки

В настоящих рекомендациях использованы нормативные ссылки на следующие стандарты:

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

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

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

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.

Издание официальное

3 Термины, определения и обозначения

3.1 Термины и определения

В настоящих рекомендациях применены следующие термины с соответствующими определениями:

3.1.1 **производный ключ:** Криптографический ключ, получаемый из производной ключевой информации путем отбрасывания части символов.

3.1.2 **производная ключевая информация:** Последовательность символов, вырабатываемая из исходной ключевой информации и общеизвестных данных в результате работы функций выработки производных ключей.

3.1.3 **исходная ключевая информация:** Совокупность данных, предназначенных для выработки по определенным правилам криптографических ключей.

3.1.4 **криптографический ключ:** Изменяемый параметр в виде последовательности символов, определяющий криптографическое преобразование.

3.1.5 **промежуточный ключ:** Криптографический ключ, вырабатываемый из исходной ключевой информации и используемый для дальнейшей выработки производных ключей.

3.2 Обозначения

В настоящих рекомендациях использованы следующие обозначения:

V_n — множество всех n-мерных двоичных (битовых) строк, т. е. строк с компонентами из поля $GF(2)$, где n — целое неотрицательное число. Нумерация подстрок и компонент строк осуществляется справа налево, начиная с нуля. При этом V_0 — множество, единственным элементом которого является пустая строка;

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

$|A|$ — число компонент (длина) строки $A \in V^*$;

APB — конкатенация строк A, $B \in V^*$, т.е. строка из $V_{|A|+|B|}$, в которой левая подстрока из $V_{|A|}$ совпадает со строкой A, а правая подстрока из $V_{|B|}$ совпадает со строкой B;

A^n — конкатенация n экземпляров строки A;

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

LB_n — операция взятия левой подстроки длины n: $\mathrm{LB}_n : V^* \setminus \bigcup_{i=0}^{n-1} V_i \to V_n$, для $M \in V^* \setminus \bigcup_{i=0}^{n-1} V_i$, $M = APB$, где $|A| = n$, $|B| = |M| - n$, полагают $\mathrm{LB}_n(M) = A$;

RB_n — операция взятия правой подстроки длины n: $\mathrm{RB}_n : V^* \setminus \bigcup_{i=0}^{n-1} V_i \to V_n$, для $M \in V^* \setminus \bigcup_{i=0}^{n-1} V_i$, $M = APB$, где $|A| = |M| - n$, $|B| = n$, полагают $\mathrm{RB}_n(M) = B$;

$\mathrm{Hash}^{(n)}$ — функция хэширования с хэш-кодом длиной n бит ($n \in \{256,512\}$), определяемая ГОСТ Р 34.11—2012 , $\mathrm{Hash}^{(n)}$: $V^* \to V_n$;

$\mathrm{MAC}^{(n)}$ — ключевая функция хэширования, вырабатывающая имитовставку длины n с использованием ключа $K \in V_k$, $\mathrm{MAC}^{(n)}$: $V_k \times V^* \to V_n$; также будем использовать обозначение $\mathrm{MAC}_K^{(n)}(\cdot) = \mathrm{MAC}^{(n)}(K,\cdot)$;

$\mathrm{CMAC}^{(n)}$ — ключевая функция хэширования, вычисляющая имитовставку длины n, определяемая по ГОСТ Р 34.13—2015, подраздел 5.6;

format — функция форматирования входных данных format: $(V^*)^6 \to V^*$;

$S \in V^*$ — исходная ключевая информация;

$C \in V^*$ — представление числа, используемого в итеративных конструкциях в качестве счетчика. Способ представления счетчика должен быть согласован между участниками информационного обмена;

$P \in V^*$ — метка использования — двоичная строка, содержащая информацию об использовании вырабатываемых производных ключей. Может содержать, например, информацию о конкретном механизме, для которого предназначается производный ключ (ключ шифрования ключей, ключ шифрования данных, ключ имитозащиты и т. п.) или, в случае одновременной выработки ключей для нескольких примитивов, информацию о разделении производного ключевого материала на различные производные ключи; допустимые значения и способ представления должны быть согласованы между участниками информационного обмена;

$U \in V^*$ — информация об участниках информационного обмена, которыми предполагается использование вырабатываемой ключевой информации; может включать в себя идентификаторы пользователей и прочую информацию, известную всем участникам, вырабатывающим производную ключевую информацию;

$A \in V^*$ — некоторая дополнительная информация, используемая при выработке производной ключевой информации, например, метка времени;

$L \in V^*$ — длина (в двоичной записи) вырабатываемого производного ключевого материала в битах;

$T \in V^*$ — соль — случайная строка фиксированной длины, обычно вырабатываемая в момент выполнения алгоритма.

