Министерство образования Республики Беларусь
Белорусский государственный университет
НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ИНСТИТУТ
ПРИКЛАДНЫХ ПРОБЛЕМ МАТЕМАТИКИ И ИНФОРМАТИКИ

УТВЕРЖДАЮ
Директор НИИ прикладных проблем
математики и информатики

Ю.С.Харин
«___» _____ 2022 г.

МЕТОДИКА ИСПЫТАНИЙ СРЕДСТВ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ НА СООТВЕТСТВИЕ ТРЕБОВАНИЯМ СТБ 34.101.66-2014

МИ.10166.10.01

Листов 53

Минск 2022

Предисловие

Настоящая методика испытаний предназначена для использования в испытательных лабораториях при проведении сертификационных испытаний средств криптографической защиты информации на соответствие требованиям СТБ 34.101.66-2014 «Информационные технологии и безопасность. Протоколы формирования общего ключа на основе эллиптических кривых».

Содержание

1 Нормативные ссылки

В настоящем документе использованы ссылки на следующие стандарты:

ГОСТ 19.202-78 «Единая система программной документации. Спецификация. Требования к содержанию и оформлению».

ГОСТ 19.401-2000 «Единая система программной документации. Текст программы. Требования к содержанию, оформлению и контролю качества».

ГОСТ 19.402-2000 «Единая система программной документации. Описание программы. Требования к содержанию, оформлению и контролю качества».

ГОСТ 19.504-79 «Единая система программной документации. Руководство программиста. Требования к содержанию и оформлению».

СТБ 34.101.31-2020 «Информационные технологии и безопасность. Алгоритмы шифрования и контроля целостности».

СТБ 34.101.45-2013 «Информационные технологии и безопасность. Алгоритмы электронной цифровой подписи и транспорта ключа на основе эллиптических кривых».

СТБ 34.101.66-2014 «Информационные технологии и безопасность. Протоколы формирования общего ключа на основе эллиптических кривых».

СТБ 34.101.77-2020 «Информационные технологии и безопасность. Криптографические алгоритмы на основе sponge-функции».

2 Термины, обозначения и сокращения

В настоящем документе применяются термины и обозначения СТБ 34.101.66, а также следующие сокращения:

ЕСПД единая система программной документации;

СКЗИ средство криптографической защиты информации;

3 Объект и цель испытаний

На испытания представляется средство криптографической защиты информации (СКЗИ), реализующее криптографические алгоритмы и протоколы СТБ 34.101.66, и документация на СКЗИ.

Целью испытаний является проверка соответствия объекта испытаний требованиям СТБ 34.101.66.

4 Требования к объекту испытаний

К программе объекта испытаний предъявляются следующие требования, подлежащие проверке во время проведения испытаний:

– в программе должны быть точно и полно реализовываны криптографические алгоритмы и протоколы СТБ 34.101.66, поддерживаемые объектом испытаний;

– программа, реализующая криптографические алгоритмы, протоколы и требования СТБ 34.101.66, не должна содержать недокументированные возможности.

Документация на объект испытаний должна включать документы «Спецификация», «Текст программы» и может включать документы «Описание программы», «Руководство

программиста» и другие документы. Документация может быть разработана в соответствии с требованиями единой системы программной документации (ЕСПД).

5 Средства и порядок испытаний

5.1 Общие сведения

Испытания программы состоят из трех этапов:

1 Анализ документации.

2 Тестирование программы.

3 Анализ исходных текстов программы.

Выполнение этапа 1 осуществляется экспертами по анализу документации, выполнение этапа 2 — экспертами по тестированию, а выполнение этапа 3 — экспертами по анализу исходных текстов. К проведению испытаний должно быть привлечено не менее двух экспертов по анализу исходных текстов и один или более эксперт по тестированию. К анализу документации должен быть привлечен, по крайней мере, один эксперт по анализу исходных текстов программ.

По результатам выполнения этапа испытаний эксперт оформляет протокол результатов проверок: протокол анализа документации, протокол тестирования, протокол анализа исходных текстов. В протоколе эксперт делает вывод о соответствии (не соответствии) программы требованиям СТБ 34.101.66. Если программа не поддерживает некоторые алгоритмы и протоколы, определенные в СТБ 34.101.66, то в протоколе делается соответствующее примечание. Примеры оформления протоколов приводятся в приложениях А, Б, В. Допускается оформления протоколов в иной форме, но с обязательным указанием результатов по каждой проводимой проверке и вывода о соответствии (не соответствии).

Если в испытуемой программе используются реализации алгоритмов или протоколов СТБ 34.101.66, которые в составе других программ имеют действующие сертификаты соответствия требованиям СТБ 34.101.66, то проверки по тестированию и анализу исходных текстов для данных реализаций могут не проводиться. При этом для подтверждения соответствия объекта испытаний требованиям СТБ 34.101.66 экспертом оформляется протокол проверки совпадения контрольных характеристик (хэш-значений) файлов реализации испытуемой программы с контрольными характеристиками соответствующих файлов, указанными в сертификатах соответствия.

На основании протоколов результатов проверок оформляется протокол испытаний, обобщающий результаты испытаний программы. В протоколе испытаний вывод о соответствии программы требованиям СТБ 34.101.66 делается тогда и только тогда, когда вывод о соответствии содержится во всех протоколах результатов проверок. Оформление протокола испытаний проводится в соответствии с требованиями технических нормативно-правовых актов в области сертификации продукции, а также документации, применяемой в испытательной лаборатории.

5.2 Анализ документации

Эксперт проводит анализ документации путем проверки соответствия документации программе объекта испытаний. Такой анализ состоит в получении экспертных заключений, касающихся проверки следующих документов:

– спецификация (см. п. 6.1.1);

– текст программы (см. п. 6.1.2);

– описание программы (см. п. 6.1.3);
– руководство программиста (см. п. 6.1.4).

Анализ документов «Описание программы» и «Руководство программиста» производится в случае их наличия.

5.3 Тестирование

Эксперт проводит тестирование путем выполнения испытуемой программы для некоторого набора проверочных входных значений и сравнения полученных результатов с истинными. Истинные результаты, используемые при тестировании, формируются с помощью эталонной реализации.

Эталонной считается реализация, которая ранее успешно прошла сертификационные испытания на соответствие СТБ 34.101.66 или которая удовлетворяет следующим условиям:

1 Проведен анализ исходных текстов программ эталонной реализации. К анализу привлекались, по меньшей мере, два независимых эксперта. Использовалась методика анализа исходных текстов, определенная в п. 6.3.

2 Проведено тестирование эталонной реализации. При тестировании использовались две другие независимые реализации. Использовались тесты, определенные в п. 6.2, а также тестовые примеры СТБ 34.101.66.

Тестированию подлежат криптографические алгоритмы и протоколы, реализованные в программе и определенные в СТБ 34.101.66, включая:

– алгоритм построения ключа (см. п. 6.2.2);
– алгоритм построения точки эллиптической кривой (см. п. 6.2.3);
– протокол BMQV (см. п. 6.2.4);
– протокол BSTS (см. п. 6.2.6);
– протокол BPACE (см. п. 6.2.6);
– протокол Диффи-Хеллмана (см. п. 6.2.7).

Если программа не реализует некоторые из алгоритмов и протоколов, определенных в СТБ 34.101.66, то тесты для них не выполняются.

Для организации тестирования в исходные тексты программы допускается вносить изменения и дополнения, касающиеся:

– способа чтения входных данных;
– способа записи выходных данных.

При внесении модификаций в исходные тексты должен быть проведен анализ корректности внесенных изменений.

При успешном выполнении тест возвращает признак `УСПЕХ`, иначе — `ОШИБКА`. Если при тестировании программы для некоторых входных значений получены результаты отличные от истинных значений, то эксперт по тестированию должен указать эти входные значения программы и результат ее работы, а также, по требованию, результаты промежуточных вычислений экспертам по анализу исходных текстов.

5.4 Анализ исходных текстов

Эксперт проводит анализ исходных текстов путем проверки корректности реализации в испытуемой программе криптографических алгоритмов и протоколов СТБ 34.101.66. Такой анализ состоит в получении экспертных заключений, касающихся:

– корректности использования локальных переменных (см. п. 6.3.1);
– корректности использования глобальных переменных (см. п. 6.3.2);
– корректности использования констант (см. п. 6.3.3);
– корректности программной логики функций программы (см. п. 6.3.4);
– корректности вызова стандартных функций (см. п. 6.3.5);
– корректности вызова функций программы (см. п. 6.3.6);
– корректности обработки исключительных ситуаций (см. п. 6.3.7);
– корректности реализации криптографических примитивов (см. п. 6.3.8);
– корректности реализации криптографических алгоритмов и протоколов (см. п. 6.3.9);
– корректности управления секретными данными (см. п. 6.3.10);
– отсутствия недокументированных возможностей (см. п. 6.3.11).

6 Методы испытаний

6.1 Анализ документации

6.1.1 Документ «Спецификация»

При анализе документа «Спецификация» эксперт проверяет, что в нем указаны компоненты и документация, представляемые на испытания.

Если документ «Спецификация» разработан в соответствии с требованиями ЕСПД, то эксперт проверяет, что содержание и оформление документа соответствует ГОСТ 19.202.

6.1.2 Документ «Текст программы»

При анализе документа «Текст программы» эксперт проверяет, что исходные тексты программы, реализующие определенные в СТБ 34.101.66 криптографические алгоритмы и протоколы, представлены полностью и в виде, который использовался при сборке программы.

Если документ «Текст программы» разработан в соответствии с требованиями ЕСПД, то эксперт проверяет, что содержание и оформление документа соответствует ГОСТ 19.401.

6.1.3 Документ «Описание программы»

При анализе документа «Описание программы» эксперт проверяет выполнение следующих требований:

– в документе должна быть указана информация, однозначно идентифицирующая вызываемые стандартные функции (версия компилятора, используемые стандартные библиотеки и т.п.);

– документ должен определять программные модули, реализующие определенные в СТБ 34.101.66 криптографические алгоритмы и протоколы;

– описание программы в терминах программных модулей должно соответствовать исходным текстам программы.

Если документ «Описание программы» разработан в соответствии с требованиями ЕСПД, то эксперт проверяет, что содержание и оформление документа соответствует ГОСТ 19.402.

6.1.4 Документ «Руководство программиста»

При анализе документа «Руководство программиста» эксперт проверяет выполнение следующих требований:

– документ должен содержать описание всех доступных для вызова функций, реализующих определенные в СТБ 34.101.66 криптографические алгоритмы и протоколы;

– описание функций, реализующих определенные в СТБ 34.101.66 криптографические алгоритмы и протоколы, и условия их использования должны соответствовать исходным текстам программы.

При описании в документации функций должны выполняться следующие условия:

– каждая функция должна иметь описание назначения;

– каждый параметр функции должен иметь описание назначения, типа и, при необходимости, диапазона допустимых значений;

– каждая функция должна иметь описание возвращаемого результата с указанием типа;

– каждая функция должна иметь описание условий, при выполнении которых в ходе работы функции могут возникать ошибочные ситуации, требующие специальной обработки;

– в случае если при реализации криптографического алгоритма используется более одной доступной для вызова функции, должны быть указаны порядок и условия вызова данных функций.

Если документ «Руководство программиста» разработан в соответствии с требованиями ЕСПД, то эксперт проверяет, что содержание и оформление документа соответствует ГОСТ 19.504.

6.2 Тестирование

6.2.1 Идентификаторы и долговременные ключи

При тестировании реализаций протоколов используются идентификаторы Id, личные ключи d и открытые ключи Q, пароли P из таблиц 1 – 3. Сертификаты сторон представляют собой объединение их идентификаторов и открытых ключей: $\mathtt{Cert}(Id, Q) = Id \| Q$.

Таблица 1 — Идентификаторы, долговременные ключи и пароль ($l = 128$)

Id_A	$\mathtt{416C696365}_{16}$
$\langle d_A \rangle_{256}$	$\mathtt{1F66B5B8\ 4B733967\ 4533F032\ 9C74F218\ 34281FED\ 0732429E}$ $\mathtt{0C79235F\ C273E269}_{16}$
$\langle Q_A \rangle_{512}$	$\mathtt{BD1A5650\ 179D79E0\ 3FCEE49D\ 4C2BD5DD\ F54CE46D\ 0CF11E4F}$ $\mathtt{F87BF7A8\ 90857FD0\ 7AC6A603\ 61E8C817\ 3491686D\ 461B2826}$ $\mathtt{190C2EDA\ 5909054A\ 9AB84D2A\ B9D99A90}_{16}$
Id_B	$\mathtt{426F62}_{16}$
$\langle d_B \rangle_{256}$	$\mathtt{4C0E74B2\ CD5811AD\ 21F23DE7\ E0FA742C\ 3ED6EC48\ 3C461CE1}$ $\mathtt{5C33A77A\ A308B7D2}_{16}$
$\langle Q_B \rangle_{512}$	$\mathtt{CCEEF1A3\ 13A40664\ 9D15DA0A\ 851D486A\ 695B641B\ 20611776}$ $\mathtt{252FFDCE\ 39C71060\ 7C9EA1F3\ 3C23D20D\ FCB8485A\ 88BE6523}$ $\mathtt{A28ECC32\ 15B47FA2\ 89D6C9BE\ 1CE837C0}_{16}$
P	$\mathtt{38303836}_{16}$

Таблица 2 — Идентификаторы, долговременные ключи и пароль ($l = 192$)

Id_A	$416C696365_{16}$
$\langle d_A \rangle_{384}$	84C21DBF 7B3C2372 DC21386C 216FA16C 9EF10AEA F9F96A87 2FD8058F 2780BA93 0F08BE3B EC804161 37E11A23 $2D93B50E_{16}$
$\langle Q_A \rangle_{768}$	212602EE 5589B84A 4585807A E8BFE371 8A52B675 8B05F644 05F9D371 6462B02D 334D51CF 27125637 37F63F5B 9BE7E4DA 8634E65F 71905CB7 204DC5BC 1229FB68 76ED4F60 EC299D49 9AB0641A 5F82F291 517F7631 4B50A0ED 389368A5 $690EC3A5_{16}$
Id_B	$426F62_{16}$
$\langle d_B \rangle_{384}$	5DBFB5CC E18A214E 66D2ED80 E966F8D9 61B3924E FB8E2DD9 A4881E0F 8630D969 3A803389 31CC9F66 65453BE8 $24ACBDD6_{16}$
$\langle Q_B \rangle_{768}$	59FFC705 02915B98 439870EC 76B3B489 0B737C00 58BD4D72 A71A744A D9730760 336BA852 348FD2A0 DE7BF1A5 1C6E0970 423A96ED 7BC9CD92 FE5B0A18 B300711C 449B6424 F97BCE90 A659B35A 8170CD17 51E4905A 4D81DA64 F08EE57D $C05F3D59_{16}$
P	38303836_{16}

Таблица 3 — Идентификаторы, долговременные ключи и пароль ($l = 256$)

Id_A	$416C696365_{16}$
$\langle d_A \rangle_{512}$	BEC09635 3EF4568A A417622A 95F2B563 33BF3A02 040B3137 2FD5737D E0F1A2BA 6090C1D1 A27155D8 711FFE5B 31027847 1B0B97CF 1B8FE821 C50205E5 $D24AB9B8_{16}$
$\langle Q_A \rangle_{1024}$	C6255C65 515274CD 10E68B2F C13E16B2 2CB7AC00 D45ABE2A 2FD0CA5E 4E472895 43C20F62 56A5FAD3 3E862894 C15A477E C4BBEE3C 139D9548 4243BA97 F200CA35 048521F7 AB27D7CF 81658CD7 D36018CE B8FE6446 8F1E096A 0CB5638D 11C4697B B7C9A1CA EAF5F243 A6477BE8 B306F20B D45E5BB5 A8986FED 554509FD $5FDC39D6_{16}$
Id_B	$426F62_{16}$
$\langle d_B \rangle_{512}$	213B96E9 F90CDFD4 BC21DB8B 59879176 D7347248 107E66C7 1438B14F FFB692B8 637E5B6E 04C41DF5 5868299D 811F4381 BE31657A CF601BDD AE57AB5B $238CA112_{16}$
$\langle Q_B \rangle_{1024}$	608879BC 5AA49480 67125B70 CA6A8F55 69C8F7E4 C9324B71 34B52957 6BF57C0C 32058123 E271A545 3A4DB1A6 53AC1242 BED760B2 589F5BF8 B2C8ECD7 9DF8D460 FD2A2C0F D59E143A E416F55B 6FC4A8EB FDACC870 5C4C68D4 C6D3FB46 82FFC524 6AE03855 73593B42 09508758 8D87C0EE 991CFE8E 3290EF97 20ECBCA8 $AA8EFF51_{16}$
P	38303836_{16}

6.2.2 Алгоритм построения ключа

При тестировании реализации алгоритма построения ключа выполняются тесты BAKE.KDF.1 – BAKE.KDF.3.

Входными данными тестов являются секретное слово $X \in \{0,1\}^*$, дополнительное слово $S \in \{0,1\}^*$ и номер ключа C — неотрицательное целое число.

В тестах для хранения результата построения ключа используется слово $Y \in \{0,1\}^{256}$.

Тест BAKE.KDF.1

1 Задать секретное слово:

$$X \leftarrow \texttt{829614D8 411DBBC4 E1F2471A 40045864 40FD8C95 53FAB6A1 A45CE417 AE97111E}_{16}.$$

2 Задать дополнительное слово:

$$S \leftarrow \texttt{00000000 00000000 00000000 00000000}_{16}.$$

3 Задать номер ключа: $C \leftarrow 0$.

4 Испытуемой реализацией выполнить построение ключа и сохранить результат в Y.

5 Если

$$Y = \texttt{0E64472D 51884074 45AE0135 846F187C 54730521 278973F4 37DC50FF 5A3143D2}_{16},$$

то возвратить `УСПЕХ`, иначе — `ОШИБКА`.

