ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ

Р 1323565.1.003— 2017

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Криптографические алгоритмы выработки ключей шифрования информации и аутентификационных векторов, предназначенные для реализации в аппаратных модулях доверия для использования в подвижной радиотелефонной связи

Издание официальное

Москва
Стандартинформ
2017

Предисловие

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

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 24 октября 2017 г. № 1504-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 (www.gost.ru)

Содержание

Поправка к Р 1323565.1.003-2017 Информационная технология. Криптографическая защита информации. Криптографические алгоритмы выработки ключей шифрования информации и аутентификационных векторов, предназначенные для реализации в аппаратных модулях доверия для использования в подвижной радиотелефонной связи

В каком месте	Напечатано	Должно быть
Пункт 5.1	$F_{OP} = K\|\|algoname\|\|OP\|\|inf_1 \in V_{287}$	$F_{OP} = K\|\|OP\|\|inf_1\|\|algoname \in V_{287}$
Пункт 5.3	Из шести строк $K \in V_{128}$, $RAND \in V_{128}$, $OP_C \in V_{128}$, $inf_2 \in V_7$, $algoname \in V_{24}$, $add \in V_{32}$ формируется строка	Из шести строк $K \in V_{128}$, $RAND \in V_{128}$, $OP_C \in V_{128}$, $inf_3 \in V_7$, $algoname \in V_{24}$, $add \in V_{32}$ формируется строка
Пункт 5.3	$f_2 = f_2[63]\|\|...\|\|f_2[0] = HF_1[511]\|\|...\|\|HF_1[448] \in V_{64}$, $f_3 = f_3[127]\|\|...\|\|f_3[0] = HF_1[447]\|\|...HF_1[320] \in V_{128}$, $f_4 = f_4[127]\|\|...\|\|f_4[0] = HF_1[319]\|\|...\|\|HF_1[192] \in V_{128}$, $f_5 = f_5[47]\|\|...\|\|f_5[0] = HF_1[191]\|\|...\|\|HF_1[144] \in V_{48}$, $f_5^* = f_5^*[47]\|\|...\|\|f_5^*[0] = HF_1[143]\|\|...\|\|HF_1[96] \in V_{48}$.	$f_2 = f_2[63]\|\|...\|\|f_2[0] = HF_2[511]\|\|...\|\|HF_2[448] \in V_{64}$, $f_3 = f_3[127]\|\|...\|\|f_3[0] = HF_2[447]\|\|...\|\|HF_2[320] \in V_{128}$, $f_4 = f_4[127]\|\|...\|\|f_4[0] = HF_2[319]\|\|...\|\|HF_2[192] \in V_{128}$, $f_5 = f_5[47]\|\|...\|\|f_5[0] = HF_2[191]\|\|...\|\|HF_2[144] \in V_{48}$, $f_5^* = f_5^*[47]\|\|...\|\|f_5^*[0] = HF_2[143]\|\|...\|\|HF_2[96] \in V_{48}$.
Пункт 6.2	Из девяти строк $KV \in V_{256}$, $RAND \in V_{128}$, $SQN \in V_{48}$, $AMF \in V_{128}$, $TOP_C \in V_{128}$, $instance \in V_8$, $add \in V_{32}$, $inf_2 \in V_8$, $algoname \in V_{72}$ формируется строка	Из девяти строк $KV \in V_{256}$, $RAND \in V_{128}$, $SQN \in V_{48}$, $AMF \in V_{128}$, $TOP_C \in V_{256}$, $instance \in V_8$, $add \in V_{32}$, $inf_2 \in V_8$, $algoname \in V_{72}$ формируется строка
Пункт 6.3	Из семи строк $RV \in V_{256}$, $RAND \in V_{128}$, $TOP_C \in V_{128}$, $instance \in V_8$, $add \in V_{32}$, $inf_3 \in V_8$, $algoname \in V_{72}$ формируется строка	Из семи строк $KV \in V_{256}$, $RAND \in V_{128}$, $TOP_C \in V_{256}$, $instance \in V_8$, $add \in V_{32}$, $inf_3 \in V_8$, $algoname \in V_{72}$ формируется строка
Пункт 6.4	Из семи строк $KV \in V_{256}$, $RAND \in V_{128}$, $TOP_C \in V_{128}$, $instance \in V_8$, $add \in V_{32}$, $inf_4 \in V_8$, $algoname \in V_{72}$ формируется строка $F_{3,4} = KV\|\|RAND\|\|TOP_C\|\|instance\|\|add\|\|inf_4\|\|algonsme \in V_{760}$, где $instance[0] = instance[1] = 1$,	Из семи строк $KV \in V_{256}$, $RAND \in V_{128}$, $TOP_C \in V_{256}$, $instance \in V_8$, $add \in V_{32}$, $inf_4 \in V_8$, $algoname \in V_{72}$ формируется строка $F_{3,4} = KV\|\|RAND\|\|TOP_C\|\|instance\|\|add\|\|inf_4\|\|algoname \in V_{760}$, где $instance[0] = 0, instance[1] = 1$,
Пункт А.2.1	Двоичное представление строки $inf_1 = (0\|\|0\|\|0\|\|0\|\|0\|\|0\|\|0)$,	Двоичное представление строки $inf_1 = (0\|\|0\|\|0\|\|0\|\|0\|\|0\|\|0\|\|0)$,
Пункт А.2.2	Двоичное представление строки $inf_2 = (0\|\|0\|\|0\|\|0\|\|0\|\|0\|\|1)$,	Двоичное представление строки $inf_2 = (0\|\|0\|\|0\|\|0\|\|0\|\|0\|\|0\|\|1)$,
Пункт А.2.3	Двоичное представление строки $inf_3 = (0\|\|0\|\|0\|\|0\|\|0\|\|1\|\|0)$,	Двоичное представление строки $inf_3 = (0\|\|0\|\|0\|\|0\|\|0\|\|0\|\|1\|\|0)$,
Пункт А.2.4	Будем считать, что $\|RES\| = 64$ и $\|CK\| = \|IK\| = 128$, тогда строка $instance = 13$. Двоичное представление строки $inf_4 = (0\|\|0\|\|0\|\|0\|\|0\|\|1\|\|1)$,	Будем считать, что $\|RES\| = 64$ и $\|CK\| = \|IK\| = 128$, тогда строка $instance = 12$. Двоичное представление строки $inf_4 = (0\|\|0\|\|0\|\|0\|\|0\|\|0\|\|1\|\|1)$,

