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 34.101.45-2013

МИ.10145.10.01

Листов 58

Минск 2022

Предисловие

Настоящая методика испытаний предназначена для использования в испытательных лабораториях при проведении сертификационных испытаний средств криптографической защиты информации на соответствие требованиям СТБ 34.101.45-2013 «Информационные технологии и безопасность. Алгоритмы электронной цифровой подписи и транспорта 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 34.101.47-2017 «Информационные технологии и безопасность. Криптографические алгоритмы генерации псевдослучайных чисел».

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 34.101.45, а также следующие сокращения:

ЕСПД единая система программной документации;

ИЭЦП идентификационная электронная цифровая подпись;

СКЗИ средство криптографической защиты информации;

ЭЦП электронная цифровая подпись.

3 Объект и цель испытаний

На испытания представляется средство криптографической защиты информации (СКЗИ), реализующее криптографические алгоритмы СТБ 34.101.45, и документация на СКЗИ.

Целью испытаний является проверка соответствия объекта испытаний требованиям СТБ 34.101.45.

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 СТБ 34.101.45, поддерживаемые объектом испытаний;

– программа, реализующая криптографические алгоритмы и требования СТБ 34.101.45, 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 34.101.45. Если программа не поддерживает некоторые алгоритмы, определенные в СТБ 34.101.45, 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 СТБ 34.101.45, которые в составе других программ имеют действующие сертификаты соответствия требованиям СТБ 34.101.45, то проверки по тестированию и анализу исходных текстов для данных реализаций могут не проводиться. При этом для подтверждения соответствия объекта испытаний требованиям СТБ 34.101.45 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 34.101.45 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 34.101.45 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 34.101.45.

Тестированию подлежат криптографические алгоритмы, реализованные в программе и определенные в СТБ 34.101.45, включая:

– алгоритмы генерации и проверки параметров эллиптической кривой (см. п. 6.2.1);
– алгоритмы генерации и проверки ключей (см. п. 6.2.2);
– алгоритм генерации одноразового личного ключа (см. п. 6.2.3);
– алгоритмы выработки и проверки электронной цифровой подписи (см. п. 6.2.4);
– алгоритмы транспорта ключа (см. п. 6.2.5);
– алгоритмы идентификационной цифровой подписи (см. п. 6.2.6);
– алгоритм построения ключа защиты по паролю (см. п. 6.2.7).

Если программа не реализует некоторые из алгоритмов, определенных в СТБ 34.101.45, 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 СТБ 34.101.45. 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 (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 34.101.45 криптографические алгоритмы, 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 34.101.45 криптографические алгоритмы;

– 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 34.101.45 криптографические алгоритмы;

– описание функций, реализующих определенные в СТБ 34.101.45 криптографические алгоритмы, 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 Алгоритмы генерации и проверки параметров эллиптической кривой

При тестировании реализации алгоритма генерации параметров эллиптической кривой выполняются тесты BIGN.GEC.1 – BIGN.GEC.3, а при тестировании реализации алгоритма проверки параметров эллиптической кривой — тесты BIGN.VEC.1 – BIGN.VEC.3.

Входными данными тестов BIGN.GEC.1 – BIGN.GEC.3 являются уровень стойкости $l \in \{128, 192, 256\}$, простой модуль p, целый коэффициент a и параметр $seed \in \{0,1\}^{64}$. Для входных данных выполняются условия: $2^{2l-1} < p < 2^{2l}$, $p \equiv 3 \pmod 4$, $0 < a < p$.

Входными данными тестов BIGN.VEC.1 – BIGN.VEC.3 являются модуль p, коэффициенты a и b, параметр $seed$, порядок q и базовая точка G. Параметры p, a, b, q являются целыми числами, $seed \in \{0,1\}^{64}$, точка G задается двумя целыми координатами.

В тестах BIGN.GEC.1 – BIGN.GEC.3 для хранения результата генерации параметров эллиптической кривой по l, p и a используются: b — для коэффициента $(0 < b < p)$, q — для порядка $(2^{2l-1} < q < 2^{2l})$, $G \in E^*_{a,b}(\mathbb{F}_p)$ — для базовой точки.