Тест BAKE.KDF.2

1 Задать секретное слово:

$$X \leftarrow \texttt{193C9DC1 0290D0BC 49AEC10A 5B1A1DE7 A13A73CA 54EA17A3 DDA50D61 C3E1A880 19733179 14AED80A A69A51A3 4C26F415}_{16}.$$

2 Задать дополнительное слово:

$$S \leftarrow \texttt{00000000 00000000 00000000 00000000 00000000 00000000}_{16}.$$

3 Задать номер ключа: $C \leftarrow 1$.

4 Испытуемой реализацией выполнить построение ключа и сохранить результат в Y.

5 Если

$$Y = \texttt{8880BA76 45E0043E 1A154179 3AED5929 0F26D0CE CD4EA0E9 8C968013 609B1E1C}_{16},$$

то возвратить `УСПЕХ`, иначе — `ОШИБКА`.

Тест BAKE.KDF.3

1 Задать секретное слово:

$$X \leftarrow \texttt{2C83E719 FD2F2CB9 80E39503 8CCDB67A 5BDCEF1F 642EB7F9}$$
$$\texttt{037C8B9A 657BE01A E995CAE7 E6121CFE 7099BE62 C9DD6534}$$
$$\texttt{EE86E7E2 92DBF610 52B36FCA 685D6462}_{16}.$$

2 Задать дополнительное слово:

$$S \leftarrow \texttt{00000000 00000000 00000000 00000000 00000000 00000000}$$
$$\texttt{00000000 00000000}_{16}.$$

3 Задать номер ключа: $C \leftarrow 2$.

4 Испытуемой реализацией выполнить построение ключа и сохранить результат в Y.

5 Если

$$Y = \texttt{FCBCD647 7CE3ECF9 5FAEC863 E25E504C 047898DF A0C6FC15}$$
$$\texttt{43604A13 F7CD8706}_{16},$$

то возвратить `УСПЕХ`, иначе — `ОШИБКА`.

6.2.3 Алгоритм построения точки эллиптической кривой

При тестировании реализации алгоритма построения точки эллиптической кривой выполняются тесты BAKE.SWU.1 – BAKE.SWU.3.

Входными данными тестов являются параметры p, a и b, которые описывают группу точек эллиптической кривой и определяют уровень стойкости l, а также слово $X \in \{0,1\}^{2l}$.

В тестах для хранения результата построения точки эллиптической кривой используется точка $W \in E^*_{a,b}(\mathbb{F}_p)$.

Тест BAKE.SWU.1

1 Задать параметры p, a и b из таблицы Б.1 СТБ 34.101.45.

2 Задать слово, для которого строится точка:

$$X \leftarrow \texttt{829614D8 411DBBC4 E1F2471A 40045864 40FD8C95 53FAB6A1}$$
$$\texttt{A45CE417 AE97111E}_{16}.$$

3 Испытуемой реализацией выполнить построение точки эллиптической кривой и сохранить результат в W.

4 Если

$$\langle W \rangle_{512} = \texttt{AD6215E0 70BD08F4 575912B7 E41EF3DB 23FDC82C C0609D85}$$
$$\texttt{084E506D 9741BA5D FE2509AB 6F85C737 8310A8B6 849C2B25}$$
$$\texttt{D5CEE3DE 3C08EEF4 74C4FA1D B10FD662}_{16},$$

то возвратить `УСПЕХ`, иначе — `ОШИБКА`.

Тест BAKE.SWU.2

1 Задать параметры p, a и b из таблицы Б.2 СТБ 34.101.45.
2 Задать слово, для которого строится точка:

$$X \leftarrow \texttt{193C9DC1 0290D0BC 49AEC10A 5B1A1DE7 A13A73CA 54EA17A3}$$
$$\texttt{DDA50D61 C3E1A880 19733179 14AED80A A69A51A3 4C26F415}_{16}.$$

3 Испытуемой реализацией выполнить построение точки эллиптической кривой и сохранить результат в W.
4 Если

$$\langle W \rangle_{768} = \texttt{687CF50D A1F5D80F 5F3558B2 B4A62B3B 97C30820 E8D84B71}$$
$$\texttt{FA9A2134 D2F4ABF2 F81E29DB FA7C124B 622172EE DD080C39}$$
$$\texttt{5F89EC7C 34C4F5B9 9F61E9DD 9C05719C 89F1B612 BDACBE5A}$$
$$\texttt{8D1F1D52 1D1684D6 DE206959 5DA09254 E0BC00FB 7B787B32}_{16},$$

то возвратить `УСПЕХ`, иначе — `ОШИБКА`.

Тест BAKE.SWU.3

1 Задать параметры p, a и b из таблицы Б.3 СТБ 34.101.45.
2 Задать слово, для которого строится точка:

$$X \leftarrow \texttt{2C83E719 FD2F2CB9 80E39503 8CCDB67A 5BDCEF1F 642EB7F9}$$
$$\texttt{037C8B9A 657BE01A E995CAE7 E6121CFE 7099BE62 C9DD6534}$$
$$\texttt{EE86E7E2 92DBF610 52B36FCA 685D6462}_{16}.$$

3 Испытуемой реализацией выполнить построение точки эллиптической кривой и сохранить результат в W.
4 Если

$$\langle W \rangle_{1024} = \texttt{7B169214 439062CD F80CDF47 D3EF49C7 BA7CFD53 0E15DD3F}$$
$$\texttt{664D58CF 8907A491 DC5FB1F6 F8EE169E EE14E41C 92A46AE4}$$
$$\texttt{1754FE1A A81FA815 9B0A9D41 E31A49AE 5D87B5E0 673F6171}$$
$$\texttt{7D19D668 48E598BF D1C11F58 C53549E6 9CE730E1 EDA50909}$$
$$\texttt{06439BBD 8256A478 88D147BB DED79629 5BE28D15 98DF62AF}$$
$$\texttt{99320745 6FA4F44F}_{16},$$

то возвратить `УСПЕХ`, иначе — `ОШИБКА`.

6.2.4 Протокол BMQV

При тестировании реализации протокола BMQV выполняются тесты BAKE.MQV.1 – BAKE.MQV.12.

Входными данными тестов являются параметры p, a, b, q и G, которые описывают группу точек эллиптической кривой и определяют уровень стойкости l, приветственные сообщения $\texttt{hello}_A$, $\texttt{hello}_B$, личные ключи d_A, d_B, сертификаты $\texttt{Cert}(Id_A, Q_A)$, $\texttt{Cert}(Id_B, Q_B)$, одноразовые личные ключи u_A, u_B.

В тестах для хранения сообщений протокола используются слова $\mathrm{M1}, \mathrm{M2}, \mathrm{M3} \in \{0,1\}^{8*}$, а для хранения общего ключа — слово $K_0 \in \{0,1\}^{256}$. При этом в сообщения не включаются приветственные сообщения и сертификаты сторон, так как они могут передаваться предварительно или неявно (см. п. 5.6 и п. 5.8 СТБ 34.101.66).

Тест BAKE.MQW.1

1 Задать параметры p, a, b, q, G из таблицы Б.1 СТБ 34.101.45.
2 Задать личные ключи d_A, d_B и сертификаты $\mathtt{Cert}(Id_A, Q_A)$, $\mathtt{Cert}(Id_B, Q_B)$ из таблицы 1.
3 Задать пустые приветственные сообщения $\mathtt{hello}_A$, $\mathtt{hello}_B$.
4 Задать одноразовые личные ключи:

$$u_A \leftarrow \mathtt{0A4E8298\ BE0839E4\ 6F19409F\ 637F4415\ 572251DD\ 0D39284F\ 0F0390D9\ 3BBCE9EC}_{16},$$

$$u_B \leftarrow \mathtt{0F51D913\ 47617C20\ BD4AB07A\ EF4F26A1\ AD1362A8\ F9A3D42F\ BE1B8E6F\ 1C88AAD5}_{16}.$$

5 Испытуемой реализацией по протоколу BMQV с явным подтверждением ключа для сторон A и B сформировать общий ключ K_0.
6 Если выполнены условия:
– при выполнении протокола ни одна из сторон не возвращает признак ОШИБКА,
– при выполнении протокола стороны обмениваются сообщениями

$$\mathrm{M1} = \mathtt{9B4EA669\ DABDF100\ A7D4B6E6\ EB76EE52\ 51912531\ F426750A\ AC8A9DBB\ 51C54D8D\ 6AB7DBF1\ 5FCBD768\ EE68A173\ F7B236EF\ C15A01E2\ AA6CD1FE\ 98B947DA\ 7B38A2A0}_{16},$$

$$\mathrm{M2} = \mathtt{1D5A382B\ 962D4ED0\ 6193258C\ A6DE535D\ 8FD7FACB\ 853171E9\ 32EF93B5\ EE800120\ 03DBB7B5\ BD070363\ 80BAFA47\ FCA7E6CA\ 3F179EDD\ D1AE5086\ 64790918\ 3628EDDC\ 413B7E18\ 1BAFB337}_{16},$$

$$\mathrm{M3} = \mathtt{B800A203\ 3AC7591B}_{16},$$

– по завершению протокола обе стороны сформировали общий ключ

$$K_0 = \mathtt{C6F86D0E\ 468D5EF1\ A9955B2E\ E0CF0581\ 050C81D1\ B4772709\ 2408E863\ C7EEB48C}_{16},$$

то возвратить УСПЕХ, иначе — ОШИБКА.

Примечание — Тест соответствует проверочному примеру, заданному в СТБ 34.101.66-2014 (таблица Б.2).

Тест BAKE.MQW.2

1 Задать параметры p, a, b, q, G из таблицы Б.1 СТБ 34.101.45.
2 Задать личные ключи d_A, d_B и сертификаты $\mathtt{Cert}(Id_A, Q_A)$, $\mathtt{Cert}(Id_B, Q_B)$ из таблицы 1.

3 Задать приветственные сообщения:

$$\texttt{hello}_A = \texttt{01000000}_{16},$$

$$\texttt{hello}_B = \texttt{02000000}_{16}.$$

4 Задать одноразовые личные ключи:

$$u_A \leftarrow \texttt{03A9C892 4C62F55A E5B35AF2 6DCCFCFA AAB463E4 8240361B 9A222D58 AEA41C59}_{16},$$

$$u_B \leftarrow \texttt{74106FD8 BF661535 75B6A661 25D95D57 75299C1C B2C84B6C 71E581F3 6FD72C6E}_{16}.$$

5 Испытуемой реализацией по протоколу BMQV с явным подтверждением ключа для сторон A и B сформировать общий ключ K_0.

6 Если выполнены условия:

– при выполнении протокола ни одна из сторон не возвращает признак ОШИБКА,

– при выполнении протокола стороны обмениваются сообщениями

$$\text{M1} = \texttt{229A38DD D74F72C5 99DC545E 6924B8B4 1A82582D DA68E122 F73EFB12 4F7E2A08 34DD90B4 7088A17E C41D1D6F 1833F2D7 9EFA46E0 4A2ADAC3 44B37292 E07DF1D7}_{16},$$

$$\text{M2} = \texttt{4E942D95 A585712D 80D1BE0C 6F373475 B2E66EE9 4C61F4E8 4566296A B3BF86CE 7DC74E29 0C4FB272 F6652F3D B4D500B8 457924C3 CD9B528B D6F59F03 D5DED537 36C3AAA6 B89104D9}_{16},$$

$$\text{M3} = \texttt{13A60B90 0787F545}_{16},$$

– по завершению протокола обе стороны сформировали общий ключ

$$K_0 = \texttt{67EFDF3C B438BCAB E5A6CE9C B070E7B3 8FCA4262 5D12A617 5E94E56C D98E4964}_{16},$$

то возвратить УСПЕХ, иначе — ОШИБКА.

Тест BAKE.MQW.3

1 Задать параметры p, a, b, q, G из таблицы Б.1 СТБ 34.101.45.

2 Задать личные ключи d_A, d_B и сертификаты $\texttt{Cert}(Id_A, Q_A)$, $\texttt{Cert}(Id_B, Q_B)$ из таблицы 1.

3 Задать пустые приветственные сообщения $\texttt{hello}_A$, $\texttt{hello}_B$.

4 Для $i = 1, 2, \ldots, 10000$ выполнить:

1) псевдослучайным методом сгенерировать одноразовые личные ключи u_A, u_B;

2) испытуемой реализацией по протоколу BMQV для стороны A и эталонной реализацией по протоколу BMQV для стороны B сформировать общий ключ K_0;

3) если при выполнении протокола одна из сторон возвращает признак ОШИБКА или общий ключ K_0 у сторон не совпадает, то вернуть ОШИБКА.

5 Возвратить УСПЕХ.

Примечание — Тест выполняется для всех возможных вариантов явного подтверждения ключа: без явного подтверждения обеими сторонами, с явным подтверждением только стороной A, с явным подтверждением только стороной B, с явным подтверждением обеими сторонами. Если испытуемая реализация не поддерживает некоторые из вариантов явного подтверждения ключа, то тест для них не выполняется, при этом в протоколе тестирования делается соответствующее примечание.

Тест BAKE.MQW.4

1 Задать параметры p, a, b, q, G из таблицы Б.1 СТБ 34.101.45.
2 Задать личные ключи d_A, d_B и сертификаты $\texttt{Cert}(Id_A, Q_A)$, $\texttt{Cert}(Id_B, Q_B)$ из таблицы 1.
3 Задать пустые приветственные сообщения $\texttt{hello}_A$, $\texttt{hello}_B$.
4 Для $i = 1, 2, \ldots, 10000$ выполнить:
1) псевдослучайным методом сгенерировать одноразовые личные ключи u_A, u_B;
2) эталонной реализацией по протоколу BMQV для стороны A и испытуемой реализацией по протоколу BMQV для стороны B сформировать общий ключ K_0;
3) если при выполнении протокола одна из сторон возвращает признак ОШИБКА или общий ключ K_0 у сторон не совпадает, то возвратить ОШИБКА.
5 Возвратить УСПЕХ.

Примечание — Тест выполняется для всех возможных вариантов явного подтверждения ключа: без явного подтверждения обеими сторонами, с явным подтверждением только стороной A, с явным подтверждением только стороной B, с явным подтверждением обеими сторонами. Если испытуемая реализация не поддерживает некоторые из вариантов явного подтверждения ключа, то тест для них не выполняется, при этом в протоколе тестирования делается соответствующее примечание.

Тест BAKE.MQW.5

1 Задать параметры p, a, b, q, G из таблицы Б.2 СТБ 34.101.45.
2 Задать личные ключи d_A, d_B и сертификаты $\texttt{Cert}(Id_A, Q_A)$, $\texttt{Cert}(Id_B, Q_B)$ из таблицы 2.
3 Задать пустые приветственные сообщения $\texttt{hello}_A$, $\texttt{hello}_B$.
4 Задать одноразовые личные ключи:

$$u_A \leftarrow \texttt{CEDE358D F0C77FC0 65235DDF F9AA1B81 CECE89D9 ECBFF573}$$
$$\texttt{323A7BDE DB9E0EBE 61F342A9 229DF1E1 72DA68C5 76360070}_{16},$$

$$u_B \leftarrow \texttt{93FC994C 1622E478 4B211FD9 460746F9 888FDB48 6D6CD8DC}$$
$$\texttt{F1F199BD 25A359FB 03CD9C93 54C613BD 39167391 D17AE5C3}_{16}.$$

5 Испытуемой реализацией по протоколу BMQV с явным подтверждением ключа для сторон A и B сформировать общий ключ K_0.
6 Если выполнены условия:
– при выполнении протокола ни одна из сторон не возвращает признак ОШИБКА,

– при выполнении протокола стороны обмениваются сообщениями

$$\mathrm{M1} = \texttt{63BD03C3 D17C40EC CCB6200C 0741B45A 99778430 7A0478F4}$$
$$\texttt{8E7B77EF 3F669548 B1914D87 D9B967F1 13117DC4 193E61DB}$$
$$\texttt{829A50FE C94816A8 1FF6D129 48939957 3CD88053 2452F278}$$
$$\texttt{4AC00B34 0411C537 E7C68BF9 992882FE F30DD7E4 68239606}_{16},$$

$$\mathrm{M2} = \texttt{A024EB19 4684C698 F6D15FE7 A21F4E0D 78CF3DD5 D70508E2}$$
$$\texttt{9C13580D 7FD9AA87 1B63D597 2666DF07 055FA69F 49E56A20}$$
$$\texttt{385B2301 B512D7D5 1A0FF2FE AF071413 713941A9 83B6B73A}$$
$$\texttt{9619BE5C FA422A4F 43AFF4B6 F4EA4C0B A8E7C327 11504129}$$
$$\texttt{CF5CB42C 5A3D0045}_{16},$$

$$\mathrm{M3} = \texttt{89D23730 6949A4AF}_{16},$$

– по завершению протокола обе стороны сформировали общий ключ

$$K_0 = \texttt{B3DEC2C2 A4227AF7 FAC14C53 A11CA533 0698DC5C 502A7464}$$
$$\texttt{431D265B C3DA77E8}_{16},$$

то возвратить `УСПЕХ`, иначе — `ОШИБКА`.

Примечание — Тест соответствует проверочному примеру, заданному в СТБ 34.101.66-2014 (таблица Б.2).

Тест BAKE.MQW.6

1 Задать параметры p, a, b, q, G из таблицы Б.2 СТБ 34.101.45.

2 Задать личные ключи d_A, d_B и сертификаты $\texttt{Cert}(Id_A, Q_A)$, $\texttt{Cert}(Id_B, Q_B)$ из таблицы 2.