Введение

В настоящее время широкое распространение в мире получили средства коммуникации, основанные на технологии подвижной радиотелефонной связи, в том числе технологии мобильной связи третьего поколения [1], где для выработки аутентификационных векторов и ключей шифрования возможно использовать процедуры [2—5]. Данная технология объединяет в себе высокоскоростной мобильный доступ к услугам радиосвязи и сети Интернет. При подключении к сети радиотелефонной связи абонентского терминала, содержащего аппаратный модуль доверия, выполняются процедуры аутентификации данного модуля и выработки ключей шифрования информации, выполняемых с использованием основного ключа, располагающегося на аппаратном модуле доверия и в центре аутентификации.

Настоящие рекомендации определяют описания криптографических алгоритмов выработки ключей шифрования информации и аутентификационных векторов, предназначенных для реализации в аппаратных модулях доверия для использования в подвижной радиотелефонной связи и использующих в качестве базового преобразования криптографический алгоритм хэширования, определенный в ГОСТ Р 34.11 с длиной хэш-кода 512 бит, получившие названия S3G-128 и S3G-256 (S3G — Secure 3G).

Необходимость разработки настоящих рекомендаций вызвана потребностью в формировании единого подхода к использованию национальных стандартизованных решений в области криптографии в алгоритмах выработки ключей шифрования информации и аутентификационных векторов, предназначенных для реализации в аппаратных модулях доверия для использования в подвижной радиотелефонной связи.

Примечание — Основная часть настоящих рекомендаций дополнена приложением А.

РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Криптографические алгоритмы выработки ключей шифрования информации и аутентификационных векторов, предназначенные для реализации в аппаратных модулях доверия для использования в подвижной радиотелефонной связи

Information technology. Information cryptographic protection. Cryptographic algorithms for a generation of information encryption keys and authentication vectors, intended for implementation in mobile networks subscriber identity modules

Дата введения — 2018—04—01

1 Область применения

S3G-128 и S3G-256 представляют собой криптографические алгоритмы выработки ключей шифрования информации и аутентификационных векторов, предназначенные для реализации в аппаратных модулях доверия для использования в подвижной радиотелефонной связи. При этом они могут использоваться как в рамках сети третьего поколения [1] вместо процедур [2—5], так и ввиду универсальности используемых механизмов в сетях как более раннего, так и позднего поколений. В частности данные алгоритмы предназначены для выработки аутентификационных векторов в процессе информационного взаимодействия абонентского терминала и базовой приемно-передающей станцией. В случае корректного завершения процедуры аутентификации между аппаратным модулем доверия и базовой приемно-передающей станцией алгоритмы S3G-128 и S3G-256 используются для выработки центром аутентификации и аппаратным модулем доверия ключей шифрования передаваемой информации, а также контроля ее целостности.