Тест BIGN.GEC.1

1 Задать уровень стойкости: $l \leftarrow 128$.

2 Задать модуль p, коэффициент a и параметр $seed$ из таблицы Б.1 СТБ 34.101.45.

3 Испытуемой реализацией выполнить генерацию параметров эллиптической кривой и сохранить результат в b, q, G.

4 Если значения b, q, $G = (0, y_G)$ совпадают со значениями, приведенными в таблицы Б.1 СТБ 34.101.45, то возвратить `УСПЕХ`, иначе — `ОШИБКА`.

Тест BIGN.GEC.2

1 Задать уровень стойкости: $l \leftarrow 192$.
2 Задать модуль p, коэффициент a и параметр *seed* из таблицы Б.2 СТБ 34.101.45.
3 Испытуемой реализацией выполнить генерацию параметров эллиптической кривой и сохранить результат в b, q, G.
4 Если значения b, q, $G = (0, y_G)$ совпадают со значениями, приведенными в таблицы Б.2 СТБ 34.101.45, то возвратить `УСПЕХ`, иначе — `ОШИБКА`.

Тест BIGN.GEC.3

1 Задать уровень стойкости: $l \leftarrow 256$.
2 Задать модуль p, коэффициент a и параметр *seed* из таблицы Б.3 СТБ 34.101.45.
3 Испытуемой реализацией выполнить генерацию параметров эллиптической кривой и сохранить результат в b, q, G.
4 Если значения b, q, $G = (0, y_G)$ совпадают со значениями, приведенными в таблицы Б.3 СТБ 34.101.45, то возвратить `УСПЕХ`, иначе — `ОШИБКА`.

Тест BIGN.VEC.1

1 Задать уровень стойкости: $l \leftarrow 128$.
2 Задать модуль p, коэффициенты a и b, параметр *seed* и базовую точку $G = (0, y_G)$ из таблицы Б.1 СТБ 34.101.45.
3 Испытуемой реализацией выполнить проверку параметров эллиптической кривой.
4 Если алгоритм проверки параметров возвратил ответ `ДА`, то возвратить `УСПЕХ`, иначе — `ОШИБКА`.

Тест BIGN.VEC.2

1 Задать уровень стойкости: $l \leftarrow 192$.
2 Задать модуль p, коэффициенты a и b, параметр *seed* и базовую точку $G = (0, y_G)$ из таблицы Б.2 СТБ 34.101.45.
3 Испытуемой реализацией выполнить проверку параметров эллиптической кривой.
4 Если алгоритм проверки параметров возвратил ответ `ДА`, то возвратить `УСПЕХ`, иначе — `ОШИБКА`.

Тест BIGN.VEC.3

1 Задать уровень стойкости: $l \leftarrow 256$.
2 Задать модуль p, коэффициенты a и b, параметр *seed* и базовую точку $G = (0, y_G)$ из таблицы Б.3 СТБ 34.101.45.
3 Испытуемой реализацией выполнить проверку параметров эллиптической кривой.
4 Если алгоритм проверки параметров возвратил ответ `ДА`, то возвратить `УСПЕХ`, иначе — `ОШИБКА`.

6.2.2 Алгоритмы генерации и проверки ключей

При тестировании реализации алгоритма генерации пары ключей выполняются тесты BIGN.GKP.1 – BIGN.GKP.3, а при тестировании реализации алгоритма проверки открытого ключа — тесты BIGN.VPK.1 – BIGN.VPK.3.

Входными данными тестов BIGN.GKP.1 – BIGN.GKP.3 являются параметры p, a, b, q, G, которые описывают группу точек эллиптической кривой, и личный ключ $d \in \{1, 2, \ldots, q-1\}$.

Входными данными тестов BIGN.VPK.1 – BIGN.VPK.3 являются параметры p, a, b, которые описывают группу точек эллиптической кривой, и открытый ключ $Q = (x_Q, y_Q)$, где x_Q, y_Q — целые числа.

