ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ

Р 1323565.1.009— 2017

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Использование алгоритмов блочного шифрования при формировании прикладных криптограмм в платежных системах

Издание официальное

Москва
Стандартинформ
2018

Предисловие

1 РАЗРАБОТАНЫ Обществом с ограниченной ответственностью «Системы практической безопасности» (ООО «СПБ») совместно с Открытым акционерным обществом «Информационные технологии и коммуникационные системы» (ОАО «ИнфоТеКС») и Обществом с ограниченной ответственностью «КРИПТО-ПРО» (ООО «КРИПТО-ПРО»)

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

3 УТВЕРЖДЕНЫ И ВВЕДЕНЫ В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 19 декабря 2017 г. № 2017-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

Введение

В настоящих рекомендациях рассмотрены алгоритмы формирования прикладных криптограмм, которые необходимы для доказательства факта выполнения транзакции держателем карты и результата транзакции. Эти криптограммы используются эмитентом для обеспечения невозможности для держателя карты отказаться от результата операции, а также для взаимной аутентификации карты и эмитента.

Примечание — Настоящие рекомендации дополнены приложением А.

РЕКОМЕНДАЦИИ ПО СТАНДАРТИЗАЦИИ

Информационная технология

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Использование алгоритмов блочного шифрования при формировании прикладных криптограмм в платежных системах

Information technology. Cryptographic data security.
Using block encryption algorithms in generation of application cryptograms for payment systems

Дата введения — 2018—06—01

1 Область применения

Описанные в настоящих рекомендациях алгоритмы рекомендуется применять для реализации механизмов обеспечения безопасности информации в платежной системе «МИР».

2 Нормативные ссылки

В настоящих рекомендациях использованы нормативные ссылки на следующие документы по стандартизации:

ГОСТ 28147—89 Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования

Р 1323565.1.010—2017 Информационная технология. Криптографическая защита информации. Использование функции диверсификации для формирования производных ключей платежного приложения

Примечание — При пользовании настоящими рекомендациями целесообразно проверить действие ссылочных документов 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 документ, на который дана недатированная ссылка, то рекомендуется использовать действующую версию этого документа с учетом всех внесенных в данную версию изменений. Если заменен ссылочный документ, на который дана датированная ссылка, то рекомендуется использовать версию этого документа с указанным выше годом утверждения (принятия). Если после утверждения настоящих рекомендаций в ссылочный документ, на который дана датированная ссылка, внесено изменение, затрагивающее положение, на которое дана ссылка, то это положение рекомендуется применять без учета данного изменения. Если ссылочный документ отменен без замены, то положение, в котором дана ссылка на него, применяется в части, не затрагивающей эту ссылку.

3 Обозначения

В настоящих рекомендациях использованы следующие обозначения:

V_n — конечномерное векторное пространство размерности n;

$A||B$ — конкатенация строк, т. е. если $A \in V_{n1}$, $B \in V_{n2}$, $A = (a_{n1-1}, a_{n1-2}, ..., a_0)$, $B = (b_{n2-1}, b_{n2-2}, ..., b_0)$, то $A||B = (a_{n1-1}, a_{n1-2}, ..., a_0, b_{n2-1}, b_{n2-2}, ..., b_0) \in V_{n1+n2}$;

Издание официальное

0^r — строка, состоящая из r нулей;

AAC — криптограмма, формируемая картой и проверяемая эмитентом в том случае, когда карта принимает решение об отклонении транзакции. Длина значения равна 8 байтам;

AC — прикладная криптограмма (Application Cryptogram), формируемая картой. Длина значения равна 8 байтам;

ARPC — криптограмма, формируемая эмитентом и проверяемая картой. Используется картой для аутентификации эмитента. Длина значения равна 8 байтам;

ARQC — криптограмма, формируемая картой и проверяемая эмитентом в том случае, когда карта принимает решение о выполнении операции в режиме онлайн. Длина значения равна 8 байтам;

CSU — card Status Update. Длина значения равна 4 байтам;

D — данные для вычисления криптограммы. Длина значения равна 72 байтам;

MAC — функция выработки имитовставки в соответствии с ГОСТ 28147—89. Длина значения равна 4 байтам;

Pad7 — фиксированные данные паддинга длиной 7 байт, имеющие в двоичном представлении значение $1||0^{55}$;

Pad56 — фиксированные данные паддинга длиной 56 байт, имеющие в двоичном представлении значение $1||0^{447}$;

SK_{AC} — сессионный ключ карты для формирования АС, сформированный в соответствии с Р 1323565.1.010—2017. Длина значения равна 32 байтам;

TC — криптограмма, формируемая картой и проверяемая эмитентом, в том случае, когда карта принимает решение об одобрении транзакции. Длина значения равна 8 байтам.