4 Общие положения

Описываемые настоящим документом функции выработки производных ключей принимают на вход шесть аргументов: исходную ключевую информацию S, длину производной ключевой информации L, соль T, метку использования P, информацию о субъектах U, дополнительную информацию A. Функции состоят из двух этапов. На первом этапе из исходной ключевой информации и соли вырабатывается промежуточный ключ длины 256 бит. Полученный промежуточный ключ вместе с остальными входными параметрами используется на втором этапе функций, выходом которых является производный ключевой материал K_o длины L.

5 Описание функций

Общая схема функций выработки производных ключей $\mathrm{kdf}(S,L,T,P,U,A)$ определяется следующей последовательностью действий:

- вычисляют $K^{(1)} = \mathrm{kdf}^{(1)}(T,S)$;
- вычисляют $K^{(2)} = \mathrm{kdf}^{(2)}(K^{(1)},L,P,U,A)$;
- полагают, что $K_o = \mathrm{kdf}(S,T,L,P,U,A) = K^{(2)}$.

Здесь $\mathrm{kdf}^{(i)}$, $i \in \{1,2\}$ — преобразования, выполняемые на первом и втором этапах, $K^{(1)} \in V_{256}$ — промежуточный ключ.

5.1 Вспомогательные преобразования

В предлагаемых функциях выработки производных ключей используют ключевые функции хэширования HMAC и NMAC [2], в качестве бесключевых функций хэширования в которых используют функции, определяемые ГОСТ Р 34.11—2012. Конструкцию HMAC определяют, следуя [1] и [2], при этом можно использовать функции хэширования с хэш-кодами длины 256 и 512 бит:

$$\mathrm{HMAC}_K^{(n)}(X) = \mathrm{Hash}^{(n)}\left[(K \oplus C_{OUT}) \,\|\, \mathrm{Hash}^{(n)}\left((K \oplus C_{IN}) \| X\right)\right]. \quad (1)$$

Конструкцию NMAC определяют, следуя [2], причем в качестве внутренней функции используют $\mathrm{Hash}^{(512)}$, а в качестве внешней функции — $\mathrm{Hash}^{(256)}$:

$$\mathrm{NMAC}_K^{(256)}(X) = \mathrm{Hash}^{(256)}\left[(K \oplus C_{OUT}) \,\|\, \mathrm{Hash}^{(512)}\left((K \oplus C_{IN}) \| X\right)\right]. \quad (2)$$

Здесь аргументы X, $K \in V^*$, а C_{IN} и C_{OUT} — константы, одинаковые для обеих конструкций, определяемые в [2] как:

$$C_{IN} = (00110110)^{64},$$

$$C_{OUT} = (01011100)^{64}.$$

5.2 Выработка промежуточного ключа

В качестве функции выработки промежуточного ключа $\mathrm{kdf}^{(1)}$ допускается использовать одну из трех конструкций.

Первая конструкция основана на функции NMAC (2):

$$K^{(1)} = \mathrm{NMAC}_T^{(256)}(S), \quad |T| \le 512.$$

Вторая конструкция основана на алгоритме выработки имитовставки HMAC (1) с использованием хэш-функции с хэш-кодом длиной 512 бит и завершающим усечением:

$$K^{(1)} = \mathrm{LB}_{256}(\mathrm{HMAC}_T^{(512)}(S)), \quad |T| \le 512.$$

Третья конструкция является упрощенной и может использоваться только в случае, когда исходная ключевая информация является ключом длины 256 бит, $S \in V_{256}$:

$$K^{(1)} = S \oplus T, \ |T| = 256.$$

Примечание — При использовании данной конструкции предполагают, что исходная ключевая информация имеет требуемую длину (256 бит), а также удовлетворяет требованиям к криптографическим ключам, определяемым разработчиком СКЗИ.

5.3 Выработка производного ключевого материала

Преобразование второго этапа предлагаемых функций $\text{kdf}^{(2)}$ заключаются в выработке выходной последовательности с использованием ключевой функции хэширования с хэш-кодом длиной n. В качестве ключа функции хэширования используют выработанный на первом этапе промежуточный ключ $K^{(1)}$. В качестве информационного входа (сообщения) используют все остальные аргументы $\text{kdf}^{(2)}$, представленные некоторым образом в виде двоичной строки с использованием процедуры форматирования format.