В тестах BIGN.GKP.1 – BIGN.GKP.3 для хранения результата генерации открытого ключа по параметрам p, a, b, q, G и личному ключу d используется точка $Q \in E^*_{a,b}(\mathbb{F}_p)$.

Тест BIGN.GKP.1

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

2 Задать личный ключ:

$$d \leftarrow \texttt{1F66B5B8 4B733967 4533F032 9C74F218 34281FED 0732429E 0C79235F C273E269}_{16}.$$

3 Испытуемой реализацией выполнить генерацию открытого ключа и сохранить результат в $Q = (x_Q, y_Q)$.

4 Если

$$x_Q = \texttt{BD1A5650 179D79E0 3FCEE49D 4C2BD5DD F54CE46D 0CF11E4F F87BF7A8 90857FD0}_{16},$$

$$y_Q = \texttt{7AC6A603 61E8C817 3491686D 461B2826 190C2EDA 5909054A 9AB84D2A B9D99A90}_{16},$$

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

Тест BIGN.GKP.2

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

2 Задать личный ключ:

$$d \leftarrow \texttt{84C21DBF 7B3C2372 DC21386C 216FA16C 9EF10AEA F9F96A87 2FD8058F 2780BA93 0F08BE3B EC804161 37E11A23 2D93B50E}_{16}.$$

3 Испытуемой реализацией выполнить генерацию открытого ключа и сохранить результат в $Q = (x_Q, y_Q)$.

4 Если

$$x_Q = \texttt{212602EE 5589B84A 4585807A E8BFE371 8A52B675 8B05F644 05F9D371 6462B02D 334D51CF 27125637 37F63F5B 9BE7E4DA}_{16},$$

$$y_Q = \texttt{8634E65F 71905CB7 204DC5BC 1229FB68 76ED4F60 EC299D49 9AB0641A 5F82F291 517F7631 4B50A0ED 389368A5 690EC3A5}_{16},$$

то возвратить УСПЕХ, иначе — ОШИБКА.

Тест BIGN.GKP.3

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

$$d \leftarrow \texttt{BEC09635 3EF4568A A417622A 95F2B563}$$
$$\texttt{33BF3A02 040B3137 2FD5737D E0F1A2BA}$$
$$\texttt{6090C1D1 A27155D8 711FFE5B 31027847}$$
$$\texttt{1B0B97CF 1B8FE821 C50205E5 D24AB9B8}_{16}.$$

3 Испытуемой реализацией выполнить генерацию открытого ключа и сохранить результат в $Q = (x_Q, y_Q)$.
4 Если

$$x_Q = \texttt{C6255C65 515274CD 10E68B2F C13E16B2}$$
$$\texttt{2CB7AC00 D45ABE2A 2FD0CA5E 4E472895}$$
$$\texttt{43C20F62 56A5FAD3 3E862894 C15A477E}$$
$$\texttt{C4BBEE3C 139D9548 4243BA97 F200CA35}_{16},$$

$$y_Q = \texttt{048521F7 AB27D7CF 81658CD7 D36018CE}$$
$$\texttt{B8FE6446 8F1E096A 0CB5638D 11C4697B}$$
$$\texttt{B7C9A1CA EAF5F243 A6477BE8 B306F20B}$$
$$\texttt{D45E5BB5 A8986FED 554509FD 5FDC39D6}_{16},$$

то возвратить УСПЕХ, иначе — ОШИБКА.

Тест BIGN.VPK.1

1 Задать параметры p, a, b из таблицы Б.1 СТБ 34.101.45.
2 Задать открытый ключ:

$$x_Q \leftarrow \texttt{BD1A5650 179D79E0 3FCEE49D 4C2BD5DD}$$
$$\texttt{F54CE46D 0CF11E4F F87BF7A8 90857FD0}_{16},$$

$$y_Q \leftarrow \texttt{7AC6A603 61E8C817 3491686D 461B2826}$$
$$\texttt{190C2EDA 5909054A 9AB84D2A B9D99A90}_{16}.$$

3 Испытуемой реализацией выполнить проверку открытого ключа $Q = (x_Q, y_Q)$.
4 Если алгоритм проверки открытого ключа возвращает ДА, то возвратить УСПЕХ, иначе — ОШИБКА.