2 Нормативные ссылки

В настоящих рекомендациях использована нормативная ссылка на следующий стандарт:

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

Примечание — При пользовании настоящими рекомендациями целесообразно проверить действие ссылочных стандартов (рекомендаций) 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 (рекомендации), на который дана недатированная ссылка, то рекомендуется использовать действующую версию этого стандарта (рекомендаций) с учетом всех внесенных в данную версию изменений. Если заменен ссылочный стандарт (рекомендации), на который дана датированная ссылка, то рекомендуется использовать версию этого стандарта (рекомендаций) с указанным выше годом утверждения (принятия). Если после утверждения настоящих рекомендаций в ссылочный стандарт (рекомендации), 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 (рекомендации) 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 в соответствии со следующими определениями:

3.1.1 **абонентский терминал:** Приемо-передающее устройство, используемое для доступа к услугам телефонной связи и сети Интернет в сетях подвижной радиотелефонной связи.

3.1.2 **аппаратный модуль доверия:** Идентификационный модуль абонента, применяемый в сетях подвижной радиотелефонной связи и содержащий основной ключ.

3.1.3 **аутентификационный вектор:** Двоичная строка фиксированной длины, используемая для обеспечения целостности передаваемой информации и аутентификации источника данных. Необходим для реализации процедуры аутентификации между аппаратным модулем доверия и центром аутентификации.

3.1.4 **базовая приемно-передающая станция:** Элемент подвижной радиотелефонной связи, выступающий посредником в рамках информационного взаимодействия, организуемого между аппаратным модулем доверия и центром аутентификации.

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

3.1.6 **ключ контроля целостности:** Криптографический ключ, используемый в рамках процедур обеспечения контроля целостности передаваемой информации.

3.1.7 **ключ анономизации:** Криптографический ключ, используемый в рамках процедуры аутентификации и применяемый для анонимизации номера попытки аутентификации.

3.1.8 **ключ шифрования информации:** Криптографический ключ, используемый в рамках процедуры шифрования передаваемой информации.

3.1.9 **оператор связи:** Элемент подвижной радиотелефонной связи, в ведомстве которого находится организация производства аппаратных модулей доверия и обеспечение бесперебойной работы центра аутентификации.

3.1.10 **основной ключ:** Долговременный параметр, располагающийся на аппаратном модуле доверия и используемый в рамках процедур выработки аутентификационных векторов и ключей шифрования информации.

3.1.11 **центр аутентификации:** Элемент подвижной радиотелефонной связи, обеспечивающий аутентификацию аппаратных модулей доверия и выработку ключей шифрования из основного ключа.

3.2 Обозначения

В настоящих рекомендациях использованы следующие обозначения:

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

V_l — множество всех двоичных строк длины l, где l — 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 большими номерами компонент из $V_{|A|}$ совпадает со строкой A, а подстрока с меньшими номерами компонент из $V_{|B|}$ совпадает со строкой $|B|$;

A^l — конкатенация l экземпляров строки A;

$H: V^* \to V_{512}$ — отображение, реализующее функцию хэширования в соответствии с ГОСТ Р 34.11 с длиной хэш-кода 512 бит;

AMF — управляющее поле аутентификации;

K — основной ключ;

SQN — номер попытки аутентификации аппаратного модуля доверия;

OP — двоичная строка, используемая в S3G-128 для персонификации оператора связи;

OP_C — двоичная строка, формируемая с использованием OP и K;

TOP — двоичная строка, используемая в S3G-256 для персонификации оператора связи;

TOP_C — двоичная строка, формируемая с использованием TOP и K;

$RAND$ — случайная двоичная строка;

AK — ключ анонимизации;

CK — ключ шифрования информации;

IK — ключ контроля целостности;

MAC_A — аутентификационный вектор сети, необходим для аутентификации аппаратным модулем доверия центра аутентификации;

MAC_S — аутентификационный вектор ресинхронизации;

RES — аутентификационный отзыв, получаемый базовой станцией от аппаратного модуля доверия;

XRES — предполагаемое значение аутентификационного отзыва, получаемое базовой станцией от центра аутентификации.