3 Задать приветственные сообщения:

$$\texttt{hello}_A = \texttt{01000000}_{16},$$

$$\texttt{hello}_B = \texttt{02000000}_{16}.$$

4 Задать одноразовые личные ключи:

$$u_A \leftarrow \texttt{E5A8A315 D5FC929B C85D86CD 51382970 C67CCDEC 2F1ECFE7}$$
$$\texttt{2DB0D3A9 8EE70328 87EA9CFA E93EE1EB 5150C894 843D146D}_{16},$$

$$u_B \leftarrow \texttt{D20C31AF 7B69378D 263B8B8A 01FAEB87 7FDD1FE7 697797D2}$$
$$\texttt{BBF3ED15 D057D951 EBBE8AB8 48B3E582 A2FDEE9C AEE02D87}_{16}.$$

5 Испытуемой реализацией по протоколу BMQV с явным подтверждением ключа для сторон A и B сформировать общий ключ K_0.

6 Если выполнены условия:

– при выполнении протокола ни одна из сторон не возвращает признак `ОШИБКА`,

– при выполнении протокола стороны обмениваются сообщениями

$$\mathrm{M1} = \texttt{F8587AA7 68573C54 3A3ED20C 3EF3E05F B5B6D32F A0D7235E}$$
$$\texttt{9E3EE176 CE481065 38D8F776 C0207A7A EDD1E3E1 68BF8812}$$
$$\texttt{874014CC 4DCA2A5F 1BCE8975 8A21E60C 790A604E CF0BF80E}$$
$$\texttt{02974953 913F204B BDC67A11 C54CA68A 18D42861 9F656DB3}_{16},$$

$$M2 = \texttt{2DFE06DC 0CE53ADD 1E9ABD87 26E8B9E2 3DEEF4EE B52A9DA4 DC168603 0801AC69 5AC4B24D A0299605 4663FA0E FF59BEBE 15F7ED48 89F5BA84 E175B7E6 59FC6A5D 8BE724AC F48FA1E4 02CD7C4B 07904343 24E7E2A4 2A5229D0 C70A6F30 804319CA A0DB12F2 15221635}_{16},$$

$$M3 = \texttt{3AD2F00C 10890981}_{16},$$

– по завершению протокола обе стороны сформировали общий ключ

$$K_0 = \texttt{86751557 91D2B9E3 378A4BAD 59B7EB94 C500774D 2DD260A8 7EF9D90F 7909BBF3}_{16},$$

то возвратить `УСПЕХ`, иначе — `ОШИБКА`.

Тест BAKE.MQW.7

1 Задать параметры p, a, b, q, G из таблицы Б.2 СТБ 34.101.45.
2 Задать личные ключи d_A, d_B и сертификаты $\texttt{Cert}(Id_A, Q_A)$, $\texttt{Cert}(Id_B, Q_B)$ из таблицы 2.
3 Задать пустые приветственные сообщения $\texttt{hello}_A$, $\texttt{hello}_B$.
4 Для $i = 1, 2, \ldots, 10000$ выполнить:
1) псевдослучайным методом сгенерировать одноразовые личные ключи u_A, u_B;
2) испытуемой реализацией по протоколу BMQV для стороны A и эталонной реализацией по протоколу BMQV для стороны B сформировать общий ключ K_0;
3) если при выполнении протокола одна из сторон возвращает признак `ОШИБКА` или общий ключ K_0 у сторон не совпадает, то вернуть `ОШИБКА`.
5 Возвратить `УСПЕХ`.

Примечание — Тест выполняется для всех возможных вариантов явного подтверждения ключа: без явного подтверждения обеими сторонами, с явным подтверждением только стороной A, с явным подтверждением только стороной B, с явным подтверждением обеими сторонами. Если испытуемая реализация не поддерживает некоторые из вариантов явного подтверждения ключа, то тест для них не выполняется, при этом в протоколе тестирования делается соответствующее примечание.

Тест BAKE.MQW.8

1 Задать параметры p, a, b, q, G из таблицы Б.2 СТБ 34.101.45.
2 Задать личные ключи d_A, d_B и сертификаты $\texttt{Cert}(Id_A, Q_A)$, $\texttt{Cert}(Id_B, Q_B)$ из таблицы 2.
3 Задать пустые приветственные сообщения $\texttt{hello}_A$, $\texttt{hello}_B$.
4 Для $i = 1, 2, \ldots, 10000$ выполнить:
1) псевдослучайным методом сгенерировать одноразовые личные ключи u_A, u_B;
2) эталонной реализацией по протоколу BMQV для стороны A и испытуемой реализацией по протоколу BMQV для стороны B сформировать общий ключ K_0;
3) если при выполнении протокола одна из сторон возвращает признак `ОШИБКА` или общий ключ K_0 у сторон не совпадает, то возвратить `ОШИБКА`.
5 Возвратить `УСПЕХ`.

Примечание — Тест выполняется для всех возможных вариантов явного подтверждения ключа: без явного подтверждения обеими сторонами, с явным подтверждением только стороной A, с явным подтверждением только стороной B, с явным подтверждением обеими сторонами. Если испытуемая реализация не поддерживает некоторые из вариантов явного подтверждения ключа, то тест для них не выполняется, при этом в протоколе тестирования делается соответствующее примечание.

Тест BAKE.MQW.9

1 Задать параметры p, a, b, q, G из таблицы Б.3 СТБ 34.101.45.

2 Задать личные ключи d_A, d_B и сертификаты $\mathtt{Cert}(Id_A, Q_A)$, $\mathtt{Cert}(Id_B, Q_B)$ из таблицы 3.

3 Задать пустые приветственные сообщения $\mathtt{hello}_A$, $\mathtt{hello}_B$.

4 Задать одноразовые личные ключи:

$$u_A \leftarrow \mathtt{F5EEE439\ 1975B857\ A7B32632\ 739E177B\ D4B0EF10\ E88CF83A\ 39757B6D\ 5589AB94\ CBECDEBE\ 55D80F29\ 4B873426\ 603DCC4D\ 3789FB71\ 18981A90\ 7296E352\ B1704B6C}_{16},$$

$$u_B \leftarrow \mathtt{1D3B400C\ A3C39E7B\ 5E592AAB\ F224C1FD\ DFAEA9F9\ 5CF1844A\ 2A31B095\ 027E4987\ 70E70190\ A97B1CC0\ 63F396A6\ F2A0BDA1\ F0CCED0C\ AF5BD4BE\ 219C1E88\ 31AA3E50}_{16}.$$

5 Испытуемой реализацией по протоколу BMQV с явным подтверждением ключа для сторон A и B сформировать общий ключ K_0.

6 Если выполнены условия:

– при выполнении протокола ни одна из сторон не возвращает признак ОШИБКА,

– при выполнении протокола стороны обмениваются сообщениями

$$\mathrm{M1} = \mathtt{E11D940E\ ECCD1911\ 695D0FAB\ 55FB533C\ 664BC69F\ B9078F2B\ 8BC2DB9C\ 179E8FA7\ CC9ACDBC\ 930D3132\ 67E2E123\ 419253C5\ FDC85C9F\ B75275E8\ 5DCFDC09\ 5964DF6E\ 40617E27\ 706E3FED\ D98F3301\ 7C3E0DDC\ 4A85A294\ 2B8C27C8\ 811D9D72\ F6FA76CF\ 21346672\ CC8E4E76\ DB11F216\ A4D68BBE\ 43844611\ E81BEE1A\ 15193508\ A7B4B8C6}_{16},$$

$$\mathrm{M2} = \mathtt{36DA3750\ 61BBA041\ 56313251\ 60D6734D\ DAAE6300\ 2E8D8C8E\ 196436D4\ 1B6EDF22\ 2C865757\ FCEDD9EE\ 7F84E39E\ 9D77A9C8\ 69FB5379\ B0326257\ EF079780\ 1F53BCEF\ E3D0615A\ 082638F0\ 55EF2CD1\ AE9D172D\ 5F8520ED\ 52EFDB8A\ 602D13CC\ 04F33882\ 9652AB82\ 908694AB\ E1CCDFCA\ C3CFE5D8\ 95B53176\ 666887B6\ ADB62C75\ CA4EFF42\ 43949C4B\ 768906F4}_{16},$$

$$\mathrm{M3} = \mathtt{BD71BC34\ 39F57A26}_{16},$$

– по завершению протокола обе стороны сформировали общий ключ

$$K_0 = \mathtt{CEEB4010\ 317F302F\ DA4D19BD\ 5E5D1B75\ D36EA080\ 9F2F2607\ 71B0BEE3\ 1F84641A}_{16},$$

то возвратить УСПЕХ, иначе — ОШИБКА.

Примечание — Тест соответствует проверочному примеру, заданному в СТБ 34.101.66-2014 (таблица Б.2).

Тест BAKE.MQW.10

1 Задать параметры p, a, b, q, G из таблицы Б.3 СТБ 34.101.45.

2 Задать личные ключи d_A, d_B и сертификаты $\mathtt{Cert}(Id_A, Q_A)$, $\mathtt{Cert}(Id_B, Q_B)$ из таблицы 3.

3 Задать приветственные сообщения:

$$\mathtt{hello}_A = \mathtt{01000000}_{16},$$

$$\mathtt{hello}_B = \mathtt{02000000}_{16}.$$

4 Задать одноразовые личные ключи:

$$u_A \leftarrow \mathtt{B445E147\ A6CFB36B\ 20BBFC60\ CE47DDC8\ 384EA56F\ 63CB05FD\ B6201CD6\ FC4ADAA9\ C02B61AB\ A5EC0FBC\ EA27C0A9\ C4ABB182\ B76CD73D\ D54D3E60\ 10361659\ 17AF5AF9}_{16},$$

$$u_B \leftarrow \mathtt{E5895561\ 53013331\ FACF526C\ CF4C4ED8\ 22325841\ CA78A226\ 8DF64622\ 57607E36\ F35917EA\ 75245A93\ 4208795D\ 83991372\ CBDDE699\ 96727E0A\ BBFDB33F\ 1C600537}_{16}.$$

5 Испытуемой реализацией по протоколу BMQV с явным подтверждением ключа для сторон A и B сформировать общий ключ K_0.

6 Если выполнены условия:

– при выполнении протокола ни одна из сторон не возвращает признак ОШИБКА,

– при выполнении протокола стороны обмениваются сообщениями

$$\mathrm{M1} = \mathtt{47A10918\ EF4B8378\ BCE3B0B0\ 182109C4\ 733947B2\ 8C91CAF5\ 1C44EADD\ 1A480AE7\ 5349F5F2\ 9569D215\ 22FAF5C2\ 4A92B3C6\ 3894D871\ 73FDA5C2\ 7F84193C\ AAD32CB0\ 38A7E0C7\ B2285A08\ FD54D7B6\ FADDDBE6\ 0F486483\ 83698580\ 417FD78F\ 10BF4D12\ 592A9427\ 09C9E2D3\ 0C70CED2\ 3B3F9D87\ 4607F103\ 0EC784F4\ 24EA3073\ 671D05F5}_{16},$$

$$\mathrm{M2} = \mathtt{CDE0837B\ 29B8F654\ C43BA8C3\ 2FD0F54F\ 85309663\ 7C35C533\ B891FEBD\ 909AB838\ EC6AAC55\ 1F042812\ 4BD330AC\ B52DA28B\ A590F4DC\ 1F45FDDC\ 7DA9B38D\ 7795D0F1\ 6F49C883\ 5CE85DAC\ D693B8C2\ 07B80066\ 8E20D805\ 36719AE3\ 98AD3AED\ 32B1FEDF\ CB605E2D\ C85815DF\ C52A94BC\ E66B3DAE\ 257555A8\ FD6B5271\ 83E0C064\ C2A1EF34\ B8F3A0C2\ F4EBB6D0}_{16},$$

$$\mathrm{M3} = \mathtt{A637885C\ 00AF7713}_{16},$$

– по завершению протокола обе стороны сформировали общий ключ

$$K_0 = \mathtt{31972DA7\ 1DEF23AD\ 37766963\ A329DB54\ DE2368A7\ 0E3B43F2\ B1BB7332\ 224323FD}_{16},$$

то возвратить УСПЕХ, иначе — ОШИБКА.

Тест BAKE.MQW.11

1 Задать параметры p, a, b, q, G из таблицы Б.3 СТБ 34.101.45.
2 Задать личные ключи d_A, d_B и сертификаты $\texttt{Cert}(Id_A, Q_A)$, $\texttt{Cert}(Id_B, Q_B)$ из таблицы 3.
3 Задать пустые приветственные сообщения $\texttt{hello}_A$, $\texttt{hello}_B$.
4 Для $i = 1, 2, \ldots, 10000$ выполнить:
1) псевдослучайным методом сгенерировать одноразовые личные ключи u_A, u_B;
2) испытуемой реализацией по протоколу BMQV для стороны A и эталонной реализацией по протоколу BMQV для стороны B сформировать общий ключ K_0;
3) если при выполнении протокола одна из сторон возвращает признак ОШИБКА или общий ключ K_0 у сторон не совпадает, то вернуть ОШИБКА.
5 Возвратить УСПЕХ.

Примечание — Тест выполняется для всех возможных вариантов явного подтверждения ключа: без явного подтверждения обеими сторонами, с явным подтверждением только стороной A, с явным подтверждением только стороной B, с явным подтверждением обеими сторонами. Если испытуемая реализация не поддерживает некоторые из вариантов явного подтверждения ключа, то тест для них не выполняется, при этом в протоколе тестирования делается соответствующее примечание.

Тест BAKE.MQW.12

1 Задать параметры p, a, b, q, G из таблицы Б.3 СТБ 34.101.45.
2 Задать личные ключи d_A, d_B и сертификаты $\texttt{Cert}(Id_A, Q_A)$, $\texttt{Cert}(Id_B, Q_B)$ из таблицы 3.
3 Задать пустые приветственные сообщения $\texttt{hello}_A$, $\texttt{hello}_B$.
4 Для $i = 1, 2, \ldots, 10000$ выполнить:
1) псевдослучайным методом сгенерировать одноразовые личные ключи u_A, u_B;
2) эталонной реализацией по протоколу BMQV для стороны A и испытуемой реализацией по протоколу BMQV для стороны B сформировать общий ключ K_0;
3) если при выполнении протокола одна из сторон возвращает признак ОШИБКА или общий ключ K_0 у сторон не совпадает, то возвратить ОШИБКА.
5 Возвратить УСПЕХ.

Примечание — Тест выполняется для всех возможных вариантов явного подтверждения ключа: без явного подтверждения обеими сторонами, с явным подтверждением только стороной A, с явным подтверждением только стороной B, с явным подтверждением обеими сторонами. Если испытуемая реализация не поддерживает некоторые из вариантов явного подтверждения ключа, то тест для них не выполняется, при этом в протоколе тестирования делается соответствующее примечание.

6.2.5 Протокол BSTS

При тестировании реализации протокола BSTS выполняются тесты BAKE.STS.1 – BAKE.STS.12.

Входными данными тестов являются параметры p, a, b, q и G, которые описывают группу точек эллиптической кривой и определяют уровень стойкости l, привет-

ственные сообщения $\texttt{hello}_A$, $\texttt{hello}_B$, личные ключи d_A, d_B, сертификаты $\texttt{Cert}(Id_A, Q_A)$, $\texttt{Cert}(Id_B, Q_B)$, одноразовые личные ключи u_A, u_B.

В тестах для хранения сообщений протокола используются слова $\mathrm{M1}, \mathrm{M2}, \mathrm{M3} \in \{0,1\}^{8*}$, а для хранения общего ключа — слово $K_0 \in \{0,1\}^{256}$. При этом в сообщения не включаются приветственные сообщения и сертификаты сторон, так как они могут передаваться предварительно или неявно (см. п. 5.6 и п. 5.8 СТБ 34.101.66).

Тест BAKE.STS.1

1 Задать параметры p, a, b, q, G из таблицы Б.1 СТБ 34.101.45.

2 Задать личные ключи d_A, d_B и сертификаты $\texttt{Cert}(Id_A, Q_A)$, $\texttt{Cert}(Id_B, Q_B)$ из таблицы 1.

3 Задать пустые приветственные сообщения $\texttt{hello}_A$, $\texttt{hello}_B$.

4 Задать одноразовые личные ключи:

$$u_A \leftarrow \texttt{0A4E8298 BE0839E4 6F19409F 637F4415 572251DD 0D39284F 0F0390D9 3BBCE9EC}_{16},$$

$$u_B \leftarrow \texttt{0F51D913 47617C20 BD4AB07A EF4F26A1 AD1362A8 F9A3D42F BE1B8E6F 1C88AAD5}_{16}.$$

5 Испытуемой реализацией по протоколу BSTS для сторон A и B сформировать общий ключ K_0.

6 Если выполнены условия:

– при выполнении протокола ни одна из сторон не возвращает признак ОШИБКА,

– при выполнении протокола стороны обмениваются сообщениями

$$\mathrm{M1} = \texttt{9B4EA669 DABDF100 A7D4B6E6 EB76EE52 51912531 F426750A AC8A9DBB 51C54D8D 6AB7DBF1 5FCBD768 EE68A173 F7B236EF C15A01E2 AA6CD1FE 98B947DA 7B38A2A0}_{16},$$

$$\mathrm{M2} = \texttt{1D5A382B 962D4ED0 6193258C A6DE535D 8FD7FACB 853171E9 32EF93B5 EE800120 03DBB7B5 BD070363 80BAFA47 FCA7E6CA 3F179EDD D1AE5086 64790918 3628EDDC A994115F 297D2FAD 342A0AF5 4FCDA66E 1E6A30FE 966662C4 3C2A73AF A3CADF69 47344287 CB200795 61645867 8B76BA61 924AD05D 80BB81F5 3F8D5C4E 0EF55EBD AFA674D7 ECD74CB0 609DE12B C0463670 64059F01 1607DD18 62407490 1F1C5A40 94C00655 9F1306D6 82000879 87}_{16},$$

$$\mathrm{M3} = \texttt{6D45B2E7 6AF24422 ADC6D5D7 A3CFA37F DCB52F7E 440222F1 AACECB98 BDED357B BD459DF0 A3EE7A3E AFE0199C A5C4C072 7C33909E 4C322216 F6F53E38 3A3727D8 34B5D4F5 C977FC3B 7EBA6DCA 55C0F1A5 69BE3CD3 464B13C3 88D0DAC3 E6A82F9D 2EF3D6CA 7A5BAC4E B2910E}_{16},$$

– по завершению протокола обе стороны сформировали общий ключ

$$K_0 = \texttt{78EF2C56 BD6DA211 6BB5BEE8 0CEE5C05 394E7609 183CF7F7 6DF0C2DC FB25C4AD}_{16},$$

то возвратить УСПЕХ, иначе — ОШИБКА.