Тест BIGN.VPK.2

1 Задать параметры p, a, b из таблицы Б.2 СТБ 34.101.45.
2 Задать открытый ключ:

$$x_Q \leftarrow \texttt{212602EE 5589B84A 4585807A E8BFE371}$$
$$\texttt{8A52B675 8B05F644 05F9D371 6462B02D}$$
$$\texttt{334D51CF 27125637 37F63F5B 9BE7E4DA}_{16},$$

$$y_Q \leftarrow \begin{array}{l}\texttt{8634E65F 71905CB7 204DC5BC 1229FB68}\\ \texttt{76ED4F60 EC299D49 9AB0641A 5F82F291}\\ \texttt{517F7631 4B50A0ED 389368A5 690EC3A5}_{16}.\end{array}$$

3 Испытуемой реализацией выполнить проверку открытого ключа $Q = (x_Q, y_Q)$.
4 Если алгоритм проверки открытого ключа возвращает `ДА`, то возвратить `УСПЕХ`, иначе — `ОШИБКА`.

Тест BIGN.VPK.3

1 Задать параметры p, a, b из таблицы Б.3 СТБ 34.101.45.
2 Задать открытый ключ:

$$x_Q \leftarrow \begin{array}{l}\texttt{C6255C65 515274CD 10E68B2F C13E16B2}\\ \texttt{2CB7AC00 D45ABE2A 2FD0CA5E 4E472895}\\ \texttt{43C20F62 56A5FAD3 3E862894 C15A477E}\\ \texttt{C4BBEE3C 139D9548 4243BA97 F200CA35}_{16},\end{array}$$

$$y_Q \leftarrow \begin{array}{l}\texttt{048521F7 AB27D7CF 81658CD7 D36018CE}\\ \texttt{B8FE6446 8F1E096A 0CB5638D 11C4697B}\\ \texttt{B7C9A1CA EAF5F243 A6477BE8 B306F20B}\\ \texttt{D45E5BB5 A8986FED 554509FD 5FDC39D6}_{16}.\end{array}$$

3 Испытуемой реализацией выполнить проверку открытого ключа $Q = (x_Q, y_Q)$.
4 Если алгоритм проверки открытого ключа возвращает `ДА`, то возвратить `УСПЕХ`, иначе — `ОШИБКА`.

6.2.3 Алгоритм генерации одноразового личного ключа

При тестировании реализации алгоритма генерации одноразового личного ключа выполняются тесты BIGN.GEK.1 – BIGN.GEK.6.

Входными данными тестов BIGN.GEK.1 – BIGN.GEK.6 являются порядок q группы точек эллиптической кривой, где $2^{2l-1} < q < 2^{2l}$, личный ключ $d \in \{1, 2, \ldots, q-1\}$, хэш-значение $H = h(X) \in \{0,1\}^{2l}$ подписываемого сообщения X и кодовое представление идентификатора алгоритма хэширования $OID(h) \in \{0,1\}^*$. В тестах переменная t задается пустым словом.

В тестах BIGN.GEK.1 – BIGN.GEK.6 для хранения результата генерации одноразового личного ключа используется $k \in \{1, 2, \ldots, q-1\}$.

Тест BIGN.GEK.1

1 Задать параметры q из таблицы Б.1 СТБ 34.101.45.
2 Задать личный ключ:

$$d \leftarrow \begin{array}{l}\texttt{1F66B5B8 4B733967 4533F032 9C74F218}\\ \texttt{34281FED 0732429E 0C79235F C273E269}_{16}.\end{array}$$

3 Задать кодовое представление идентификатора:

$$OID(h) \leftarrow \texttt{06092A70 00020022 651F51}_{16}.$$

4 Задать хэш-значение:

$$H \leftarrow \texttt{ABEF9725 D4C5A835 97A367D1 4494CC25}\\ \texttt{42F20F65 9DDFECC9 61A3EC55 0CBA8C75}_{16}.$$

5 Испытуемой реализацией выполнить генерацию одноразового личного ключа и сохранить результат в k.