4 Общие положения

В процессе функционирования криптографических алгоритмов S3G-128 и S3G-256 вычисляются семь функций $f_1, f_1^*, f_2, f_3, f_4, f_5, f_5^*$. Значения, получаемые в результате вычисления каждой из данных функций, ассоциируются со следующими формируемыми значениями:

$$f_1(A) = MAC_A,$$
$$f_1^*(A) = MAC_S,$$
$$f_2(A) = RES,$$
$$f_3(A) = CK,$$
$$f_4(A) = IK,$$
$$f_5(A) = AK,$$
$$f_5^*(A) = AK,$$

где *A* — некоторая двоичная строка, определяемая реализуемым криптографическим преобразованием.

5 Описание S3G-128

Начальное заполнение имеет вид:

1 $algoname \in V_{24}$ содержит название алгоритма «*AUT*» (без кавычек) в ASCII-кодировке;

2 $inf_1 = 0^7$;

3 $inf_2 = 0^6||1$;

4 $inf_3 = 0^5||1||0$;

5 $add = 0^{32}$ (при необходимости может выбираться оператором связи).

Двоичные строки *K*, *SQN*, *OP*, *AMF* и *RAND* считаются заданными.

5.1 Вычисление значения

Из четырех строк $K \in V_{128}$, $algoname \in V_{24}$, $OP \in V_{128}$, $inf_1 \in V_7$ формируется строка

$$F_{OP} = K||algoname||OP||inf_1 \in V_{287}.$$

Далее вычисляется

$$H(F_{OP}) = HO[511]|| \ldots ||HO[0] \in V_{512},$$

тогда

$$OP_C = OP_C[127]|| \ldots ||OP_C[0] = HO[511]|| \ldots ||HO[384] \in V_{128}.$$

5.2 Вычисление значений f_1, f_1^*

Из восьми строк $K \in V_{128}$, $RAND \in V_{128}$, $SQN \in V_{48}$, $AMF \in V_{16}$, $OP_C \in V_{128}$, $inf_2 \in V_7$, $algoname \in V_{24}$, $add \in V_{32}$ формируется строка

$$F_1 = K||REND||SQN||AMF||OP_C||add||inf_2||algoname \in V_{511}.$$

Далее вычисляется

$$H(F_1) = HF_1[511]|| \ldots ||HF_1[0] \in V_{512},$$

тогда

$$f_1 = f_1[63]|| \ldots ||f_1[0] = HF_1[511]|| \ldots ||HF_1[448] \in V_{64},$$

$$f_1^* = f_1^*[63]|| \ldots ||f_1^*[0] = HF_1[447]|| \ldots HF_1[384] \in V_{64}.$$

5.3 Вычисление значений $f_2, f_3, f_4, f_5, f_5^*$

Из шести строк $K \in V_{128}$, $RAND \in V_{128}$, $OP_C \in V_{128}$, $inf_2 \in V_7$, $algoname \in V_{24}$, $add \in V_{32}$ формируется строка

$$f_2 = K||RAND||OP_C||add||inf_3||algoname \in V_{447}.$$

Далее вычисляется

$$H(F_2) = HF_2[511]|| \dots ||HF_2[0] \in V_{512},$$

тогда

$$f_2 = f_2[63]|| \dots ||f_2[0] = HF_1[511]|| \dots ||HF_1[448] \in V_{64},$$
$$f_3 = f_3[127]|| \dots ||f_3[0] = HF_1[447]|| \dots HF_1[320] \in V_{128},$$
$$f_4 = f_4[127]|| \dots ||f_4[0] = HF_1[319]|| \dots ||HF_1[192] \in V_{128},$$
$$f_5 = f_5[47]|| \dots ||f_5[0] = HF_1[191]|| \dots ||HF_1[144] \in V_{48},$$
$$f_5^* = f_5^*[47]|| \dots ||f_5^*[0] = HF_1[143]|| \dots ||HF_1[96] \in V_{48}.$$

6 Описание S3G-256

Начальное заполнение имеет вид:

1 $algoname \in V_{72}$ содержит строку «*GOSTR*3411» (без кавычек) в ASCII-кодировке;
2 $inf_1 = 0^8$;
3 $inf_2 = 0^7||1$;
4 $inf_3 = 0^6||1||0$;
5 $inf_4 = 0^6||1^2$;
6 $add = 0^{32}$ (при необходимости может выбираться оператором связи);

7 $$KV = \begin{cases} K, \text{если } |K| = 256, \\ K||0^{128}, \text{если } |K| = 128. \end{cases}$$

Двоичные строки *K*, *SQN*, *TOP*, *AMF* и *RAND* считаются заданными.