4 Описание алгоритмов

Возможные значения аргументов функций в представленных алгоритмах ограничены допустимостью их использования в качестве входных параметров преобразований.

4.1 Алгоритм формирования прикладных криптограмм ARQC, TC, AAC

Формирование прикладных криптограмм *ARQC, TC, AAC* осуществляется на основе функции вычисления имитовставки (*MAC*) от *D* и *Pad7* в соответствии с ГОСТ 28147—89 в режиме выработки имитовставки с имитовставки с узлом замены id-tc26-gost-28147-param-Z:

$ARQC = MAC\ (SK_{AC},\ D||Pad7)||MAC\ (SK_{AC},\ D||Pad7)$

$TC = MAC\ (SK_{AC},\ D||Pad7)||MAC\ (SK_{AC},\ D||Pad7)$

$AAC = MAC\ (SK_{AC},\ D||Pad7)||MAC\ (SK_{AC},\ D||Pad7)$

где данные *D* представлены в виде, определенном в таблице 1.

Таблица 1

Поле	Размер, байт	Источник
Amount, Authorised	6	Терминал
Amount, Other	6	Терминал
Terminal Country Code	2	Терминал
Terminal Verification Results	5	Терминал
Transaction Currency Code	2	Терминал
Transaction Date	3	Терминал
Transaction Type	1	Терминал
Unpredictable Number	4	Терминал
Application Interchange Profile	2	Приложение
Application Transaction Counter	2	Приложение
Issuer Application Data	32	Приложение

Данные для вычисления криптограмм *ARQC, AAC и TC* отличаются в 5—8 битах 4-го байта поля Issuer Application Data. Данные биты формируются по правилу, приведенному в таблице 2.

Таблица 2

b8	b7	b6	b5	b4	b3	b2	b1	Значение
x	x							Тип криптограммы, возвращенной после второй команды GENERATE AC
0	0							AAC
0	1							TC
1	0							Вторая команда GENERATE AC не отправлялась
1	1							Зарезервировано для использования
		x	x					Тип криптограммы, возвращенной после первой команды GENERATE AC
		0	0					AAC
		0	1					TC
		1	0					ARQC
		1	1					Зарезервировано для использования

Далее полученная криптограмма вместе с данными для вычисления криптограммы направляется эмитенту для верификации.

Примечание — При офлайн-аутентификации карта самостоятельно принимает решение об одобрении транзакции и ограничивается созданием криптограммы AAC/TC, отправляемой в составе клирингового сообщения.

4.2 Алгоритм формирования прикладной криптограммы ARPC

Формирование прикладной криптограммы *ARPC* осуществляется в случае положительного результата проверки криптограммы *ARQC* эмитентом. Для этого вычисляется имитовставка (*MAC*) от *ARQC, CSU* и *Pad56* в соответствии с ГОСТ 28147—89 в режиме выработки имитовставки с имитовставки с узлом замены id-tc26-gost-28147-param-Z:

$$ARPC = MAC(SK_{AC}, ARQC||CSU||0x00||0x00||0x00||0x00||Pad56)||$$
$$MAC(SK_{AC}, ARQC||CSU||0x00||0x00||0x00||0x00||Pad56)$$

Далее полученная криптограмма вместе с *CSU* направляется платежному приложению карты для верификации.

Приложение А
(справочное)

Контрольные примеры

Приводимые ниже значения параметров *D*, *CSU*, а также значение ключа SK_{AC} рекомендуется использовать только для проверки корректной работы конкретной реализации алгоритмов, описанных в настоящих рекомендациях.

Все числовые значения приведены в десятичной или шестнадцатеричной записи. Нижний индекс в записи числа обозначает основание системы счисления.

В данном приложении двоичные строки из V^*, длина которых кратна 4, записаны в шестнадцатеричном виде, а символ конкатенации («||») опускается. То есть строка $a \in V_{4r}$ будет представлена в виде $a_{r-1}\, a_{r-2} \ldots a_0$, где $a_i \in \{0, 1, \ldots, 9, a, b, c, d, e, f\}$, $i = 0, 1, \ldots, r-1$. Соответствие между двоичными строками длины 4 и шестнадцатеричными строками длины 1 задается естественным образом (таблица А.1).