Примечание — Тест соответствует проверочному примеру, заданному в СТБ 34.101.66-2014 (таблица Б.3).

Тест BAKE.STS.2

1 Задать параметры p, a, b, q, G из таблицы Б.1 СТБ 34.101.45.

2 Задать личные ключи d_A, d_B и сертификаты $\mathtt{Cert}(Id_A, Q_A)$, $\mathtt{Cert}(Id_B, Q_B)$ из таблицы 1.

3 Задать приветственные сообщения:

$$\mathtt{hello}_A = \mathtt{01000000}_{16},$$

$$\mathtt{hello}_B = \mathtt{02000000}_{16}.$$

4 Задать одноразовые личные ключи:

$$u_A \leftarrow \mathtt{03A9C892\ 4C62F55A\ E5B35AF2\ 6DCCFCFA\ AAB463E4\ 8240361B\ 9A222D58\ AEA41C59}_{16},$$

$$u_B \leftarrow \mathtt{74106FD8\ BF661535\ 75B6A661\ 25D95D57\ 75299C1C\ B2C84B6C\ 71E581F3\ 6FD72C6E}_{16}.$$

5 Испытуемой реализацией по протоколу BSTS для сторон A и B сформировать общий ключ K_0.

6 Если выполнены условия:

– при выполнении протокола ни одна из сторон не возвращает признак ОШИБКА,

– при выполнении протокола стороны обмениваются сообщениями

$$\mathrm{M1} = \mathtt{229A38DD\ D74F72C5\ 99DC545E\ 6924B8B4\ 1A82582D\ DA68E122\ F73EFB12\ 4F7E2A08\ 34DD90B4\ 7088A17E\ C41D1D6F\ 1833F2D7\ 9EFA46E0\ 4A2ADAC3\ 44B37292\ E07DF1D7}_{16},$$

$$\mathrm{M2} = \mathtt{4E942D95\ A585712D\ 80D1BE0C\ 6F373475\ B2E66EE9\ 4C61F4E8\ 4566296A\ B3BF86CE\ 7DC74E29\ 0C4FB272\ F6652F3D\ B4D500B8\ 457924C3\ CD9B528B\ D6F59F03\ D5DED537\ 7DB5D0D7\ 4FB51994\ 3DEE9F7C\ D189D5CF\ C6CD6EBE\ 607CF035\ 74AA7DD2\ 4DB37903\ A2E44BA8\ 7B62BCAE\ D8730A41\ 6509BC45\ 914ADF59\ 72F8DAF7\ 477D9E64\ 71B67E14\ E1FECB85\ AD8A5348\ 3BD2521A\ 568C802B\ 8F912D80\ 47DE2719\ D31383A9\ CFACAE88\ FAA3883E\ B8A9275A\ 75B005FB\ 59}_{16},$$

$$\mathrm{M3} = \mathtt{703008D2\ EB9D7191\ 654519D8\ EE15F602\ 13FA0D7F\ B379CD91\ 93DBD39C\ FF639164\ FDF2263D\ 35A8E139\ 517A40C2\ E8AF7D7B\ 335D3C9C\ 463BBD28\ 452CF8E3\ 2A56F49E\ BBB5D87B\ DE29FE45\ 8676BFA8\ 7D79032C\ 5E6D8C46\ 38E195C5\ 93401350\ 3F1F29DA\ 90A0EC95\ 78FCF7F1\ F6EA7C}_{16},$$

– по завершению протокола обе стороны сформировали общий ключ

$$K_0 = \mathtt{AD9D9689\ 32C130D7\ 89268EA6\ D56ECA0D\ 0EA1C960\ E239F393\ EFCD35FC\ FD6A73D0}_{16},$$

то возвратить УСПЕХ, иначе — ОШИБКА.

Тест BAKE.MQW.3

1 Задать параметры p, a, b, q, G из таблицы Б.1 СТБ 34.101.45.
2 Задать личные ключи d_A, d_B и сертификаты $\texttt{Cert}(Id_A, Q_A)$, $\texttt{Cert}(Id_B, Q_B)$ из таблицы 1.
3 Задать пустые приветственные сообщения $\texttt{hello}_A$, $\texttt{hello}_B$.
4 Для $i = 1, 2, \ldots, 10000$ выполнить:
1) псевдослучайным методом сгенерировать одноразовые личные ключи u_A, u_B;
2) испытуемой реализацией по протоколу BSTS для стороны A и эталонной реализацией по протоколу BSTS для стороны B сформировать общий ключ K_0;
3) если при выполнении протокола одна из сторон возвращает признак ОШИБКА или общий ключ K_0 у сторон не совпадает, то вернуть ОШИБКА.
5 Возвратить УСПЕХ.

Тест BAKE.STS.4

1 Задать параметры p, a, b, q, G из таблицы Б.1 СТБ 34.101.45.
2 Задать личные ключи d_A, d_B и сертификаты $\texttt{Cert}(Id_A, Q_A)$, $\texttt{Cert}(Id_B, Q_B)$ из таблицы 1.
3 Задать пустые приветственные сообщения $\texttt{hello}_A$, $\texttt{hello}_B$.
4 Для $i = 1, 2, \ldots, 10000$ выполнить:
1) псевдослучайным методом сгенерировать одноразовые личные ключи u_A, u_B;
2) эталонной реализацией по протоколу BSTS для стороны A и испытуемой реализацией по протоколу BSTS для стороны B сформировать общий ключ K_0;
3) если при выполнении протокола одна из сторон возвращает признак ОШИБКА или общий ключ K_0 у сторон не совпадает, то возвратить ОШИБКА.
5 Возвратить УСПЕХ.

Тест BAKE.STS.5

1 Задать параметры p, a, b, q, G из таблицы Б.2 СТБ 34.101.45.
2 Задать личные ключи d_A, d_B и сертификаты $\texttt{Cert}(Id_A, Q_A)$, $\texttt{Cert}(Id_B, Q_B)$ из таблицы 2.
3 Задать пустые приветственные сообщения $\texttt{hello}_A$, $\texttt{hello}_B$.
4 Задать одноразовые личные ключи:

$$u_A \leftarrow \texttt{CEDE358D F0C77FC0 65235DDF F9AA1B81 CECE89D9 ECBFF573}$$
$$\texttt{323A7BDE DB9E0EBE 61F342A9 229DF1E1 72DA68C5 76360070}_{16},$$

$$u_B \leftarrow \texttt{93FC994C 1622E478 4B211FD9 460746F9 888FDB48 6D6CD8DC}$$
$$\texttt{F1F199BD 25A359FB 03CD9C93 54C613BD 39167391 D17AE5C3}_{16}.$$

5 Испытуемой реализацией по протоколу BSTS для сторон A и B сформировать общий ключ K_0.
6 Если выполнены условия:
– при выполнении протокола ни одна из сторон не возвращает признак ОШИБКА,

– при выполнении протокола стороны обмениваются сообщениями

$$\mathrm{M1} = \texttt{63BD03C3 D17C40EC CCB6200C 0741B45A 99778430 7A0478F4}$$
$$\texttt{8E7B77EF 3F669548 B1914D87 D9B967F1 13117DC4 193E61DB}$$
$$\texttt{829A50FE C94816A8 1FF6D129 48939957 3CD88053 2452F278}$$
$$\texttt{4AC00B34 0411C537 E7C68BF9 992882FE F30DD7E4 68239606}_{16},$$

$$\mathrm{M2} = \texttt{A024EB19 4684C698 F6D15FE7 A21F4E0D 78CF3DD5 D70508E2}$$
$$\texttt{9C13580D 7FD9AA87 1B63D597 2666DF07 055FA69F 49E56A20}$$
$$\texttt{385B2301 B512D7D5 1A0FF2FE AF071413 713941A9 83B6B73A}$$
$$\texttt{9619BE5C FA422A4F 43AFF4B6 F4EA4C0B A8E7C327 11504129}$$
$$\texttt{2843059C 64C03B46 A91978BE 24250E45 6C0E3F79 3621E4CE}$$
$$\texttt{A8A68163 1FF8648E 4382802D E0A5C018 EA69153C 28B1093B}$$
$$\texttt{2796390F 7AE10E0A 392E48D6 AF80F99F E7FF81B4 726BD1F6}$$
$$\texttt{CDDAA861 CF8E8969 D1AA4069 6DD4A731 5E212E7C 874B703E}$$
$$\texttt{FDBA32E3 50D97229 E5996509 86058AEB 7B9B7E2E FAF29D88}$$
$$\texttt{D1FB5C8D 220B2723 C9285BB6 4AB3CF72 B55C6F44 93DE2BDD}$$
$$\texttt{D6DC2605 EA9B3C01 66D3E45A A9}_{16},$$

$$\mathrm{M3} = \texttt{778317A9 2BE32A1F 1C8E1D73 476859DE 63C1DDD8 9EF51AF1}$$
$$\texttt{A02DF40B 6316E094 A9A93BC5 39013A13 505BA0DB B3CBD740}$$
$$\texttt{CDFA3547 8490AFFF 4031AA76 E5D3197A 50AD4877 1AC1FDB2}$$
$$\texttt{9D999014 B11085EF 4178C83F 9F03284B 877381E7 8E73F84B}$$
$$\texttt{182DCCFA FCB9932A F8DF22AA 4FAF672F B82659DE 4678AA13}$$
$$\texttt{1C0159A7 23C5931C DADD4E9E 0A075629 22A74CC0 CB7E6F42}$$
$$\texttt{13A58ECA 2ABEB5BE 498240}_{16},$$

– по завершению протокола обе стороны сформировали общий ключ

$$K_0 = \texttt{297F8724 542E636F 5974260C E1889AF3 C62C8FBA 1A6A60B2}$$
$$\texttt{E4D7A703 EBD3953B}_{16},$$

то возвратить `УСПЕХ`, иначе — `ОШИБКА`.

Примечание — Тест соответствует проверочному примеру, заданному в СТБ 34.101.66-2014 (таблица Б.3).

Тест BAKE.STS.6

1 Задать параметры p, a, b, q, G из таблицы Б.2 СТБ 34.101.45.

2 Задать личные ключи d_A, d_B и сертификаты $\texttt{Cert}(Id_A, Q_A)$, $\texttt{Cert}(Id_B, Q_B)$ из таблицы 2.

3 Задать приветственные сообщения:

$$\texttt{hello}_A = \texttt{01000000}_{16},$$

$$\texttt{hello}_B = \texttt{02000000}_{16}.$$

4 Задать одноразовые личные ключи:

$$u_A \leftarrow \texttt{E5A8A315 D5FC929B C85D86CD 51382970 C67CCDEC 2F1ECFE7}$$
$$\texttt{2DB0D3A9 8EE70328 87EA9CFA E93EE1EB 5150C894 843D146D}_{16},$$

$u_B \leftarrow$ D20C31AF 7B69378D 263B8B8A 01FAEB87 7FDD1FE7 697797D2
BBF3ED15 D057D951 EBBE8AB8 48B3E582 A2FDEE9C AEE02D87$_{16}$.

5 Испытуемой реализацией по протоколу BSTS для сторон A и B сформировать общий ключ K_0.

6 Если выполнены условия:

– при выполнении протокола ни одна из сторон не возвращает признак ОШИБКА,

– при выполнении протокола стороны обмениваются сообщениями

M1 = F8587AA7 68573C54 3A3ED20C 3EF3E05F B5B6D32F A0D7235E
9E3EE176 CE481065 38D8F776 C0207A7A EDD1E3E1 68BF8812
874014CC 4DCA2A5F 1BCE8975 8A21E60C 790A604E CF0BF80E
02974953 913F204B BDC67A11 C54CA68A 18D42861 9F656DB3$_{16}$,

M2 = 2DFE06DC 0CE53ADD 1E9ABD87 26E8B9E2 3DEEF4EE B52A9DA4
DC168603 0801AC69 5AC4B24D A0299605 4663FA0E FF59BEBE
15F7ED48 89F5BA84 E175B7E6 59FC6A5D 8BE724AC F48FA1E4
02CD7C4B 07904343 24E7E2A4 2A5229D0 C70A6F30 804319CA
F39D8226 6EA2F65F B808B8EE 035C500C DC342352 F97288EE
622BBA6F 42AEDABC D2CB3517 ECC978E1 8B7ADD57 3C914A6A
EE7B2324 F8BD11EF 1470A28B 84F2E8CC 91F9160F 0E8E9136
59DB90B3 5A555917 F17B89FD 285D9620 7724F668 09B7619C
FA88A98E 5A0E5B00 D770285A D693BBAF 219C967E C6736EDD
9E0516D6 FDA14076 5F451D48 4EBE3A7A 47314BB5 2B9D851E
7544532B B653924D 2B8BF929 DA$_{16}$,

M3 = 55DB8F47 E8E3BEBF 91D96B56 E2152451 76CCDF3D 48385A39
0A1CC2AC FC3A3510 A99B622F 1C42AA5E 321E3A27 98B12A94
56888B90 B6B27598 31E9B0B3 84385F47 7B89CFC5 86E2F7C2
35591124 ADD5E674 416507A9 A53C0AA9 55292B2F 31E90ECF
A7286FEB F607F0CA 275780C6 75368055 AF4E33F5 B63EBEBD
559F0C9A 50CD5C5A 6F312EA5 EE2E16AC 9557573A F61581CE
BDE0B766 161BB4A9 C7DB27$_{16}$,

– по завершению протокола обе стороны сформировали общий ключ

K_0 = E4585654 CD179306 BC132960 CC9845F7 740F1DB7 925F6676
3C975A0B B55CF49C$_{16}$,

то возвратить УСПЕХ, иначе — ОШИБКА.

Тест BAKE.MQW.7

1 Задать параметры p, a, b, q, G из таблицы Б.2 СТБ 34.101.45.

2 Задать личные ключи d_A, d_B и сертификаты $\mathtt{Cert}(Id_A, Q_A)$, $\mathtt{Cert}(Id_B, Q_B)$ из таблицы 2.

3 Задать пустые приветственные сообщения $\mathtt{hello}_A$, $\mathtt{hello}_B$.

4 Для $i = 1, 2, \ldots, 10000$ выполнить:

1) псевдослучайным методом сгенерировать одноразовые личные ключи u_A, u_B;

2) испытуемой реализацией по протоколу BSTS для стороны A и эталонной реализацией по протоколу BSTS для стороны B сформировать общий ключ K_0;
3) если при выполнении протокола одна из сторон возвращает признак `ОШИБКА` или общий ключ K_0 у сторон не совпадает, то вернуть `ОШИБКА`.
5 Возвратить `УСПЕХ`.

Тест BAKE.STS.8

1 Задать параметры p, a, b, q, G из таблицы Б.2 СТБ 34.101.45.
2 Задать личные ключи d_A, d_B и сертификаты $\mathtt{Cert}(Id_A, Q_A)$, $\mathtt{Cert}(Id_B, Q_B)$ из таблицы 2.
3 Задать пустые приветственные сообщения $\mathtt{hello}_A$, $\mathtt{hello}_B$.
4 Для $i = 1, 2, \ldots, 10000$ выполнить:
1) псевдослучайным методом сгенерировать одноразовые личные ключи u_A, u_B;
2) эталонной реализацией по протоколу BSTS для стороны A и испытуемой реализацией по протоколу BSTS для стороны B сформировать общий ключ K_0;
3) если при выполнении протокола одна из сторон возвращает признак `ОШИБКА` или общий ключ K_0 у сторон не совпадает, то возвратить `ОШИБКА`.
5 Возвратить `УСПЕХ`.

Тест BAKE.STS.9

1 Задать параметры p, a, b, q, G из таблицы Б.3 СТБ 34.101.45.
2 Задать личные ключи d_A, d_B и сертификаты $\mathtt{Cert}(Id_A, Q_A)$, $\mathtt{Cert}(Id_B, Q_B)$ из таблицы 3.
3 Задать пустые приветственные сообщения $\mathtt{hello}_A$, $\mathtt{hello}_B$.
4 Задать одноразовые личные ключи:

$u_A \leftarrow$ `F5EEE439 1975B857 A7B32632 739E177B D4B0EF10 E88CF83A 39757B6D 5589AB94 CBECDEBE 55D80F29 4B873426 603DCC4D 3789FB71 18981A90 7296E352 B1704B6C`$_{16}$,

$u_B \leftarrow$ `1D3B400C A3C39E7B 5E592AAB F224C1FD DFAEA9F9 5CF1844A 2A31B095 027E4987 70E70190 A97B1CC0 63F396A6 F2A0BDA1 F0CCED0C AF5BD4BE 219C1E88 31AA3E50`$_{16}$.