6 Если

$$k = \texttt{829614D8 411DBBC4 E1F2471A 40045864}\\ \texttt{40FD8C95 53FAB6A1 A45CE417 AE97111E}_{16},$$

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

Тест BIGN.GEK.2

1 Задать параметры q из таблицы Б.1 СТБ 34.101.45.

2 Задать личный ключ:

$$d \leftarrow \texttt{79628979 DF369BEB 94DEF329 9476AED4}\\ \texttt{14F39148 AA69E31A 7397E8AA 70578AB3}_{16}.$$

3 Задать кодовое представление идентификатора:

$$OID(h) \leftarrow \texttt{06092A70 00020022 651F51}_{16}.$$

4 Задать хэш-значение:

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

5 Испытуемой реализацией выполнить генерацию одноразового личного ключа и сохранить результат в k.

6 Если

$$k = \texttt{0BA66DA6 214E48A7 01F22695 BA9CD6D5}\\ \texttt{67DE17A1 C6010624 88728ED8 BBF48ED0}_{16},$$

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

Тест BIGN.GEK.3

1 Задать параметры q из таблицы Б.2 СТБ 34.101.45.

2 Задать личный ключ:

$$d \leftarrow \texttt{84C21DBF 7B3C2372 DC21386C 216FA16C}\\ \texttt{9EF10AEA F9F96A87 2FD8058F 2780BA93}\\ \texttt{0F08BE3B EC804161 37E11A23 2D93B50E}_{16}.$$

3 Задать кодовое представление идентификатора:

$$OID(h) \leftarrow \texttt{06092A70 00020022 654D0C}_{16}.$$

4 Задать хэш-значение:

$$H \leftarrow \begin{array}{l}\texttt{64334AF8 30D33F63 E9ACDFA1 84E32522}\\ \texttt{103FFF5C 6860110A 2CD369ED BC04387C}\\ \texttt{501D8F92 F749AE4D E15A8305 C353D64D}_{16}.\end{array}$$

5 Испытуемой реализацией выполнить генерацию одноразового личного ключа и сохранить результат в k.

6 Если

$$k = \begin{array}{l}\texttt{E48C1A79 06765348 6533401B 25D8D93D}\\ \texttt{174DE469 5DD2125C 0D2F9468 CC41387E}\\ \texttt{3C1D8D90 3E950903 2A1FEBF7 92C74D18}_{16},\end{array}$$

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

Тест BIGN.GEK.4

1 Задать параметры q из таблицы Б.2 СТБ 34.101.45.

2 Задать личный ключ:

$$d \leftarrow \begin{array}{l}\texttt{04E1315F 05B86B66 2D809209 D6104DE8}\\ \texttt{D25DB189 FBCE4BFF E6F6CBDE 84C96024}\\ \texttt{302D154E F8A7EEF0 B6FD2927 89C3272D}_{16}.\end{array}$$

3 Задать кодовое представление идентификатора:

$$OID(h) \leftarrow \texttt{06092A70 00020022 654D0C}_{16}.$$

4 Задать хэш-значение:

$$H \leftarrow \begin{array}{l}\texttt{D06EFBC1 6FD6C088 0CBFC6A4 E3D65AB1}\\ \texttt{01FA8282 6934190F AABEBFBF FEDE93B2}\\ \texttt{2B85EA72 A7FB3147 A133A5A8 FEBD8320}_{16}.\end{array}$$

5 Испытуемой реализацией выполнить генерацию одноразового личного ключа и сохранить результат в k.

6 Если

$$k = \begin{array}{l}\texttt{76BF95EA F9876FD9 8619501F 2120D8F7}\\ \texttt{8DCE2AFB C2E37353 B57B576E 24D821B2}\\ \texttt{6A078978 F6C3648A 51E67B60 DE40BCE7}_{16},\end{array}$$

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

Тест BIGN.GEK.5

1 Задать параметры q из таблицы Б.3 СТБ 34.101.45.