Преобразование, ставящее в соответствие двоичной строке длины $4r$ шестнадцатеричную строку длины r, и соответствующее обратное преобразование для простоты записи опускаются.

Таблица А.1 — Соответствие между двоичными и шестнадцатеричными строками

0000	0
0001	1
0010	2
0011	3
0100	4
0101	5
0110	6
0111	7
1000	8
1001	9
1010	a
1011	b
1100	c
1101	d
1110	e
1111	f

А.1 Исходные данные

Для вычисления прикладных криптограмм *ARQC, TC, AAC* и *ARPC* используются следующие данные:
CSU = $a3feee5b_{16}$

Данные *D* для вычисления криптограммы *ARQC*
D = 0102030405060708090*a*0*b*0*c*0*d*0*e*0*f*10\\
11121314151617181 91a1b1c1d1e1f20\\
21222324*a*0262728292*a*2*b*2*c*2*d*2*e*2*f*30\\
3132333435363738393*a*3*b*3*c*3*d*3*e*3*f*40\\
0180000000000000_{16}

Данные *D* для вычисления криптограммы *TC*
D = 0102030405060708090*a*0*b*0*c*0*d*0*e*0*f*10\\
11121314151617181 91*a*1*b*1*c*1*d*1*e*1*f*20\\
21222324 90262728292*a*2*b*2*c*2*d*2*e*2*f*30\\
3132333435363738393*a*3*b*3*c*3*d*3*e*3*f*40\\
0280000000000000_{16}

Данные *D* для вычисления криптограммы *AAC*

D = 0102030405060708090*a*0*b*0*c*0*d*0*e*0*f*10\\
1112131415161718191*a*1*b*1*c*1*d*1*e*1*f*20\\
2122232480262728292*a*2*b*2*c*2*d*2*e*2*f*30\\
3132333435363738393*a*3*b*3*c*3*d*3*e*3*f*40\\
0380000000000000_{16}

Символ «\\» обозначает перенос числа на новую строку.

А.1.1 Ключ шифрования

Для вычисления криптограмм используется следующее значение сессионного ключа SK_{AC}:

SK_{AC} = 0*ad*0*b*272*ecaa*5*a*5*dd*6917788*b*33609*dd*\\
*c*55*ff*7641311414*eff*9*d*11*cc*25*aa*85*b*5$_{16}$

А.1.2 Формирование прикладных криптограмм ARQC, TC, AAC

На основе исходных данных и сессионного ключа SK_{AC} получают следующие значения прикладных криптограмм:

AAC = 92122*fbe*92122*fbe*$_{16}$

TC = 5*c*75*b*8*ec*5*c*75*b*8*ec*$_{16}$

ARQC = 137*b*5307137*b*5307$_{16}$

А.1.3 Формирования прикладной криптограммы ARPC

На основе исходных данных, сессионного ключа SK_{AC} и полученного значения криптограммы *ARQC* вычисляют прикладную криптограмму *ARPC*:

ARPC = 8*b*9*cf*1*b*78*b*9*cf*1*b*7$_{16}$

А.2 Исходные данные

Для вычисления прикладных криптограмм *ARQC, TC, AAC* и *ARPC* используют следующие данные:

CSU = *a*2*fdee*5*c*$_{16}$

Данные *D* для вычисления криптограммы *ARQC*

D = 0102030405060708090*a*0*b*0*c*0*d*0*e*0*f*10\\
1112131415161718191*a*1*b*1*c*1*d*1*e*1*f*20\\
21222324*a*0262728292*a*2*b*2*c*2*d*2*e*2*f*30\\
3132333435363738393*a*3*b*3*c*3*d*3*e*3*f*40\\
2180000000000000_{16}

Данные *D* для вычисления криптограммы *TC*

D = 0102030405060708090*a*0*b*0*c*0*d*0*e*0*f*10\\
1112131415161718191*a*1*b*1*c*1*d*1*e*1*f*20\\
2122232490262728292*a*2*b*2*c*2*d*2*e*2*f*30\\
3132333435363738393*a*3*b*3*c*3*d*3*e*3*f*40\\
2280000000000000_{16}