5 Испытуемой реализацией по протоколу BSTS для сторон A и B сформировать общий ключ K_0.
6 Если выполнены условия:
– при выполнении протокола ни одна из сторон не возвращает признак `ОШИБКА`,
– при выполнении протокола стороны обмениваются сообщениями

M1 = `E11D940E ECCD1911 695D0FAB 55FB533C 664BC69F B9078F2B 8BC2DB9C 179E8FA7 CC9ACDBC 930D3132 67E2E123 419253C5 FDC85C9F B75275E8 5DCFDC09 5964DF6E 40617E27 706E3FED D98F3301 7C3E0DDC 4A85A294 2B8C27C8 811D9D72 F6FA76CF 21346672 CC8E4E76 DB11F216 A4D68BBE 43844611 E81BEE1A 15193508 A7B4B8C6`$_{16}$,

$$M2 = \texttt{36DA3750 61BBA041 56313251 60D6734D DAAE6300 2E8D8C8E}$$
$$\texttt{196436D4 1B6EDF22 2C865757 FCEDD9EE 7F84E39E 9D77A9C8}$$
$$\texttt{69FB5379 B0326257 EF079780 1F53BCEF E3D0615A 082638F0}$$
$$\texttt{55EF2CD1 AE9D172D 5F8520ED 52EFDB8A 602D13CC 04F33882}$$
$$\texttt{9652AB82 908694AB E1CCDFCA C3CFE5D8 95B53176 666887B6}$$
$$\texttt{ADB62C75 CA4EFF42 C7763274 B15F0CDF 14378A1E 3FBA9EF9}$$
$$\texttt{F6F6AD4C C2019B64 683F6FEE D36939A5 45D2AF39 32D08743}$$
$$\texttt{516C26BD AF9CB704 3C00F21A 40EAC7E1 1D65B512 4DC4C1A9}$$
$$\texttt{9FA7B3A3 59434259 FF141FFC 280EEE7D C7C3858A FAD3447F}$$
$$\texttt{B34BE0EC 5F391954 13356807 3833284A 93C18C22 3DEDFB72}$$
$$\texttt{AE5D63B4 7F89A2EE 66AB9EF4 B40728B1 7BE00A80 FEF9111B}$$
$$\texttt{0F090A00 BCDD182C 7727E50A 036FACB9 CD419342 C2673445}$$
$$\texttt{9F7B488F 8731E7ED 32FE55C6 C8318654 27413784 C69516A5}$$
$$\texttt{8B61C5C1 E1F02086 0BC798E8 770F9A8C 6DA7805B } 81_{16},$$

$$M3 = \texttt{1235CF00 7EC1260E C93D0F9A 272EAABB 86CECEA8 4C6897C7}$$
$$\texttt{8AF28979 216F1D1A 69E3FE20 EA5FC914 B3336A2D 4DB52FBB}$$
$$\texttt{130F6407 69FE8D4D C0266D08 5DCABABB 18A2106A AB08EE1C}$$
$$\texttt{CF373624 0381DAB7 B7626611 0EB48E95 35B3EE67 4235B0A3}$$
$$\texttt{A8ADD368 2D5FA282 9C1B5E7A 67C1143C 229014C2 CE271BD7}$$
$$\texttt{F89312AE 6114332A EA4A9EEC B5ACA209 411D45F9 FA02881F}$$
$$\texttt{52B6AB81 9E632BFD 8A42D9CD 15137F3F 8C8C0FF1 8F24D8DF}$$
$$\texttt{DC70AD95 415D3AF6 73F2AB29 9D5C15CD 2391ECC4 5B8F4F0B}$$
$$\texttt{B83C0132 869545E5 F4B890}_{16},$$

– по завершению протокола обе стороны сформировали общий ключ

$$K_0 = \texttt{AAFF2826 59EEC97A BA5E65CD 0AB8E6EB AE04B076 39DF64C1}$$
$$\texttt{5EC63FE3 00EC6945}_{16},$$

то возвратить `УСПЕХ`, иначе — `ОШИБКА`.

Примечание — Тест соответствует проверочному примеру, заданному в СТБ 34.101.66-2014 (таблица Б.3).

Тест BAKE.STS.10

1 Задать параметры p, a, b, q, G из таблицы Б.3 СТБ 34.101.45.

2 Задать личные ключи d_A, d_B и сертификаты $\texttt{Cert}(Id_A, Q_A)$, $\texttt{Cert}(Id_B, Q_B)$ из таблицы 3.

3 Задать приветственные сообщения:

$$\texttt{hello}_A = \texttt{01000000}_{16},$$

$$\texttt{hello}_B = \texttt{02000000}_{16}.$$

4 Задать одноразовые личные ключи:

$$u_A \leftarrow \texttt{B445E147 A6CFB36B 20BBFC60 CE47DDC8 384EA56F 63CB05FD}$$
$$\texttt{B6201CD6 FC4ADAA9 C02B61AB A5EC0FBC EA27C0A9 C4ABB182}$$
$$\texttt{B76CD73D D54D3E60 10361659 17AF5AF9}_{16},$$

$u_B \leftarrow$ E5895561 53013331 FACF526C CF4C4ED8 22325841 CA78A226
8DF64622 57607E36 F35917EA 75245A93 4208795D 83991372
CBDDE699 96727E0A BBFDB33F 1C600537$_{16}$.

5 Испытуемой реализацией по протоколу BSTS для сторон A и B сформировать общий ключ K_0.

6 Если выполнены условия:

– при выполнении протокола ни одна из сторон не возвращает признак ОШИБКА,

– при выполнении протокола стороны обмениваются сообщениями

M1 = 47A10918 EF4B8378 BCE3B0B0 182109C4 733947B2 8C91CAF5
1C44EADD 1A480AE7 5349F5F2 9569D215 22FAF5C2 4A92B3C6
3894D871 73FDA5C2 7F84193C AAD32CB0 38A7E0C7 B2285A08
FD54D7B6 FADDDBE6 0F486483 83698580 417FD78F 10BF4D12
592A9427 09C9E2D3 0C70CED2 3B3F9D87 4607F103 0EC784F4
24EA3073 671D05F5$_{16}$,

M2 = CDE0837B 29B8F654 C43BA8C3 2FD0F54F 85309663 7C35C533
B891FEBD 909AB838 EC6AAC55 1F042812 4BD330AC B52DA28B
A590F4DC 1F45FDDC 7DA9B38D 7795D0F1 6F49C883 5CE85DAC
D693B8C2 07B80066 8E20D805 36719AE3 98AD3AED 32B1FEDF
CB605E2D C85815DF C52A94BC E66B3DAE 257555A8 FD6B5271
83E0C064 C2A1EF34 FBF55289 E44BC7F6 B70C815A BBCE6B26
0B5E9C10 CE0C2522 C8C921F8 7470427A 8DFB0A2F 70AFF85A
7C0C0933 BCB369B3 A0DAC91E 472DD6FB D1B6D86F 66429651
E8DB1641 C4147654 0B4BD9D0 5B0CFA0A B918145A 81F9D7B5
8E989B81 561DDDC6 E4CCA523 6AF8199E 88B6AE67 9D66837F
6372B1BC 3A9ABDA7 645EE35D 3A9BF810 82502C6F 3E5F9E00
A48D1A3D 68B8D134 D0B3B3B4 A93611DC 82CE189F 40E28909
1E5C5EBD 37D00805 810F8A3F 8E352B2A F4C83730 8AB83FF9
DD5B74E7 BE120B4B EE947213 9F879D09 1A98F42F 1E$_{16}$,

M3 = 478DE2BC 2515CB35 CF9B4F3E D36F7A66 8E5AC54B 1457E245
645D84D9 BD8B7C0A ED479D9B A00C373C 3E55CF2B 5EF51C76
07A0239D 8AF8837A D985CD6E 63A248E2 E3BD4C19 DC799161
CB3D1E8D 15FC7D2F B5D2C6B7 F467C58B ECD9A61F 5F31283A
0F461A1E EA7D55DB F82FD660 78469640 87B60EAF F064F6FC
295BA051 1A1CD1EC A95D9352 D61E6599 223DF634 DBFC1E5C
0F75B3A8 218E70C8 79563AD6 3FDFD392 3D61F2AC 9A58FC56
4D5D5418 CB6C50A8 4BCC5218 006B15DB 878AF1A5 198AC4D5
98BBF229 B0DCF550 21668E$_{16}$,

– по завершению протокола обе стороны сформировали общий ключ

K_0 = FF3051CC FA5C3FCA B162996A 1F048046 B792743F 75152765
D17D726F 3B96160C$_{16}$,

то возвратить УСПЕХ, иначе — ОШИБКА.

Тест BAKE.MQW.11

1 Задать параметры p, a, b, q, G из таблицы Б.3 СТБ 34.101.45.
2 Задать личные ключи d_A, d_B и сертификаты $\texttt{Cert}(Id_A, Q_A)$, $\texttt{Cert}(Id_B, Q_B)$ из таблицы 3.
3 Задать пустые приветственные сообщения $\texttt{hello}_A$, $\texttt{hello}_B$.
4 Для $i = 1, 2, \ldots, 10000$ выполнить:
1) псевдослучайным методом сгенерировать одноразовые личные ключи u_A, u_B;
2) испытуемой реализацией по протоколу BSTS для стороны A и эталонной реализацией по протоколу BSTS для стороны B сформировать общий ключ K_0;
3) если при выполнении протокола одна из сторон возвращает признак ОШИБКА или общий ключ K_0 у сторон не совпадает, то вернуть ОШИБКА.
5 Возвратить УСПЕХ.

Тест BAKE.STS.12

1 Задать параметры p, a, b, q, G из таблицы Б.3 СТБ 34.101.45.
2 Задать личные ключи d_A, d_B и сертификаты $\texttt{Cert}(Id_A, Q_A)$, $\texttt{Cert}(Id_B, Q_B)$ из таблицы 3.
3 Задать пустые приветственные сообщения $\texttt{hello}_A$, $\texttt{hello}_B$.
4 Для $i = 1, 2, \ldots, 10000$ выполнить:
1) псевдослучайным методом сгенерировать одноразовые личные ключи u_A, u_B;
2) эталонной реализацией по протоколу BSTS для стороны A и испытуемой реализацией по протоколу BSTS для стороны B сформировать общий ключ K_0;
3) если при выполнении протокола одна из сторон возвращает признак ОШИБКА или общий ключ K_0 у сторон не совпадает, то возвратить ОШИБКА.
5 Возвратить УСПЕХ.

6.2.6 Протокол BPACE

При тестировании реализации протокола BPACE выполняются тесты BAKE.PACE.1 – BAKE.PACE.12.

Входными данными тестов являются параметры p, a, b, q и G, которые описывают группу точек эллиптической кривой и определяют уровень стойкости l, приветственные сообщения $\texttt{hello}_A$, $\texttt{hello}_B$, общий пароль P, одноразовые секретные ключи R_A, R_B, одноразовые личные ключи u_A, u_B.

В тестах для хранения сообщений протокола используются слова $\mathrm{M1}, \mathrm{M2}, \mathrm{M3}, \mathrm{M4} \in \{0,1\}^{8*}$, а для хранения общего ключа — слово $K_0 \in \{0,1\}^{256}$. При этом в сообщения не включаются приветственные сообщения, так как они могут передаваться предварительно или неявно (см. п. 5.8 СТБ 34.101.66).

Тест BAKE.PACE.1

1 Задать параметры p, a, b, q, G из таблицы Б.1 СТБ 34.101.45.
2 Задать общий пароль P из таблицы 1.
3 Задать пустые приветственные сообщения $\texttt{hello}_A$, $\texttt{hello}_B$.
4 Задать одноразовые секретные ключи:

$$R_A \leftarrow \texttt{AD1362A8 F9A3D42F BE1B8E6F 1C88AAD5}_{16},$$

$$R_B \leftarrow \texttt{0F51D913 47617C20 BD4AB07A EF4F26A1}_{16}.$$

5 Задать одноразовые личные ключи:

$$u_A \leftarrow \texttt{0A4E8298 BE0839E4 6F19409F 637F4415 572251DD 0D39284F 0F0390D9 3BBCE9EC}_{16},$$

$$u_B \leftarrow \texttt{F81B29D5 71F6452F F8B2B97F 57E18A58 BC946FEE 45EAB32B 06FCAC23 A33F422B}_{16}.$$

6 Испытуемой реализацией по протоколу BPACE с явным подтверждением ключа для сторон A и B сформировать общий ключ K_0.

7 Если выполнены условия:

– при выполнении протокола ни одна из сторон не возвращает признак ОШИБКА,

– при выполнении протокола стороны обмениваются сообщениями

$$\text{M1} = \texttt{991E8169 0B4C687C 86BFD11C EBDA2421}_{16},$$

$$\text{M2} = \texttt{CE41B54D C13A28BD F74CEBD1 90881802 6B13ACBB 086FB876 18BCC2EF 20A3FA89 475654CB 367E670A 2441730B 24B8AB31 8209C81C 9640C47A 77B28E90 AB9211A1 DF21DE87 8191C314 061E347C 5125244F}_{16},$$

$$\text{M3} = \texttt{CD3D6487 DC4EEB23 45697818 6A069C71 375D75C2 DF198BAD 1E61EEA0 DBBFF737 3D1D9ED1 7A7AD460 AA420FB1 1952D580 78BC1CC9 F408F2E2 58FDE97F 22A44C6F 28FD4859 D78BA971}_{16},$$

$$\text{M4} = \texttt{5D93FD9A 7CB863AA}_{16},$$

– по завершению протокола обе стороны сформировали общий ключ

$$K_0 = \texttt{DAC4D8F4 11F9C523 D28BBAAB 32A5270E 4DFA1F0F 757EF8E0 F30AF08F BDE1E7F4}_{16},$$

то возвратить УСПЕХ, иначе — ОШИБКА.

Примечание — Тест соответствует проверочному примеру, заданному в СТБ 34.101.66-2014 (таблица Б.4).

Тест BAKE.PACE.2

1 Задать параметры p, a, b, q, G из таблицы Б.1 СТБ 34.101.45.

2 Задать общий пароль P из таблицы 1.

3 Задать приветственные сообщения:

$$\texttt{hello}_A = \texttt{01000000}_{16},$$

$$\texttt{hello}_B = \texttt{02000000}_{16}.$$

4 Задать одноразовые секретные ключи:

$$R_A \leftarrow \texttt{75299C1C B2C84B6C 71E581F3 6FD72C6E}_{16},$$

$$R_B \leftarrow \texttt{74106FD8 BF661535 75B6A661 25D95D57}_{16}.$$

5 Задать одноразовые личные ключи:

$$u_A \leftarrow \texttt{03A9C892 4C62F55A E5B35AF2 6DCCFCFA AAB463E4 8240361B 9A222D58 AEA41C59}_{16},$$

$$u_B \leftarrow \texttt{9D02EE44 6FB6A29F E5C982D4 B13AF9D3 E90861BC 4CEF27CF 306BFB0B 174A154A}_{16}.$$

6 Испытуемой реализацией по протоколу BPACE с явным подтверждением ключа для сторон A и B сформировать общий ключ K_0.

7 Если выполнены условия:

– при выполнении протокола ни одна из сторон не возвращает признак ОШИБКА,

– при выполнении протокола стороны обмениваются сообщениями

$$\text{M1} = \texttt{D514398A 577922BF BA728BA2 D87C580B}_{16},$$

$$\text{M2} = \texttt{28027092 23BD3DE6 76496A0D 1E4D5D51 715C51B2 34AC3B92 54C33C44 848EA434 67DDF988 D8EB86BC 34935F7A 93003B3A F7D2AC64 8297581A 8AB622F1 EEE67A76 7F29CF86 719C9896 93C719E3 9A8D4F63}_{16},$$

$$\text{M3} = \texttt{5133B3A4 40034303 D57545F8 51E6E32B 8CCBBF0A FD3234FD DA311248 41E18E16 10EA7F24 4C0B7887 C29D6539 39BB42D4 3661652A F28BF833 F5E67A5C 06BCBEEF D6503D9E 7A3D39B1}_{16},$$

$$\text{M4} = \texttt{243763DC 7B4EC944}_{16},$$

– по завершению протокола обе стороны сформировали общий ключ

$$K_0 = \texttt{730F15EF 37EA0C82 9A15C38B C2EAF504 0CB7124D 801CD016 DCDC0E02 67291300}_{16},$$

то возвратить УСПЕХ, иначе — ОШИБКА.

Тест BAKE.PACE.3

1 Задать параметры p, a, b, q, G из таблицы Б.1 СТБ 34.101.45.

2 Задать общий пароль P из таблицы 1.

3 Задать пустые приветственные сообщения $\texttt{hello}_A$, $\texttt{hello}_B$.

4 Для $i = 1, 2, \ldots, 10000$ выполнить:

1) псевдослучайным методом сгенерировать одноразовые секретные ключи R_A, R_B;

2) псевдослучайным методом сгенерировать одноразовые личные ключи u_A, u_B;

3) испытуемой реализацией по протоколу BPACE для стороны A и эталонной реализацией по протоколу BPACE для стороны B сформировать общий ключ K_0;

4) если при выполнении протокола одна из сторон возвращает признак ОШИБКА или общий ключ K_0 у сторон не совпадает, то вернуть ОШИБКА.

5 Возвратить УСПЕХ.

Примечание — Тест выполняется для всех возможных вариантов явного подтверждения ключа: без явного подтверждения обеими сторонами, с явным подтверждением только стороной

A, с явным подтверждением только стороной B, с явным подтверждением обеими сторонами. Если испытуемая реализация не поддерживает некоторые из вариантов явного подтверждения ключа, то тест для них не выполняется, при этом в протоколе тестирования делается соответствующее примечание.

Тест BAKE.PACE.4

1 Задать параметры p, a, b, q, G из таблицы Б.1 СТБ 34.101.45.
2 Задать общий пароль P из таблицы 1.
3 Задать пустые приветственные сообщения $\texttt{hello}_A$, $\texttt{hello}_B$.
4 Для $i = 1, 2, \ldots, 10000$ выполнить:
1) псевдослучайным методом сгенерировать одноразовые секретные ключи R_A, R_B;
2) псевдослучайным методом сгенерировать одноразовые личные ключи u_A, u_B;
3) эталонной реализацией по протоколу BPACE для стороны A и испытуемой реализацией по протоколу BPACE для стороны B сформировать общий ключ K_0;
4) если при выполнении протокола одна из сторон возвращает признак ОШИБКА или общий ключ K_0 у сторон не совпадает, то вернуть ОШИБКА.
5 Возвратить УСПЕХ.