В общем виде преобразование второго этапа описывают следующим образом:

$$\begin{aligned} &C_0 = 0; \\ &z_0 = IV; \\ &\left.\begin{aligned} &C_i = C_{i-1} + 1, \\ &z_i = \text{MAC}^{(n)}_{K^{(1)}}(\text{format}(z_{i-1}, C_i, P, U, A, L)), \end{aligned}\right\} \quad i = \overline{1, \lceil L/n \rceil}; \\ &K_o = \text{LB}_L\left(z_1 \text{P} z_2 \text{P} \ldots \text{P} z_{\lceil L/n \rceil}\right). \end{aligned}$$

В качестве ключевой функции хэширования MAC можно использовать: ключевую функцию хэширования $\text{CMAC}^{(n)}_K$, ключевую функцию хэширования $\text{HMAC}^{(n)}_K$, ключевую функцию хэширования $\text{NMAC}^{(256)}_K$.

Все участники информационного обмена должны согласовать использование одинаковых алгоритмов в качестве MAC. Также участниками информационного обмена должно быть согласовано значение IV. При этом его можно вычислять при каждом запуске алгоритма, оно может быть долговременным параметром или быть постоянным.

6 Форматирование данных

Процедура форматирования данных format заключается в формировании строки V^*, подаваемой на вход алгоритма MAC, из набора входных аргументов функций. Как и в случае выбора алгоритма MAC, все участники информационного обмена должны согласовать процедуру форматирования данных.

К процедуре форматирования данных предъявляют следующие требования:

- процедура форматирования данных может существенно не зависеть от части своих параметров, но должна существенно зависеть от всех бит z_{i-1} или от всех бит счетчика C_i;
- процедура форматирования должна быть инъективной (т. е. не допускать коллизий) при всевозможных значениях существенных параметров;
- процедура форматирования данных должна задавать длины полей, соответствующих представлениям различных аргументов;
- процедура форматирования должна быть эффективно реализуемой.

Приложение А
(справочное)

Пример процедуры форматирования данных

В настоящем приложении дано описание семейства из 48 различных процедур форматирования данных, отличающихся друг от друга набором переменных, являющихся существенными. Пусть $f \in V_8$, $f = (f_7, ..., f_0)$ — массив «флагов», сигнализирующих о существенной зависимости выхода процедуры форматирования от всех бит одного из входов. Каждой переменной соответствует один флаг f_i (см. таблицу А.1). Если процедура форматирования существенно зависит от всех бит некоторого входа, то значение флага равно 1, а в противном случае — равно 0. Флаги f_0, f_1 не используют, хотя бы один из флагов f_7 и f_6 должен быть равен 1.

Т а б л и ц а А.1 — Соответствие флагов и переменных

Флаг	f_7	f_6	f_5	f_4	f_3	f_2	f_1	f_0
Переменная	C_i	z_{i-1}	L	P	U	A	0	0

Процедура форматирования выглядит следующим образом:

$$\text{format}(z_{i-1}, C_i, P, U, A, L) = \underbrace{f}_{8} \| \underbrace{C_i}_{256} \| \underbrace{z_{i-1}}_{512} \| \underbrace{L}_{248} \| \underbrace{P}_{256} \| \underbrace{U}_{128} \| \underbrace{A}_{128},$$

где под каждой переменной указана длина поля в битах, используемого для записи значения этой переменной. Длина записи каждой из входных переменных не должна превосходить длину поля, отведенного под эту переменную в выходной строке процедуры форматирования. С учетом размера поля для L длина вырабатываемого ключевого материала при использовании описанной процедуры форматирования не может превышать $2^{248} - 1$ бит. В случае если какую-либо из переменных по существу не используют, то соответствующее поле заполняют нулями.

Длины полей для L, P, U, A могут быть увеличены или уменьшены исходя из эксплуатационных условий и требований для каждого конкретного СКЗИ.

Библиография

[1] Р 50.1.113—2016 Информационная технология. Криптографическая защита информации. Криптографические алгоритмы, сопутствующие применению алгоритмов электронной цифровой подписи и функции хэширования

[2] Bellare, M. New Proofs for NMAC and HMAC: Security without collision resistance/ M. Bellare // Advances in Cryptology — CRYPTO 2006, 26th Annual International Cryptology Conference, Santa Barbara, California, USA, August 20—24, 2006, Proceedings / ed. by C. Dwork. V. 4117 of Lecture Notes in Computer Science. Springer, 2006. P. 602—619

УДК 681.3.06:006.354 ОКС 35.040

Ключевые слова: информационная технология, криптографическая защита информации, ключ, производный ключ, функции выработки

БЗ 12—2018/51

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

Сдано в набор 17.12.2018. Подписано в печать 09.01.2019. Формат 60×84 1/8. Гарнитура Ариал.
Усл. печ. л. 1,40. Уч.-изд. л. 1,20.
Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Создано в единичном исполнении 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