6.1 Вычисление значения TOP_C

Из пяти строк $KV \in V_{256}$, $instance \in V_8$, $algoname \in V_{72}$, $TOP \in V_{256}$, $inf_1 \in V_8$ формируется строка

$$T = KV||TOP||instance||inf_1||algoname \in V_{600},$$

где $$instance = \begin{cases} 0^8, \text{если } |K| = 128, \\ 1||0^7, \text{если } |K| = 256. \end{cases}$$

Далее вычисляется

$$H(T) = HT[511]|| \dots ||HT[0] \in V_{512},$$

тогда

$$TOP_C = TOP_C[255]|| \dots ||TOP_C[0] = HT[511]|| \dots ||HT[256] \in V_{256}.$$

6.2 Вычисление значений f_1, f_1^*

Из девяти строк $KV \in V_{256}$, $RAND \in V_{128}$, $SQN \in V_{48}$, $AMF \in V_{128}$, $TOP_C \in V_{128}$, $instance \in V_8$, $add \in V_{32}$, $inf_2 \in V_8$, $algoname \in V_{72}$ формируется строка

$$F_1 = KV||RAND||SQN||AMF||TOP_C||instance||add||inf_2||algoname \in V_{936},$$

где $instance[0] = instance[1] = instance[5] = instance[6] = 0$,

$$instance[2] = instance[3] = instance[4] = \begin{cases} 0||0||1, \text{если } |MAC_A| = 64, \\ 0||1||1, \text{если } |MAC_A| = 128, \\ 1||0||0, \text{если } |MAC_A| = 256, \end{cases}$$

$$instance[7] = \begin{cases} 0, \text{если } |K| = 128, \\ 1, \text{если } |K| = 256. \end{cases}$$

Далее вычисляется

$$H(F_1) = HF_1[522]|| \ldots ||HF_1[0] \in V_{512},$$

тогда

$$f_1 = \begin{cases} f_1[63]|| \ldots ||f_1[0] = HF_1[511]|| \ldots ||HF_1[448] \in V_{64}, \text{если } |MAC_A| = 64, \\ f_1[127]|| \ldots ||f_1[0] = HF_1[511]|| \ldots ||HF_1[384] \in V_{128}, \text{если } |MAC_A| = 128, \\ f_1[255]|| \ldots ||f_1[0] = HF_1[511]|| \ldots ||HF_1[256] \in V_{256}, \text{если } |MAC_A| = 256, \end{cases}$$

$$f_1^* = \begin{cases} f_1^*[63]|| \ldots ||f_1^*[0] = HF_1[255]|| \ldots ||HF_1[192] \in V_{64}, \text{если } |MAC_S| = 64, \\ f_1^*[127]|| \ldots ||f_1^*[0] = HF_1[255]|| \ldots ||HF_1[128] \in V_{128}, \text{если } |MAC_S| = 128, \\ f_1^*[255]|| \ldots ||f_1^*[0] = HF_1[255]|| \ldots ||HF_1[0] \in V_{256}, \text{если } |MAC_S| = 256. \end{cases}$$

6.3 Вычисление значений f_2, f_5, f_5^*

Из семи строк $RV \in V_{256}$, $RAND \in V_{128}$, $TOP_C \in V_{128}$, $instance \in V_8$, $add \in V_{32}$, $inf_3 \in V_8$, $algoname \in V_{72}$ формируется стока

$$F_{2,5} = KV||RAND||TOP_C||instance||add||inf_3||algoname \in V_{760},$$

где $instance[0] = instance[1] = 1$,

$$instance[2]||instance[3]||instance[4] = \begin{cases} 0||0||0, \text{если } |RES| = 32, \\ 0||0||1, \text{если } |RES| = 64, \\ 0||1||0, \text{если } |RES| = 128, \\ 1||0||0, \text{если } |RES| = 256, \end{cases}$$

$$instance[5] = \begin{cases} 0, \text{если } |CK| = 128, \\ 1, \text{если } |CK| = 256, \end{cases}$$

$$instance[6] = \begin{cases} 0, \text{если } |IK| = 128, \\ 1, \text{если } |IK| = 256, \end{cases}$$

$$instance[7] = \begin{cases} 0, \text{если } |K| = 128, \\ 1, \text{если } |K| = 256. \end{cases}$$