Примечание — Тест выполняется для всех возможных вариантов явного подтверждения ключа: без явного подтверждения обеими сторонами, с явным подтверждением только стороной A, с явным подтверждением только стороной B, с явным подтверждением обеими сторонами. Если испытуемая реализация не поддерживает некоторые из вариантов явного подтверждения ключа, то тест для них не выполняется, при этом в протоколе тестирования делается соответствующее примечание.

Тест BAKE.PACE.5

1 Задать параметры p, a, b, q, G из таблицы Б.2 СТБ 34.101.45.
2 Задать общий пароль P из таблицы 2.
3 Задать пустые приветственные сообщения $\texttt{hello}_A$, $\texttt{hello}_B$.
4 Задать одноразовые секретные ключи:

$$R_A \leftarrow \texttt{F1F199BD 25A359FB 03CD9C93 54C613BD 39167391 D17AE5C3}_{16},$$

$$R_B \leftarrow \texttt{93FC994C 1622E478 4B211FD9 460746F9 888FDB48 6D6CD8DC}_{16}.$$

5 Задать одноразовые личные ключи:

$$u_A \leftarrow \texttt{CEDE358D F0C77FC0 65235DDF F9AA1B81 CECE89D9 ECBFF573 323A7BDE DB9E0EBE 61F342A9 229DF1E1 72DA68C5 76360070}_{16},$$

$$u_B \leftarrow \texttt{B2B6335D 3F5296A0 189EBBAE A5971B13 9731EBFD 91FE90DD 31EB6EE7 ABC35C42 3AF129A2 618DC2DD B83F8C1E 2DFA31C2}_{16}.$$

6 Испытуемой реализацией по протоколу BPACE с явным подтверждением ключа для сторон A и B сформировать общий ключ K_0.
7 Если выполнены условия:
– при выполнении протокола ни одна из сторон не возвращает признак ОШИБКА,
– при выполнении протокола стороны обмениваются сообщениями

$$\text{M1} = \texttt{B9F77C72 C59EFE21 4C4FBD49 BE9DB173 CD200FB6 0E5C23DB}_{16},$$

$$M2 = \texttt{D7686A09 149A7B92 9A6907E6 F8F65610 DF72498C 50A1DD1F A810E96D 72000EC3 D882EB36 E4D600C7 0D338A2B 7E2736B4 277A3249 694CCD5D A8C7A143 9EAA8C88 D3049D74 53094EC5 05E72A84 E1293DE2 E8252D80 C2F8CB37 D6EDE39E 4D4B61E9 A3716D91 D139E716 D13AF714 D3104FDD C0FCD451 B3C48A57}_{16},$$

$$M3 = \texttt{2528AAAC 5101923A F182D838 1D348B64 BF2A2CB9 956C04AC AF67FB0F 9B065D7E A695E460 388794EB B57A6CE8 80E7CEF5 CD939F3B 46C396B5 85E8BAD5 F0C53F60 07634AED 23F47741 7D5CA156 D47CBB21 98753060 11914FFD 7D296D78 168979AE 71EFD2BB 509A4C2E}_{16},$$

$$M4 = \texttt{AE26B57F AAC76D05}_{16},$$

– по завершению протокола обе стороны сформировали общий ключ

$$K_0 = \texttt{2FD96B74 3846A962 7D274E6F 80517BFF 090A076F A37E5ED7 5B0B2E5E 37C870FE}_{16},$$

то возвратить `УСПЕХ`, иначе — `ОШИБКА`.

Примечание — Тест соответствует проверочному примеру, заданному в СТБ 34.101.66-2014 (таблица Б.4).

Тест BAKE.PACE.6

1 Задать параметры p, a, b, q, G из таблицы Б.2 СТБ 34.101.45.

2 Задать общий пароль P из таблицы 2.

3 Задать приветственные сообщения:

$$\texttt{hello}_A = \texttt{01000000}_{16},$$

$$\texttt{hello}_B = \texttt{02000000}_{16}.$$

4 Задать одноразовые секретные ключи:

$$R_A \leftarrow \texttt{BBF3ED15 D057D951 EBBE8AB8 48B3E582 A2FDEE9C AEE02D87}_{16},$$

$$R_B \leftarrow \texttt{D20C31AF 7B69378D 263B8B8A 01FAEB87 7FDD1FE7 697797D2}_{16}.$$

5 Задать одноразовые личные ключи:

$$u_A \leftarrow \texttt{E5A8A315 D5FC929B C85D86CD 51382970 C67CCDEC 2F1ECFE7 2DB0D3A9 8EE70328 87EA9CFA E93EE1EB 5150C894 843D146D}_{16},$$

$$u_B \leftarrow \texttt{99AED613 5E2EBA3F 299C3184 00F95325 6B2B4B44 0A5D42C0 4EFB393B 0D448A3E 6E8037E7 6C0A3EDF F31A2B53 DA1F4C2D}_{16}.$$

6 Испытуемой реализацией по протоколу BPACE с явным подтверждением ключа для сторон A и B сформировать общий ключ K_0.

7 Если выполнены условия:

– при выполнении протокола ни одна из сторон не возвращает признак `ОШИБКА`,

– при выполнении протокола стороны обмениваются сообщениями

$$\mathrm{M1} = \texttt{26CD6375 C1CA56C4 4C5D196B 9DC07CCE 12670CEB 88F6F8B5}_{16},$$

$$\mathrm{M2} = \begin{array}{l}\texttt{2397A35F 4577EE0C 7B80A6E1 7259F5E7 1EB8E602 447A7318}\\ \texttt{B268889D 21B6789D 257B9317 1F116532 D725704E 85C554D2}\\ \texttt{20767973 206A1135 E9B179CE 2E838908 15BA5D36 21687520}\\ \texttt{479474EC B12B7739 FE64B1E0 CB4F055C 97688C54 CC860E34}\\ \texttt{4205175E 343FAA75 3843B9DE E0AA756A 139A90C3 6D6D1ACB}_{16},\end{array}$$

$$\mathrm{M3} = \begin{array}{l}\texttt{22D85EF7 6878BE79 99782C85 C745C52A 4927BA4D 88A19D63}\\ \texttt{79F2FADF E89CE542 65A3C967 1CB9D737 898FF7E9 BD837C4E}\\ \texttt{DB81FE46 3F94AEFF 4C969678 6126BB89 26DA9FCC 679E9502}\\ \texttt{DADD600F FEF7B718 6BB66932 CA9834E9 379F9F2E 2F9B21FC}\\ \texttt{97DB8837 AA28772A}_{16},\end{array}$$

$$\mathrm{M4} = \texttt{2510AD8F AC4AE78F}_{16},$$

– по завершению протокола обе стороны сформировали общий ключ

$$K_0 = \begin{array}{l}\texttt{24364DDB 1BB524FF DFE98704 0F61FB6C 32126522 888DFB12}\\ \texttt{FC95E933 FC9071A9}_{16},\end{array}$$

то возвратить `УСПЕХ`, иначе — `ОШИБКА`.

Тест BAKE.PACE.7

1 Задать параметры p, a, b, q, G из таблицы Б.2 СТБ 34.101.45.
2 Задать общий пароль P из таблицы 2.
3 Задать пустые приветственные сообщения $\texttt{hello}_A$, $\texttt{hello}_B$.
4 Для $i = 1, 2, \ldots, 10000$ выполнить:
1) псевдослучайным методом сгенерировать одноразовые секретные ключи R_A, R_B;
2) псевдослучайным методом сгенерировать одноразовые личные ключи u_A, u_B;
3) испытуемой реализацией по протоколу BPACE для стороны A и эталонной реализацией по протоколу BPACE для стороны B сформировать общий ключ K_0;
4) если при выполнении протокола одна из сторон возвращает признак `ОШИБКА` или общий ключ K_0 у сторон не совпадает, то вернуть `ОШИБКА`.
5 Возвратить `УСПЕХ`.

Примечание — Тест выполняется для всех возможных вариантов явного подтверждения ключа: без явного подтверждения обеими сторонами, с явным подтверждением только стороной A, с явным подтверждением только стороной B, с явным подтверждением обеими сторонами. Если испытуемая реализация не поддерживает некоторые из вариантов явного подтверждения ключа, то тест для них не выполняется, при этом в протоколе тестирования делается соответствующее примечание.

Тест BAKE.PACE.8

1 Задать параметры p, a, b, q, G из таблицы Б.2 СТБ 34.101.45.
2 Задать общий пароль P из таблицы 2.
3 Задать пустые приветственные сообщения $\texttt{hello}_A$, $\texttt{hello}_B$.
4 Для $i = 1, 2, \ldots, 10000$ выполнить:
1) псевдослучайным методом сгенерировать одноразовые секретные ключи R_A, R_B;
2) псевдослучайным методом сгенерировать одноразовые личные ключи u_A, u_B;
3) эталонной реализацией по протоколу BPACE для стороны A и испытуемой реализацией по протоколу BPACE для стороны B сформировать общий ключ K_0;
4) если при выполнении протокола одна из сторон возвращает признак ОШИБКА или общий ключ K_0 у сторон не совпадает, то вернуть ОШИБКА.
5 Возвратить УСПЕХ.

Примечание — Тест выполняется для всех возможных вариантов явного подтверждения ключа: без явного подтверждения обеими сторонами, с явным подтверждением только стороной A, с явным подтверждением только стороной B, с явным подтверждением обеими сторонами. Если испытуемая реализация не поддерживает некоторые из вариантов явного подтверждения ключа, то тест для них не выполняется, при этом в протоколе тестирования делается соответствующее примечание.

Тест BAKE.PACE.9

1 Задать параметры p, a, b, q, G из таблицы Б.3 СТБ 34.101.45.
2 Задать общий пароль P из таблицы 3.
3 Задать пустые приветственные сообщения $\texttt{hello}_A$, $\texttt{hello}_B$.
4 Задать одноразовые секретные ключи:

$$R_A \leftarrow \texttt{70E70190 A97B1CC0 63F396A6 F2A0BDA1 F0CCED0C AF5BD4BE 219C1E88 31AA3E50}_{16},$$

$$R_B \leftarrow \texttt{1D3B400C A3C39E7B 5E592AAB F224C1FD DFAEA9F9 5CF1844A 2A31B095 027E4987}_{16}.$$

5 Задать одноразовые личные ключи:

$$u_A \leftarrow \texttt{F5EEE439 1975B857 A7B32632 739E177B D4B0EF10 E88CF83A 39757B6D 5589AB94 CBECDEBE 55D80F29 4B873426 603DCC4D 3789FB71 18981A90 7296E352 B1704B6C}_{16},$$

$$u_B \leftarrow \texttt{D2201B1F 97E0FF04 C3BC83B2 160A1773 9E181AC2 FBAA7991 30BC0DA4 8BFB3E5E 17B3C085 D9CF95AF 0F0D8EBC B30E2CCA 46816CA3 F137E520 67CF5A89 830A23A5}_{16}.$$

6 Испытуемой реализацией по протоколу BPACE с явным подтверждением ключа для сторон A и B сформировать общий ключ K_0.
7 Если выполнены условия:
– при выполнении протокола ни одна из сторон не возвращает признак ОШИБКА,
– при выполнении протокола стороны обмениваются сообщениями

$$\text{M1} = \texttt{701FB02C A9983CE6 1B273999 6C40D013 1F6E7995 F3A5F7A7 794F4557 9D7F7E9A}_{16},$$

$$M2 = \texttt{58F85497 74A3EA9E F0AA1289 B6CEE02C 59BE2C92 14A3CE2E}$$
$$\texttt{7A85DE12 0152D8CA 1781D85C A1770AFD 1BAC2FAD DE42469F}$$
$$\texttt{144045C7 7BC83665 1CA2D708 D0391864 3934A846 3B49A38F}$$
$$\texttt{5F869165 8E1C69B2 7C5D14B4 F779F5A3 8A5E02D4 7E374EA4}$$
$$\texttt{642D6AA2 6AD292D2 DBDD2553 20486610 1D696EF0 41ED91AC}$$
$$\texttt{A085B433 C43E7566 6478BC3A 193E4514 BD4FC253 3F55C190}$$
$$\texttt{87D6B266 1B3DE321 ECEFB105 58211F2F}_{16},$$

$$M3 = \texttt{F3D47EE0 F24FB783 09222A3E 980412FB B61352ED B36D7FAC}$$
$$\texttt{0DFB1792 C088DD32 84579C43 AC6EA082 2D38F87C 34149AF4}$$
$$\texttt{F783DE8A 7752BC57 062DE1E4 38DDCEF3 22DEEDA4 45E7CC0B}$$
$$\texttt{EE243A1B 2D249F69 A6B8F4FB 2BA807D7 4C315DCE D3C03FEA}$$
$$\texttt{D2C10CD3 507994A2 3DEC5E8A 430A49E2 2E98647C A24C6981}$$
$$\texttt{B0FA481A C8D4DA08 A299ABB0 76A354C2}_{16},$$

$$M4 = \texttt{EF39BDF0 5C3B535E}_{16},$$

– по завершению протокола обе стороны сформировали общий ключ

$$K_0 = \texttt{73C5EE21 A8C0FD65 5B8CB2B8 FF645441 57325B27 CB984E06}$$
$$\texttt{EEC2CB90 3DD88146}_{16},$$

то возвратить `УСПЕХ`, иначе — `ОШИБКА`.

Примечание — Тест соответствует проверочному примеру, заданному в СТБ 34.101.66-2014 (таблица Б.4).

Тест BAKE.PACE.10

1 Задать параметры p, a, b, q, G из таблицы Б.3 СТБ 34.101.45.

2 Задать общий пароль P из таблицы 3.

3 Задать приветственные сообщения:

$$\texttt{hello}_A = \texttt{01000000}_{16},$$

$$\texttt{hello}_B = \texttt{02000000}_{16}.$$

4 Задать одноразовые секретные ключи:

$$R_A \leftarrow \texttt{F35917EA 75245A93 4208795D 83991372 CBDDE699 96727E0A}$$
$$\texttt{BBFDB33F 1C600537}_{16},$$

$$R_B \leftarrow \texttt{E5895561 53013331 FACF526C CF4C4ED8 22325841 CA78A226}$$
$$\texttt{8DF64622 57607E36}_{16}.$$

5 Задать одноразовые личные ключи:

$$u_A \leftarrow \texttt{B445E147 A6CFB36B 20BBFC60 CE47DDC8 384EA56F 63CB05FD}$$
$$\texttt{B6201CD6 FC4ADAA9 C02B61AB A5EC0FBC EA27C0A9 C4ABB182}$$
$$\texttt{B76CD73D D54D3E60 10361659 17AF5AF9}_{16},$$

$$u_B \leftarrow \texttt{8123B654 9EB775C1 BA96FA64 F865DBE7 E0234241 ED61445D}$$
$$\texttt{24CFF2D6 B38E02C3 FD9AA8C0 010E7A32 8B25BB2A 3734F7A0}$$
$$\texttt{D00065C3 CCBB5CC9 837C3F65 B53132D9}_{16}.$$

6 Испытуемой реализацией по протоколу BPACE с явным подтверждением ключа для сторон A и B сформировать общий ключ K_0.
7 Если выполнены условия:
– при выполнении протокола ни одна из сторон не возвращает признак ОШИБКА,
– при выполнении протокола стороны обмениваются сообщениями

$$\mathrm{M1} = \texttt{2F9506B1 A8CE7761 230153E4 E8BB0649 5D9D6A3A 76D59F39 5FEAD066 FF472483}_{16},$$

$$\mathrm{M2} = \texttt{FBEF4653 1A68C9CA 49F6F587 1CC8E448 4617FA26 7B29CF8E 7614B280 AF32C4A2 431E8D24 E188A193 07470584 DFA3788F 68C969A8 80B771F3 09CB0118 035A96FF 7472EFF5 6F31AB72 2D0F9326 FFB623E6 4840900F 86F04701 3A9BB0C4 DCB3DB0A 7AACA25B 766C615E F1020CEF 70E48F60 F0A42555 5A73B4C3 0A0806AB F318E639 8B83302F 392BC489 D2DA12C0 1A4043DA 704FE66F 1052D254 5CCAF368 9C28E854}_{16},$$

$$\mathrm{M3} = \texttt{1494F12B 0F33435D 6EC7D35F 07AFB827 08B0D4BC E153B1B0 435B2E20 075720CA FA830E03 8AF58319 04FE7B40 319EFAEA A587E4C4 4888CA01 8EEF5B10 E3E5E2DF DA1740CE 6CE4ECB6 772EF57C 106C845C 5D99D432 31B46E3F 26583EB7 8F8CB08A 135FFD6D 2B513AAD 0C7188DA BB4B7E24 FBBC93BC A6124BCC BE5D752B 72C46331 669854AC 3F892690}_{16},$$

$$\mathrm{M4} = \texttt{B8AAA05B 51C4B877}_{16},$$

– по завершению протокола обе стороны сформировали общий ключ

$$K_0 = \texttt{441DC9DC 7B9449A1 8B3D9768 1064BC5B B1BB8909 EFE8583D 7020E4C2 0FB63C55}_{16},$$

то возвратить УСПЕХ, иначе — ОШИБКА.

Тест BAKE.PACE.11

1 Задать параметры p, a, b, q, G из таблицы Б.3 СТБ 34.101.45.
2 Задать общий пароль P из таблицы 3.
3 Задать пустые приветственные сообщения $\texttt{hello}_A$, $\texttt{hello}_B$.
4 Для $i = 1, 2, \ldots, 10000$ выполнить:
1) псевдослучайным методом сгенерировать одноразовые секретные ключи R_A, R_B;
2) псевдослучайным методом сгенерировать одноразовые личные ключи u_A, u_B;
3) испытуемой реализацией по протоколу BPACE для стороны A и эталонной реализацией по протоколу BPACE для стороны B сформировать общий ключ K_0;
4) если при выполнении протокола одна из сторон возвращает признак ОШИБКА или общий ключ K_0 у сторон не совпадает, то вернуть ОШИБКА.
5 Возвратить УСПЕХ.