Данные *D* для вычисления криптограммы *AAC*

D = 0102030405060708090*a*0*b*0*c*0*d*0*e*0*f*10\\
1112131415161718191*a*1*b*1*c*1*d*1*e*1*f*20\\
2122232480262728292*a*2*b*2*c*2*d*2*e*2*f*30\\
3132333435363738393*a*3*b*3*c*3*d*3*e*3*f*40\\
2380000000000000_{16}

А.2.1 Ключ шифрования

Для вычисления криптограмм используют следующее значение сессионного ключа SK_{AC}:

SK_{AC} = 2*fc*05*c*579*fe*55720*a*6*aa*0*e*0*a*1567*ef*38\\
*bd*46*fc*4*fe*462*c*0*a*01*ed*485*fe*2743897*c*$_{16}$

А.2.2 Формирование прикладных криптограмм ARQC, TC, AAC

На основе исходных данных и сессионного ключа SK_{AC} получают следующие значения прикладных криптограмм:

AAC = 66df461d66df461d$_{16}$

TC = be786781be786781$_{16}$

ARQC = 3e39dd7b3e39dd7b$_{16}$

А.2.3 Формирования прикладной криптограммы ARPC

На основе исходных данных, сессионного ключа SK_{AC} и полученного значения криптограммы *ARQC* вычисляют прикладную криптограмму *ARPC*:

ARPC = *bd*663*e*7*bbd*663*e*7*b*$_{16}$

А.3 Исходные данные

Для вычисления прикладных криптограмм *ARQC, TC, AAC* и *ARPC* использованы следующие данные:
CSU = *a*1*fcee*5*d*$_{16}$

Данные *D* для вычисления криптограммы *ARQC*
D = 0102030405060708090*a*0*b*0*c*0*d*0*e*0*f*10\\
11121314151617181 91*a*1*b*1*c*1*d*1*e*1*f*20\\
21222324*a*0262728292*a*2*b*2*c*2*d*2*e*2*f*30\\
313233343536373839 3*a*3*b*3*c*3*d*3*e*3*f*40\\
3180000000000000$_{16}$

Данные *D* для вычисления криптограммы *TC*
D = 0102030405060708090*a*0*b*0*c*0*d*0*e*0*f*10\\
11121314151617181 91*a*1*b*1*c*1*d*1*e*1*f*20\\
21222324902627282 92*a*2*b*2*c*2*d*2*e*2*f*30\\
313233343536373839 3*a*3*b*3*c*3*d*3*e*3*f*40\\
3280000000000000$_{16}$

Данные *D* для вычисления криптограммы *AAC*
D = 0102030405060708090*a*0*b*0*c*0*d*0*e*0*f*10\\
11121314151617181 91*a*1*b*1*c*1*d*1*e*1*f*20\\
21222324802627282 92*a*2*b*2*c*2*d*2*e*2*f*30\\
313233343536373839 3*a*3*b*3*c*3*d*3*e*3*f*40\\
3380000000000000$_{16}$

А.3.1 Ключ шифрования

Для вычисления криптограмм использовано следующее значение сессионного ключа SK_{AC}:
SK_{AC} = *f*5*d*49771*ba*7*ab*6*b*1*a*8110*d*12*dcb*160*fd*\\
*a*478*f*81*b*9*b*17*f*24*d*938*be*111*a*68*ffcfa*$_{16}$

А.3.2 Формирование прикладных криптограмм ARQC, TC, AAC

На основе исходных данных и сессионного ключа SK_{AC} получают следующие значения прикладных криптограмм:

AAC = 125*f*0*aaa*125*f*0*aaa*$_{16}$
TC = 4694330046943300$_{16}$
ARQC = 3780602937806029$_{16}$

А.3.3 Формирования прикладной криптограммы ARPC

На основе исходных данных, сессионного ключа SK_{AC} и полученного значения криптограммы *ARQC* вычисляется прикладная криптограмма *ARPC*:

ARPC = 5*b*3918725*b*391872$_{16}$

УДК 681.3.06:006.354 ОКС 35.040

Ключевые слова: информационная технология, криптографическая защита информации, аутентификация, ключ, прикладная криптограмма, транзакция, платежное приложение, платежная карта

БЗ 1—2018/94

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

Сдано в набор 20.12.2017. Подписано в печать 13.02.2018. Формат 60 × 84$^{1}/_{8}$. Гарнитура Ариал.
Усл. печ. л. 1,40. Уч.-изд. л.1,26. Тираж 19 экз. Зак. 101.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

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

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