Далее вычисляется

$$H(F_{2,5}) = HF_{2,5}[511]|| \ldots ||HF_{2,5}[0] \in V_{512},$$

тогда

$$f_2 = \begin{cases} f_2[31]|| \ldots ||f_2[0] = HF_{2,5}[511]|| \ldots ||HF_{2,5}[480] \in V_{32}, \text{если } |RES| = 32, \\ f_2[63]|| \ldots ||f_2[0] = HF_{2,5}[511]|| \ldots ||HF_{2,5}[448] \in V_{64}, \text{если } |RES| = 64, \\ f_2[127]|| \ldots ||f_2[0] = HF_{2,5}[511]|| \ldots ||HF_{2,5}[384] \in V_{128}, \text{если } |RES| = 128, \\ f_2[255]|| \ldots ||f_2[0] = HF_{2,5}[511]|| \ldots ||HF_{2,5}[256] \in V_{256}, \text{если } |RES| = 256, \end{cases}$$

$$f_5 = f_5[47]|| \ldots ||f_5[0] = HF_{2,5}[255]|| \ldots ||HF_{2,5}[208] \in V_{48},$$
$$f_5^* = f_5^*[47]|| \ldots ||f_5^*[0] = HF_{2,5}[207]|| \ldots ||HF_{2,5}[160] \in V_{48}.$$

6.4 Вычисление значения f_3, f_4

Из семи строк $KV \in V_{256}$, $RAND \in V_{128}$, $TOP_C \in V_{128}$, $instance \in V_8$, $add \in V_{32}$, $inf_4 \in V_8$, $algoname \in V_{72}$ формируется строка

$$F_{3,4} = KV||RAND||TOP_C||instance||add||inf_4||algonsme \in V_{760},$$

где $instance[0] = instance[1] = 1$,

$$instance[2]||instance[3]||instance[4] = \begin{cases} 0||0||0, \text{если } |RES| = 32, \\ 0||0||1, \text{если } |RES| = 64, \\ 0||1||0, \text{если } |RES| = 128, \\ 1||0||0, \text{если } |RES| = 256, \end{cases}$$

$$instance[5] = \begin{cases} 0, \text{если } |CK| = 128, \\ 1, \text{ если } |CK| = 256, \end{cases}$$

$$instance[6] = \begin{cases} 0, \text{если } |IK| = 128, \\ 1, \text{ если } |IK| = 256, \end{cases}$$

$$instance[7] = \begin{cases} 0, \text{если } |K| = 128, \\ 1, \text{ если } |K| = 256. \end{cases}$$

Далее вычисляется

$$H(F_{3,4}) = H(F_{3,4})[511]|| \ldots ||H(F_{3,4})[0] \in V512,$$

тогда

$$f_3 = \begin{cases} f_3[127]|| \ldots ||f_3[0] = HF_{3,4}[511]|| \ldots ||HF_{3,4}[384] \in V_{128}, \textit{если } |CK| = 128, \\ f_3[255]|| \ldots ||f_3[0] = HF_{3,4}[511]|| \ldots ||HF_{3,4}[256] \in V_{256}, \textit{если } |CK| = 256, \end{cases}$$

$$f_4 = \begin{cases} f_4[127]|| \ldots ||f_4[0] = HF_{3,4}[255]|| \ldots ||HF_{3,4}[128] \in V_{128}, \textit{если } |IK| = 128, \\ f_4[255]|| \ldots ||f_4[0] = HF_{3,4}[255]|| \ldots ||HF_{3,4}[0] \in V_{256}, \textit{если } |IK| = 256. \end{cases}$$

Приложение А
(справочное)

Контрольные примеры

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

А.1 S3G-128

Пусть заданы строки:
1) *k* = 088*d*39*f*02*c*95*f*5925*c*9*e*94*c*7425*ee*37*b*;
2) *RAND* = 6009393*d*6*c*9*a*491*e*624*a*77510399*b*1*a*7;
3) *SQN* = 5121*d*1690714;
4) *AMF* = 055*a*;
5) *OP* = *f*26*dd*1*c*9*f*062819*c*40555228*e*0*db*07*ef*;
6) *add* = 00000000;
7) *algoname* = 415554.