Примечание — Тест выполняется для всех возможных вариантов явного подтверждения ключа: без явного подтверждения обеими сторонами, с явным подтверждением только стороной

A, с явным подтверждением только стороной B, с явным подтверждением обеими сторонами. Если испытуемая реализация не поддерживает некоторые из вариантов явного подтверждения ключа, то тест для них не выполняется, при этом в протоколе тестирования делается соответствующее примечание.

Тест BAKE.PACE.12

1 Задать параметры p, a, b, q, G из таблицы Б.3 СТБ 34.101.45.
2 Задать общий пароль P из таблицы 3.
3 Задать пустые приветственные сообщения $\texttt{hello}_A$, $\texttt{hello}_B$.
4 Для $i = 1, 2, \ldots, 10000$ выполнить:
1) псевдослучайным методом сгенерировать одноразовые секретные ключи R_A, R_B;
2) псевдослучайным методом сгенерировать одноразовые личные ключи u_A, u_B;
3) эталонной реализацией по протоколу BPACE для стороны A и испытуемой реализацией по протоколу BPACE для стороны B сформировать общий ключ K_0;
4) если при выполнении протокола одна из сторон возвращает признак ОШИБКА или общий ключ K_0 у сторон не совпадает, то вернуть ОШИБКА.
5 Возвратить УСПЕХ.

Примечание — Тест выполняется для всех возможных вариантов явного подтверждения ключа: без явного подтверждения обеими сторонами, с явным подтверждением только стороной A, с явным подтверждением только стороной B, с явным подтверждением обеими сторонами. Если испытуемая реализация не поддерживает некоторые из вариантов явного подтверждения ключа, то тест для них не выполняется, при этом в протоколе тестирования делается соответствующее примечание.

6.2.7 Протокол Диффи-Хеллмана

При тестировании реализации протокола Диффи-Хеллмана выполняются тесты BAKE.DH.1 – BAKE.DH.6.

Входными данными тестов являются параметры p, a, b, q и G, которые описывают группу точек эллиптической кривой и определяют уровень стойкости l, одноразовые личные ключи $u_A, u_B \in \{1, 2, \ldots, q-1\}$.

В тестах для хранения одноразовых открытых ключей используются точки $V_A, V_B \in E^*_{a,b}(\mathbb{F}_p)$, а для хранения общей точки — $K \in E^*_{a,b}(\mathbb{F}_p)$.

Тест BAKE.DH.1

1 Задать параметры p, a, b, q, G из таблицы Б.1 СТБ 34.101.45.
2 Задать одноразовые личные ключи:

$u_A \leftarrow$ `0A4E8298 BE0839E4 6F19409F 637F4415 572251DD 0D39284F 0F0390D9 3BBCE9EC`$_{16}$,

$u_B \leftarrow$ `0F51D913 47617C20 BD4AB07A EF4F26A1 AD1362A8 F9A3D42F BE1B8E6F 1C88AAD5`$_{16}$.

3 Испытуемой реализацией по протоколу Диффи-Хеллмана для сторон A и B сформировать общий ключ K.
4 Если выполнены условия:
– при выполнении протокола ни одна из сторон не возвращает признак ОШИБКА,

– при выполнении протокола стороны формируются одноразовые открытые ключи

$$V_A = \texttt{1D5A382B 962D4ED0 6193258C A6DE535D 8FD7FACB 853171E9}$$
$$\texttt{32EF93B5 EE800120 03DBB7B5 BD070363 80BAFA47 FCA7E6CA}$$
$$\texttt{3F179EDD D1AE5086 64790918 3628EDDC}_{16},$$

$$V_B = \texttt{9B4EA669 DABDF100 A7D4B6E6 EB76EE52 51912531 F426750A}$$
$$\texttt{AC8A9DBB 51C54D8D 6AB7DBF1 5FCBD768 EE68A173 F7B236EF}$$
$$\texttt{C15A01E2 AA6CD1FE 98B947DA 7B38A2A0}_{16},$$

– по завершению протокола обе стороны сформировали общую точку

$$K = \texttt{C9121850 4B2F10C8 B307B3F8 5A292930 8E48F334 51D2810A}$$
$$\texttt{AD788DE8 CA4C7347 76932167 30B95FD3 C1439D6C B99A1A0B}$$
$$\texttt{2898FC56 3558C8F5 18E235B9 D7441A6E}_{16},$$

то возвратить `УСПЕХ`, иначе — `ОШИБКА`.

Тест BAKE.DH.2

1 Задать параметры p, a, b, q, G из таблицы Б.1 СТБ 34.101.45.

2 Для $i = 1, 2, \ldots, 10000$ выполнить:

1) псевдослучайным методом сгенерировать одноразовые личные ключи u_A, u_B;

2) испытуемой реализацией по протоколу Диффи-Хеллмана для стороны A и эталонной реализацией по протоколу Диффи-Хеллмана для стороны B сформировать общий ключ K;

3) если при выполнении протокола одна из сторон возвращает признак `ОШИБКА` или общая точка K у сторон не совпадает, то вернуть `ОШИБКА`.

3 Возвратить `УСПЕХ`.

Тест BAKE.DH.3

1 Задать параметры p, a, b, q, G из таблицы Б.2 СТБ 34.101.45.

2 Задать одноразовые личные ключи:

$$u_A \leftarrow \texttt{CEDE358D F0C77FC0 65235DDF F9AA1B81 CECE89D9 ECBFF573}$$
$$\texttt{323A7BDE DB9E0EBE 61F342A9 229DF1E1 72DA68C5 76360070}_{16},$$

$$u_B \leftarrow \texttt{93FC994C 1622E478 4B211FD9 460746F9 888FDB48 6D6CD8DC}$$
$$\texttt{F1F199BD 25A359FB 03CD9C93 54C613BD 39167391 D17AE5C3}_{16}.$$

3 Испытуемой реализацией по протоколу Диффи-Хеллмана для сторон A и B сформировать общий ключ K.

4 Если выполнены условия:

– при выполнении протокола ни одна из сторон не возвращает признак `ОШИБКА`,

– при выполнении протокола стороны формируются одноразовые открытые ключи

$$V_A = \texttt{A024EB19 4684C698 F6D15FE7 A21F4E0D 78CF3DD5 D70508E2}$$
$$\texttt{9C13580D 7FD9AA87 1B63D597 2666DF07 055FA69F 49E56A20}$$
$$\texttt{385B2301 B512D7D5 1A0FF2FE AF071413 713941A9 83B6B73A}$$
$$\texttt{9619BE5C FA422A4F 43AFF4B6 F4EA4C0B A8E7C327 11504129}_{16},$$

$$V_B = \begin{array}{l}\texttt{63BD03C3 D17C40EC CCB6200C 0741B45A 99778430 7A0478F4}\\ \texttt{8E7B77EF 3F669548 B1914D87 D9B967F1 13117DC4 193E61DB}\\ \texttt{829A50FE C94816A8 1FF6D129 48939957 3CD88053 2452F278}\\ \texttt{4AC00B34 0411C537 E7C68BF9 992882FE F30DD7E4 68239606}_{16},\end{array}$$

– по завершению протокола обе стороны сформировали общую точку

$$K = \begin{array}{l}\texttt{B9633FBE 5CCE1D20 4F03D11D 6C429B81 76D0285D 9957CF6E}\\ \texttt{61E7AE6A 8F40700B A8EC9468 7EEEB3FD 72DD0478 CC4D939E}\\ \texttt{4372434A 5A38F2B6 34C822A0 A0915ADF D029FE27 A24465FA}\\ \texttt{80FE609E A1057D5D 1EA0B701 188A7738 520D9850 63460AB0}_{16},\end{array}$$

то возвратить `УСПЕХ`, иначе — `ОШИБКА`.

Тест BAKE.DH.4

1 Задать параметры p, a, b, q, G из таблицы Б.2 СТБ 34.101.45.

2 Для $i = 1, 2, \ldots, 10000$ выполнить:

1) псевдослучайным методом сгенерировать одноразовые личные ключи u_A, u_B;

2) испытуемой реализацией по протоколу Диффи-Хеллмана для стороны A и эталонной реализацией по протоколу Диффи-Хеллмана для стороны B сформировать общий ключ K;

3) если при выполнении протокола одна из сторон возвращает признак `ОШИБКА` или общая точка K у сторон не совпадает, то вернуть `ОШИБКА`.

3 Возвратить `УСПЕХ`.

Тест BAKE.DH.5

1 Задать параметры p, a, b, q, G из таблицы Б.3 СТБ 34.101.45.

2 Задать одноразовые личные ключи:

$$u_A \leftarrow \begin{array}{l}\texttt{F5EEE439 1975B857 A7B32632 739E177B D4B0EF10 E88CF83A}\\ \texttt{39757B6D 5589AB94 CBECDEBE 55D80F29 4B873426 603DCC4D}\\ \texttt{3789FB71 18981A90 7296E352 B1704B6C}_{16},\end{array}$$

$$u_B \leftarrow \begin{array}{l}\texttt{1D3B400C A3C39E7B 5E592AAB F224C1FD DFAEA9F9 5CF1844A}\\ \texttt{2A31B095 027E4987 70E70190 A97B1CC0 63F396A6 F2A0BDA1}\\ \texttt{F0CCED0C AF5BD4BE 219C1E88 31AA3E50}_{16}.\end{array}$$

3 Испытуемой реализацией по протоколу Диффи-Хеллмана для сторон A и B сформировать общий ключ K.

4 Если выполнены условия:

– при выполнении протокола ни одна из сторон не возвращает признак `ОШИБКА`,

– при выполнении протокола стороны формируются одноразовые открытые ключи

$$V_A = \begin{array}{l}\texttt{36DA3750 61BBA041 56313251 60D6734D DAAE6300 2E8D8C8E}\\ \texttt{196436D4 1B6EDF22 2C865757 FCEDD9EE 7F84E39E 9D77A9C8}\\ \texttt{69FB5379 B0326257 EF079780 1F53BCEF E3D0615A 082638F0}\\ \texttt{55EF2CD1 AE9D172D 5F8520ED 52EFDB8A 602D13CC 04F33882}\\ \texttt{9652AB82 908694AB E1CCDFCA C3CFE5D8 95B53176 666887B6}\\ \texttt{ADB62C75 CA4EFF42}_{16},\end{array}$$

$V_B =$ E11D940E ECCD1911 695D0FAB 55FB533C 664BC69F B9078F2B
8BC2DB9C 179E8FA7 CC9ACDBC 930D3132 67E2E123 419253C5
FDC85C9F B75275E8 5DCFDC09 5964DF6E 40617E27 706E3FED
D98F3301 7C3E0DDC 4A85A294 2B8C27C8 811D9D72 F6FA76CF
21346672 CC8E4E76 DB11F216 A4D68BBE 43844611 E81BEE1A
15193508 A7B4B8C6$_{16}$,

– по завершению протокола обе стороны сформировали общую точку

$K =$ DDEC917D 28562390 1E042406 6D44AD99 2103A5D5 48EFC98C
B64FA5DF 0004D50C 0052BDE4 E3CB4F9E 9C7B6C28 D0EE796A
B1B52587 FDA992EC 0EBA427C 5010DEEB DF27B11D 1FD3AB53
B93E3BDE 0B62F669 0451D59F 72EE94B6 D56F741A 8675638E
FF255718 588CD8EA 27DAEEB5 BEFCEC1F C9D3F04D 9B8E0A39
957E0798 6921C9E5$_{16}$,

то возвратить `УСПЕХ`, иначе — `ОШИБКА`.

Тест BAKE.DH.6

1 Задать параметры p, a, b, q, G из таблицы Б.3 СТБ 34.101.45.
2 Для $i = 1, 2, \ldots, 10000$ выполнить:
1) псевдослучайным методом сгенерировать одноразовые личные ключи u_A, u_B;
2) испытуемой реализацией по протоколу Диффи-Хеллмана для стороны A и эталонной реализацией по протоколу Диффи-Хеллмана для стороны B сформировать общий ключ K;
3) если при выполнении протокола одна из сторон возвращает признак `ОШИБКА` или общая точка K у сторон не совпадает, то вернуть `ОШИБКА`.
3 Возвратить `УСПЕХ`.

6.3 Анализ исходных текстов

6.3.1 Корректность использования локальных переменных

Анализ корректности использования локальных переменных проводится для всех функций программы.

Под функцией понимается часть программы, которая выполняет специфические действия и описывается типом возвращаемого значения, именем функции, формальными параметрами. Выполнение функции осуществляется посредством вызова из программы или другой функции. Данному термину в языках программирования соответствуют такие понятия как «функция», «процедура», «метод» и т.п.

Для каждой локальной переменной v функции f эксперт определяет языковые конструкции f, в которых v встречается, и выполняет следующие проверки:

1 При использовании v в левой части оператора присваивания тип присваиваемого значения должен совпадать с типом v, в противном случае эксперт проверяет корректность результата, учитывая стандартные правила преобразования типов, определенные в используемом языке программирования.

2 Перед использованием значения переменной v должна быть выполнена ее инициализация.

3 Обращение на чтение/запись к переменной v должно происходить в пределах установленных для нее границ, в частности, если v является переменной составного типа, то обращение к элементам v должно происходить в пределах заданных размерностей.

4 Если v является переменной вещественного типа, то ее использование в операциях сравнения запрещено.

5 Если память для v выделяется в динамической области, то перед каждым выходом из f динамическая память должна быть освобождена. После освобождения памяти не должно быть языковых конструкций, ссылающихся на нее.

Примечание — В языках программирования, снабженных средствами «сборки мусора», освобождение динамической памяти, выделяемой для локальной переменной, может быть неявным.

6.3.2 Корректность использования глобальных переменных

Для каждой глобальной переменной v эксперт определяет языковые конструкции программы, в которых v встречается. Далее выполняются проверки 1 – 4 из п. 6.3.1 и следующие проверки:

1 Если память для v выделяется в динамической области, то перед каждым выходом из программы динамическая память должна быть освобождена. После освобождения памяти не должно быть языковых конструкций, ссылающихся на нее.

2 Если v может использоваться в многопоточном режиме работы программы, то должны быть реализованы механизмы, обеспечивающие разграничение доступа к v (механизмы синхронизации доступа к глобальной переменной), при этом данные механизмы не должны блокировать доступ к v на неограниченное время.

Примечание – В языках программирования, снабженных средствами «сборки мусора», освобождение динамической памяти, выделяемой для глобальной переменной, может быть неявным.

6.3.3 Корректность использования констант

Эксперт определяет языковые конструкции программы, в которых встречаются значения стандартных параметров эллиптической кривой p, a, b, q, $G = (0, y_G)$ (прил. Б СТБ 34.101.45). Для каждой языковой конструкции эксперт проверяет, что стандартные параметры заданы правильно.

6.3.4 Корректность программной логики функций программы

Для каждой функции программы эксперт выполняет следующие проверки:

1 Проверка допустимости переданных параметров и используемых глобальных переменных выполняется до их использования. Проверка может не выполняться, если в документации или в комментариях к функции оговорены ограничения на входные данные, при которых функция работает правильно, и эти ограничения соблюдаются для входных данных во всех вызовах функции.

2 Все заданные варианты условных переходов возможны.

3 Все адреса безусловных переходов доступны.

4 Каждый цикл завершается за конечное число шагов, т.е. завершение цикла гарантировано.

5 После выполнения операторов функции завершение функции гарантировано: достигается одна из точек выхода из функции.

6 Отсутствуют недостижимые участки кода.

7 Цепочки последовательных действий (например, открытие файла, чтение из файла, закрытие файла) корректны. Проверка выполняется, если в функции требуется выполнить некоторое действие, требующее определенной последовательности операций.

6.3.5 Корректность вызова стандартных функций

Эксперт проверяет, что в документации, комментариях исходных текстов программ или конфигурационных файлах указана информация, однозначно идентифицирующая вызываемые стандартные функции (версии компилятора, используемых стандартных библиотек и т.п.).

Для каждого вызова стандартной функции в программе эксперт проверяет:

1 Типы и значения параметров, фактически переданных в функцию, соответствуют типам и допустимым значениям параметров функции, указанным в документации на функцию (с учетом стандартных правил преобразования типов языка программирования).

2 Если в документации на функцию указано, что функция возвращает значение, то проводится анализ корректности использования возвращаемого значения, например, корректность использования в операторе присваивания, допустимость игнорирования возвращаемого значения и т.п.

3 Если в документации на функцию указано, что вызов функции может привести к возникновению исключительной ситуации или ошибки, проверяется наличие и корректность обработки исключительной ситуации.

4 Если в документации на функцию указано, что до и после вызова функции должны выполняться определенные действия, то проверяется наличие и корректность выполнения требуемых действий.

6.3.6 Корректность вызова функций программы

Эксперт проверяет, что в документации или комментариях исходных текстов программ для каждой функции программы указана информация, определяющая:

– допустимые входные параметры и возвращаемые значения функции;

– условия, при выполнении которых в ходе работы функции могут возникать исключительные ситуации (при наличии);

– действия, которые должны выполняться до и(или) после вызова функции (при наличии).

Для каждого вызова функции программы эксперт выполняет следующие проверки:

1 Типы и значения параметров, фактически переданных в функцию, соответствуют типам и допустимым значениям параметров функции (с учетом стандартных правил преобразования типов языка программирования).

2 Если функция возвращает значение, то проводится анализ корректности использования возвращаемого значения, например, корректность использования в операторе присваивания, допустимость игнорирования возвращаемого значения и т.п.

3 Если вызов функции может привести к возникновению исключительной ситуации или ошибки, проверяется наличие и корректность обработки исключительной ситуации.

4 Если до и после вызова функции должны выполняться определенные действия, то проверяется наличие и корректность выполнения требуемых действий.

5 Если функция использует глобальные переменные, то проверяется наличие инициализации данных переменных.