А.1.1 Вычисление значения OP_C

Двоичное представление строки inf_1 = (0||0||0||0||0||0||0||0), тогда двоичное представление строки F_{OP} имеет следующий вид:

F_{OP} = 0000100010001101001110011111000000101100100101011111010110010010011011 0
01111010010100110001110100001001011110111000110111101111110010011011 01
11010001110010011111000001100010100000011001110001000000010101010100
10001010001110000011011011000001111110111100000000100000101010101010100,

тогда OP_C = 7*fddefd*5*d*53*d*94231*bb*4*d*6*f*005951513.

А.1.2 Вычисление значения f_1, f_1^*

Двоичное представление строки inf_2 = (0||0||0||0||0||0||1), а строка OP_C = 7*fddefd*5*d*53*d*94231*bb*4*d*6*f*005951513, тогда двоичное представление строки F_1 имеет следующий вид:

F_1 = 0000100010001101001110011111000000101100100
10101111101011001001001011100 10
01111010010100110001110100001001011110111000110111101111011000000000 1001
00111001001111010111011001001101001001001000111100110001001001010011101
11010100010000001110011001101100011010011101010001001000011101000 10110
10010000011100010100000001010101101001111111111011101111011111101010111
01010100111101100101000010001100011011101101001101011011110000000000101
10010101000101010001001100000000000000000000000000000000000000010100000
10101010101010100,

тогда f_1 = 6*a*58*ba*22*c*5*fe*9684 и f_1^* = *39f*7722129*dc*7*b*2*f*.

А.1.3 Вычисление значения $f_2, f_3, f_4, f_5, f_5^*$

Двоичное представление строки inf_2 = (0||0||0||0||0||1||0), а строка OP_C = 7*fddefd*5*d*53*d*94231*bb*4*d*6*f*005951513, тогда двоичное представление строки F_2 имеет следующий вид:

F_2 = 0000100010001101001110011111000000
10110010010101111101011001001001011100 10
01111010010100110001110100001001011110111000110111101111011000000000 1001
00111001001111010111011001001101001001001000111100110001001001010011101
11010100010000001110011001101100011010011101111111111011101111011111101
01011101010100111101100101000010001100011011101101001101011011110000000
00010110010101000101010001001100000000000000000000000000000000000000100
10000010101010101010100,

тогда

f_2 = 69*d*3*fe*288*be*95455,
f_3 = *c*748*a*67*aa*18*b*69*cf*8*eb*8*dd*9*c*5*a*551*d*49,
f_4 = 0448*e*4304*ade*3*bb*78142*e*7479*de*9*ee*9*e*,
f_5 = *b*207587*ff*31*d*,
f_5^* = *5af*1*a*6*d*14558.

А.2 S3G-256

Пусть заданы строки:

1) K = 088d39f02c95f5925c9e94c7425ee37b, тогда

KV = 088d39f02c95f5925c9e94c7425ee37b00000000000000000000000000000000

2) $RAND$ = a33c95d77713419f335ae19949195cc9;

3) SQN = e7b4ba4cf16d;

4) AMF = 5599610d52727524a2b61f4f5a5d17e6;

5) TOP = d0639a3$bced$0524a1ccd44ceb8de35dc96ed7$cfafb$9edd72db02c853998df6c9;

6) add = 00000000;

7) $algoname$ = 474f53545234333131.

А.2.1 Вычисление значения TOP_C

Двоичное представление строки inf_1 = (0||0||0||0||0||0||0), и $instance$ = 00, следовательно:

T = 088d39f02c95f5925c9e94c7425ee37b00000000000000000000

00000000000d0639a3$bced$0524a1ccd44ceb8de35dc96ed7cfafb9edd72db02c853998df6c90000474f$53545234333131,

тогда

TOP_C = 25b19816a39c2da75c29d618f1ed564aa09d25e8f068ad1b33d27c688862d03c.

А.2.2 Вычисление значения f_1, f_1^*

Будем считать, что $|MAC_A| = |MAC_S| = 64$, тогда строка $instance$ = 10. Двоичное представление строки inf_2 = (0||0||0||0||0||0||1), а строка

TOP_C = 25b19816a39c2da75c29d618f1ed564aa09d25e8f068ad1b33d27c688862d03c, следовательно:

F_1 = 088d39f02c95f5925c9e94c7425ee37b00000000000000000000000000000000
a33c95d77713419f335ae19949195cc9
e7b4ba4cf16d5599610d52727524a2b61f4f5a5d17
e625b19816a39c2da75c29d618f1ed564aa09d25e8f068ad1b33d27
c688862d03c100000000001474f53545234333131,

тогда

f_1 = 7229892127d6fb7e,
f_1^* = $677283b$5835c9aca.

А.2.3 Вычисление значения f_2, f_5, f_5^*

Будем считать, что $|RES|$ = 64 и $|CK| = |IK|$ = 128, тогда строка $instance$ = 13. Двоичное представление строки inf_3 = (0||0||0||0||0||1||0), а строка

TOP_C = 25b19816a39c2da75c29d618f1ed564aa09d25e8f068ad1b22d27c688862d03c, следовательно

$F_{2,5}$ = 088d39f02c95f5925c9e94c7425ee37b00000000000000000000000000000000
a33c95d77713419f335ae19949195cc925b19816a39c2
da75c29d618f1ed564aa09d25e8f068ad1b33d27c68886
2d03c130000000002474f53545234333131,

тогда

f_2 = 71cc28$becf$5cbb8f,
f_5 = 0c30d0ff9cc3,
f_5^* = 7b3f75928187.

А.2.4 Вычисление значения f_3, f_4

Будем считать, что $|RES|$ = 64 и $|CK| = |IK|$ = 128, тогда строка $instance$ = 13. Двоичное представление строки inf_4 = (0||0||0||0||0||1||1), а строка

TOP_C = 25b19816a39c2da75c29d618f1ed564aa09d25e8f068ad1b33d27c688862d03c, следовательно:

$F_{3,4}$ = 088d39f02c95f5925c9e94c7425ee37b00000000000000000000000000000000
a33c95d77713419f335ae19949195cc925b19816a39c2
da75c29d618f1ed564aa09d25e8f068ad1b33d27c68886
2d03c120000000003474f53545234333131,

тогда

f_3 = 9$bbac$93abd5872d0cd486f4b97f0975,
f_4 = 6e298dac304bb81ccb2d3b1aca22f871.

Библиография

[1] Описание архитекруры общей универсальной мобильной телекоммуникационной системы (3GPP TS 23.101 General Universal Mobile Telecommunications System (UMTS) architecture)

[2] Спецификации алгоритма MILENAGE: Пример алгоритма аутентификации и выработки ключей функциями f1, f1*, f2, f3, f4, f5 and f5*. Основное (3GPP TS 35.205. 3rd Generation Partnership Project;Technical Speciffcation Group Services and System Aspects; 3G Security; Speciffcation of the MILENAGE Algorithm Set: An example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 1: General)

[3] Спецификации алгоритма MILENAGE: Пример алгоритма аутентификации и выработки ключей функциями f1, f1*, f2, f3, f4, f5 and f5*. Описание алгоритма (3GPP TS 35.206. 3rd Generation Partnership Project; Technical Speciffcation Group Services and System Aspects; 3G Security; Speciffcation of the MILENAGE Algorithm Set: An example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 2: Algorithm Speciffcation)

[4] Спецификации алгоритма Tuak: Второй пример алгоритма аутентификации и выработки ключей функциями f1, f1*, f2, f3, f4, f5 and f5*. Описание алгоритма (3GPP TS 35.231. 3rd Generation Partnership Project; Technical Speciffcation Group Services and System Aspects; Speciffcation of the Tuak algorithm set: A second example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 1: Algorithm speciffcation)

[5] Спецификации алгоритма Tuak: Второй пример алгоритма аутентификации и выработки ключей функциями f1, f1*, f2, f3, f4, f5 and f5*. Описание контрольного примера (3GPP TS 35.233. 3rd Generation Partnership Project; Technical Speciffcation Group Services and System Aspects; Speciffcation of the Tuak algorithm set: A second example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 3: Design conformance test data)

УДК 681.3.06:006.354 ОКС 35.040

Ключевые слова: информационная технология, криптографическая защита информации, аутентификация, ключ, функция хэширования

БЗ 12—2017/52

Редактор *В.Н. Шмельков*
Технический редактор *В.Н. Прусакова*
Корректор *М.И. Першина*
Компьютерная верстка *И.А. Налейкиной*

Сдано в набор 27.10.2017. Подписано в печать 08.11.2017. Формат 60 × 84 1/8. Гарнитура Ариал.
Усл. печ. л. 1,86. Уч.-изд. л. 1,68. Тираж 21 экз. Зак. 2219.
Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Издано и отпечатано во ФГУП «СТАНДАРТИНФОРМ», 123001 Москва, Гранатный пер., 4.
www.gostinfo.ru info@gostinfo.ru