6.3.7 Корректность обработки исключительных ситуаций

Под исключительной ситуацией понимается ошибочная ситуация, возникающая при выполнении программы и требующая специальной обработки. Данному термину в языках программирования соответствует такие понятия как «ошибка», «исключение» и т.п.

Для анализа корректности обработки исключительных ситуаций эксперт формирует список функций, включающий стандартные функции и функции программы, вызов которых может приводить к возникновению исключительной ситуации.

Для каждого вызова функции из составленного списка эксперт проверяет:

1 После каждого вызова функции имеются проверка на случай возникновения исключительной ситуации и соответствующая обработка исключительной ситуации.

2 При проверке и обработке исключительной ситуации учтены все возможные виды исключительных ситуаций, возникновение которых возможно для вызываемой функции.

3 Исключительные ситуации обрабатываются адекватно (возвращаются верные коды ошибок и сообщения об ошибках и т.п.).

6.3.8 Корректность реализации криптографических примитивов

Криптографический примитив — это определенное в СТБ 34.101.66 вспомогательное преобразование, являющееся композиционной частью некоторого криптографического алгоритма или протокола.

В СТБ 34.101.66 определены следующие криптографические примитивы:

– арифметические и логические операции над большими числами (вычитание, сравнение, умножение, деление, умножение по модулю, возведение в степень по модулю, обращение по модулю);

– арифметические операции в группе точек эллиптической кривой (сложение, удвоение, нахождение кратной точки);

– алгоритмы `belt-hash` (п. 6.1.2, 7.2 СТБ 34.101.66), `belt-keyrep` (п. 6.1.2 СТБ 34.101.66), `belt-keywrap` (п. 6.2.2 СТБ 34.101.66), `belt-ecb` (п. 7.2 СТБ 34.101.66), `belt-ecb`$^{-1}$ (п. 7.2 СТБ 34.101.66), `belt-cfb` (п. 7.2 СТБ 34.101.66), `belt-cfb`$^{-1}$ (п. 7.2 СТБ 34.101.66), `belt-mac` (п. 7.2 СТБ 34.101.66). Проверка данных алгоритмов должна проводиться по согласованной с Органом по сертификации методике испытаний программы, реализующей криптографические алгоритмы согласно СТБ 34.101.31. Проверка может не проводиться, если реализации данных алгоритмов уже прошли испытания по указанной методике. В таких случаях эксперт может зачесть результаты испытаний реализаций алгоритмов предварительно проверив совпадение испытанных ранее реализаций с проверяемыми;

– алгоритм проверки открытого ключа (п. 7.2, прил. А СТБ 34.101.66). При реализации алгоритма, отличного от указанного в п. 6.2.3 СТБ 34.101.45, необходимо провести проверку реализации в соответствии с документацией на алгоритм. Алгоритм должен быть математически обоснован.

Анализируя структуру программы и используя документацию, эксперт формирует список криптографических примитивов, реализованных в программе. Для каждого примитива $g : A \to B$, осуществляющего отображение множества A в множество B, эксперт проверяет:

– наличие реализации примитива g в виде отдельной функции, части функции или композиции нескольких функций;

– тождественность реализации примитива g спецификации;

– отсутствие в g операций, не используемых для реализации примитива (наличие операций, не предусмотренных спецификацией на примитив, отражается в приложении к протоколу результатов анализа исходных текстов).

Допускается, что действие отображения g определено на множестве A^*, которое является подмножеством A. В этом случае эксперт дополнительно проверяет, что при выполнении программы прообразы отображения g всегда являются элементами A^*.

6.3.9 Корректность реализации криптографических алгоритмов и протоколов

В СТБ 34.101.66 определены следующие криптографические алгоритмы и протоколы:

– алгоритм построения ключа (п. 6.1 СТБ 34.101.66);

– алгоритм построения точки эллиптической кривой (п. 6.2 СТБ 34.101.66);

– протокол BMQV (п. 7.4 СТБ 34.101.66);

– протокол BSTS (п. 7.5 СТБ 34.101.66);

– протокол BPACE (п. 7.6 СТБ 34.101.66);

– протокол Диффи-Хеллмана (прил. А СТБ 34.101.66).

Примечание — Согласно СТБ 34.101.66 криптографическим протоколом является интерактивный криптографический алгоритм, который выполняют несколько сторон-участников, обмениваясь между собой сообщениями, содержащими промежуточные результаты вычислений. В связи с этим далее под криптографическим алгоритмов понимается как алгоритм, так и протокол.

Анализируя структуру программы и используя документацию, эксперт формирует список криптографических алгоритмов, реализованных в программе. Для каждого алгоритма $f : X \times \Theta \to Y$, который ставит в соответствие входным данным $x \in X$ и параметру $\theta \in \Theta$ результат криптографического преобразования $y \in Y$, эксперт проверяет наличие соответствующей реализации алгоритма. Затем эксперт определяет множества функций реализации, в которых:

1) задаются параметры $\theta \in \Theta$;
2) задаются входные данные $x \in X$;
3) реализуется отображение f;
4) возвращается результат $y \in Y$.

Данные множества функций обозначаются соответственно F_1, F_2, F_3, F_4. Множества могут пересекаться или совпадать.

Для функций из множества F_1 эксперт проверяет корректность задания параметров $\theta \in \Theta$. При этом допустимым является использование в программном компоненте множества параметров Θ^*, которое является подмножеством Θ. Однако, использованное сужение множества Θ не должно состоять в ограничении области значений секретных параметров.

Для функций из множества F_2 эксперт проверяет корректность задания входных данных $x \in X$. При этом допускается, что множество входных данных X^* алгоритма является подмножеством X. Однако, использованное сужение множества входных данных должно быть оговорено в документации.

Примечание – Программа может обрабатывать не все допустимые входные данные. Например, могут использоваться только стандартные долговременные параметры.

Для функций из множества F_3 эксперт проверяет тождественность отображения, реализуемого функциями, спецификации на алгоритм f (при возможных ограничениях на

параметры и входные данные, использованные в реализации отображения). Для этого, по результатам анализа элементов множества F_3, составляются использованные в реализации f композиции криптографических примитивов. Затем проверяется тождественность реализованных композиций композициям криптографических примитивов, заданным в спецификации и реализующим анализируемый криптографический алгоритм. Кроме этого, эксперт проводит проверку корректности реализации вспомогательных алгоритмов, использованных в программе и не описанных в спецификации. Если такой анализ провести не удается (алгоритм не описан в документации или описан не полно, без указания использованных источников), то по данному пункту проверки выдается отрицательное заключение по причине недостаточности данных. Если использованы простые вспомогательные алгоритмы, призванные оптимизировать выполнение программы и понятные эксперту, то их описание в документации не требуется.

Для функций из множества F_4 эксперт проверяет корректность выдачи результатов $y \in Y$ выполнения криптографического алгоритма. Сужение в реализации алгоритма f множества результатов Y является недопустимым.

Для протокола Диффи-Хеллмана эксперт дополнительно проверяет, что в программе реализован механизм безопасности, предназначенный для защиты протокола от злоумышленника «посередине». Могут использоваться следующие два механизма безопасности (см. прил. А СТБ 34.101.66):

1 Механизм, который состоит в контроле целостности и подлинности открытых ключей при их передаче между сторонами. К данному механизму относятся:

- передача долговременных открытых ключей протокола в виде сертификатов;
- использование долговременных ключей электронной цифровой подписи, с помощью которых стороны вырабатывают и проверяют подписи данных обмена (именно такой подход использован в протоколе BSTS, п. 7.5 СТБ 34.101.66);
- использование долговременных секретных ключей имитозащиты, с помощью которых стороны вырабатывают и проверяют имитовставки данных обмена.

2 Механизм, который состоит в использовании дополнительных секретных данных при построении общего ключа: на вход алгоритма построения ключа кроме общей секретной точки K подаются секретные ключи, предварительно распределенные или полученные в результате выполнения других протоколов.

6.3.10 Корректность управления секретными данными

Секретные данные — это ключи, параметры и другие данные криптографических алгоритмов и протоколов, значения которых в соответствии со стандартом или документацией на СКЗИ должны быть защищены от раскрытия, т.е. должны храниться в секрете.

Секретными данными СТБ 34.101.66 являются:

- личный ключ d (п. 5.4 СТБ 34.101.66);
- пароль P (п. 5.5 СТБ 34.101.66);
- одноразовый личный ключ u (п. 5.7);
- одноразовый секретный ключ R (п. 5.7 СТБ 34.101.66);
- общий ключ K_0 (п. 6.1, приложение А СТБ 34.101.66);
- одноразовые подписи s_A, s_B, вырабатываемые в протокле BMQV (п. 7.2 СТБ 34.101.66);
- общая секретная точка K (п. 7.2, прил. А СТБ 34.101.66);
- служебные ключи K_1, K_2 (п. 7.2 СТБ 34.101.66);

– переменная W (п. 7.2 СТБ 34.101.66);

– одноразовый или долговременный личный ключ u (прил. А СТБ 34.101.66).

Эксперт проверяет, что секретные данные используются в строгом соответствии с криптографическим алгоритмом. Допускается использование секретных данных во вспомогательных операциях с целью повышения быстродействия программной реализации криптоалгоритма. Другие операции с секретными данными не допускаются.

Эксперт проверяет, что все копии секретных данных в открытом виде уничтожаются при завершении работы с ними, при этом:

– значение секретных данных, размещенное в области памяти глобальной переменной, уничтожается перед каждым выходом из программы;

– значение секретных данных, размещенное в области памяти локальной переменной функции, уничтожается перед каждым выходом из данной функции;

– значение секретных данных, размещенное в динамической памяти, уничтожается перед каждым освобождением динамической памяти.

Примечание – Под уничтожением понимается такое изменение данных, хранящихся в электронных устройствах (оперативная память, память на магнитных носителях и др.), которое предотвращает их последующее восстановление. Например, уничтожение может состоять в записи в области памяти, занимаемой значениями секретных данных, фиксированных или случайно выбранных значений.

6.3.11 Отсутствие недокументированных возможностей

Эксперт определяет отсутствие недокументированных возможностей по результатам проверок, выполненных в п. 6.3.1 – 6.3.10.

Обнаруженные недокументированные возможности отражаются в протоколе анализа исходных текстов или в приложении к нему.

Приложение А
Форма протокола анализа документации

Экз. {Поле 1}

Протокол № {Поле 2} **от** {Поле 3}
результатов анализа документации
объекта испытаний {Поле 4}, реализующего криптографические алгоритмы и протоколы согласно СТБ 34.101.66-2014

1. Документы:

№	Название документа	Номер
1	{Поле 5}	{Поле 6}
2	{Поле 7}	{Поле 8}
3	{Поле 9}	{Поле 10}
4	{Поле 11}	{Поле 12}

2. При анализе документации были выполнены следующие проверки:

№	Название проверки	Отметка о выполнении
1	Проверка документа «Спецификация»	{Поле 13}
2	Проверка документа «Текст программы»	{Поле 13}
3	Проверка документа «Описание программы»	{Поле 13}
4	Проверка документа «Руководство программиста»	{Поле 13}

3. Заключение по результатам анализа документации: документация {Поле 6}, {Поле 8}, {Поле 10}, {Поле 12} соответствует (не соответствует) программе объекта испытаний в части реализации криптографических алгоритмов и протоколов согласно СТБ 34.101.66-2014.

Эксперт, {Поле 15} {Поле 16}
{Поле 14}

В поле 1 указывается номер экземпляра протокола.

В поле 2 указывается номер, однозначно идентифицирующий протокол.

В поле 3 указывается дата составления протокола.

В поле 4 указывается название объекта испытаний в соответствии с представленной к испытаниям документацией.

В полях 5 и 6 указываются соответственно полное название документа «Спецификация» и его идентификационный/децимальный номер.

В полях 7 и 8 указываются соответственно полное название документа «Текст программы» и его идентификационный/децимальный номер.

В полях 9 и 10 указываются соответственно полное название документа «Описание программы» и его идентификационный/децимальный номер.

В полях 11 и 12 указываются соответственно полное название документа «Руководство программиста» и его идентификационный/децимальный номер.

В поле 13 указывается результат выполнения проверки: «положительно» — результат проверки положительный, «отрицательно» — результат проверки отрицательный. После завершения анализа документации и заполнения таблицы делается вывод о соответствии (не соответствии) документации программе объекта испытаний в части реализации криптографических алгоритмов и протоколов согласно СТБ 34.101.66. Вывод о соответствии делается только тогда, когда результаты всех проверок являются положительными.

В полях 14 и 16 указываются соответственно должность и Ф. И. О. эксперта.

В поле 15 ставится собственноручная подпись эксперта.

Информация об обнаруженных несоответствиях приводится в протоколе или приложении к протоколу в произвольной форме.

Приложение Б
Форма протокола тестирования

Экз. {Поле 1}

Протокол № {Поле 2} **от** {Поле 3}
результатов тестирования
объекта испытаний {Поле 4}, реализующего криптографические алгоритмы и протоколы согласно СТБ 34.101.66-2014

1. Файлы исходных текстов программ:

№	Имя файла	Хэш-значение
1	{Поле 5}	{Поле 6}
2	{Поле 5}	{Поле 6}
...	...	...

Хэш-значения для файлов вычислены согласно {Поле 7}.

2. В ходе тестирования объекта испытаний были выполнены следующие тесты:

№	Название теста	Отметка о выполнении
1	BAKE.KDF.1	{Поле 8}
2	BAKE.KDF.2	{Поле 8}
3	BAKE.SWU.1	{Поле 8}
4	BAKE.SWU.2	{Поле 8}
5	BAKE.SWU.3	{Поле 8}
6	BAKE.BMQV.1	{Поле 8}
...	...	...

3. Заключение по результатам тестирования: объект испытаний {Поле 4} соответствует (не соответствует) требованиям, установленным в СТБ 34.101.66-2014.

Эксперт, {Поле 10} {Поле 11}
{Поле 9}

В поле 1 указывается номер экземпляра протокола.

В поле 2 указывается номер, однозначно идентифицирующий протокол.

В поле 3 указывается дата составления протокола.

В поле 4 указывается название объекта испытаний в соответствии с представленной к испытаниям документацией.

В поле 5 указываются имена исходных файлов программ объекта испытаний.

В поле 6 указывается значение функции хэширования для тестируемых файлов, вычисленное в соответствии со стандартом, указанным в поле 7. Разрешается использовать функции хэширования, определенные в СТБ 34.101.31 или СТБ 34.101.77.

В поле 8 указывается результат выполнения теста: «положительно» — тест завершен успешно, «отрицательно» — тест завершен с ошибкой; «не проводился» — тест не проводился, так как программа не поддерживает алгоритм или режим, определенный в тесте.

После завершения тестирования и заполнения таблицы делается вывод о соответствии (не соответствии) программной реализации объекта испытаний СТБ 34.101.66. Вывод о соответствии делается только тогда, когда все проводимые тесты выполнены успешно.

В полях 9, 11 указываются соответственно должность и Ф. И. О. эксперта.

В поле 10 ставится собственноручная подпись эксперта.

Приложение В
Форма протокола анализа исходных текстов программ

Экз. {Поле 1}

Протокол № {Поле 2} **от** {Поле 3}
результатов анализа исходных текстов программ
объекта испытаний {Поле 4}, реализующего криптографические алгоритмы и протоколы согласно СТБ 34.101.66-2014

1. Файлы исходных текстов программ:

№	Имя файла	Хэш-значение
1	{Поле 5}	{Поле 6}
2	{Поле 5}	{Поле 6}
	...	...

Хэш-значения для файлов вычислены согласно {Поле 7}.

2. В ходе анализа исходных текстов программ были выполнены следующие проверки:

№	Название проверки	Результат проверки
1	Корректность использования локальных переменных	{Поле 8}
2	Корректность использования глобальных переменных	{Поле 8}
3	Корректность использования констант	{Поле 8}
4	Корректность программной логики функций программы	{Поле 8}
5	Корректность вызова стандартных функций	{Поле 8}
6	Корректность вызова функций программы	{Поле 8}
7	Корректность обработки исключительных ситуаций	{Поле 8}
8	Корректность реализации криптографических примитивов	{Поле 8}
9	Корректность реализации криптографических алгоритмов и протоколов	{Поле 8}
10	Корректность управления секретными данными	{Поле 8}
11	Отсутствие недокументированных возможностей	{Поле 8}

3. Заключение по результатам анализа исходных текстов программ: объект испытаний {Поле 4} соответствует требованиям, установленным в СТБ 34.101.66-2014.

Эксперт, {Поле 9} {Поле 10} {Поле 11}

В поле 1 указывается номер экземпляра протокола.

В поле 2 указывается номер, однозначно идентифицирующий протокол.

В поле 3 указывается дата составления протокола.

В поле 4 указывается название объекта испытаний в соответствии с представленной к испытаниям документацией.

В поле 5 указываются имена исходных файлов программ объекта испытаний.

В поле 6 указывается значение функции хэширования для исходных файлов программ, вычисленное в соответствии со стандартом, указанным в поле 7. Разрешается использовать функции хэширования, определенные в СТБ 34.101.31 или СТБ 34.101.77.

В поле 8 указывается результат выполнения проверки: «положительно» — результат проверки положительный, «отрицательно» — результат проверки отрицательный, «не проводилась» — проверка не требуется по причине специфики реализации программ объекта испытаний (например, в программе не используются глобальные переменные). После завершения анализа исходных текстов программ и заполнения таблицы делается вывод о соответствии (не соответствии) объекта испытаний СТБ 34.101.66. Вывод о соответствии делается только тогда, когда результаты всех проводимых проверок являются положительными.

В полях 9, 11 указываются соответственно должность и Ф. И. О. эксперта.

В поле 10 ставится собственноручная подпись эксперта.

Информация об обнаруженных ошибках и недокументированных возможностях приводится в протоколе или приложении к протоколу в произвольной форме и должна включать:

1) описание ошибки или недокументированной возможности;
2) имя файла и номера строк программы, содержащих ошибку.