2 Задать личный ключ:

$$d \leftarrow \begin{array}{l}\texttt{BEC09635 3EF4568A A417622A 95F2B563}\\ \texttt{33BF3A02 040B3137 2FD5737D E0F1A2BA}\\ \texttt{6090C1D1 A27155D8 711FFE5B 31027847}\\ \texttt{1B0B97CF 1B8FE821 C50205E5 D24AB9B8}_{16}.\end{array}$$

3 Задать кодовое представление идентификатора:

$$OID(h) \leftarrow \texttt{06092A70 00020022 654D0D}_{16}.$$

4 Задать хэш-значение:

$$H \leftarrow \begin{array}{l}\texttt{2A66C87C 189C12E2 55239406 123BDEDB}\\ \texttt{F19955EA F0808B2A D705E249 220845E2}\\ \texttt{0F4786FB 6765D0B5 C48984B1 B16556EF}\\ \texttt{19EA8192 B985E423 3D9C0950 8D6339E7}_{16}.\end{array}$$

5 Испытуемой реализацией выполнить генерацию одноразового личного ключа и сохранить результат в k.

6 Если

$$k = \begin{array}{l}\texttt{B1CAB7FE 937559E2 074BD6CB A402F39D}\\ \texttt{55F94B6C B1073939 6B63AF93 88306A96}\\ \texttt{89428B71 A57CC827 6F9608E8 EBB597F3}\\ \texttt{5CC03B72 90AD2B80 A40CF7E3 642A38E8}_{16},\end{array}$$

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

Тест BIGN.GEK.6

1 Задать параметры q из таблицы Б.3 СТБ 34.101.45.

2 Задать личный ключ:

$$d \leftarrow \begin{array}{l}\texttt{A90188D4 EAA8D5B3 1FD54F3E 02E10FEB}\\ \texttt{F1577A14 642D7C88 B9951F3B 957C006C}\\ \texttt{567A20BD 7635B9FF 02C3045E DDD84553}\\ \texttt{D484DE44 9CFC054C 5A96C8CD 5CEA0E33}_{16}.\end{array}$$

3 Задать кодовое представление идентификатора:

$$OID(h) \leftarrow \texttt{06092A70 00020022 654D0D}_{16}.$$

4 Задать хэш-значение:

$$H \leftarrow \begin{array}{l}\texttt{07ABBF85 80E7E5A3 21E9B940 F667AE20}\\ \texttt{9E2952CE F557978A E743DB08 6BAB4885}\\ \texttt{B708233C 3F5541DF 8AAFC361 1482FDE4}\\ \texttt{98E58B33 79A6622D AC2664C9 C118A162}_{16}.\end{array}$$

5 Испытуемой реализацией выполнить генерацию одноразового личного ключа и сохранить результат в k.

6 Если

$$k = \begin{array}{l}\texttt{47F9F579 98B359FE 1EF1E693 D5ADF97E}\\ \texttt{208314C0 ED013235 101E6EDA 7675BABD}\\ \texttt{125F4D99 93B4A810 9B4A9832 21DF6A42}\\ \texttt{E7CCA9F4 15A45810 84B1F203 5FD80376}_{16},\end{array}$$

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

6.2.4 Алгоритмы выработки и проверки электронной цифровой подписи

При тестировании реализации алгоритмов выработки и проверки электронной цифровой подписи (ЭЦП) выполняются тесты BIGN.ECS.1 – BIGN.ECS.12.

Входными данными тестов являются параметры p, a, b, q, G, которые описывают группу точек эллиптической кривой и определяют уровень стойкости l, хэш-значение $H \in \{0,1\}^{2l}$ сообщения X, кодовое представление идентификатора алгоритма хэширования $OID(h) \in \{0,1\}^*$, личный ключ $d \in \{1,2,\ldots,q-1\}$, одноразовый личный ключ $k \in \{1,2,\ldots,q-1\}$, открытй ключ $Q = (x_Q, y_Q) \in E^*_{a,b}(\mathbb{F}_p)$ и подпись $S \in \{0,1\}^{3l}$.

В тестах для хранения результата выработки подписи используются слова $S, S' \in \{0,1\}^{3l}$.

Тест BIGN.ECS.1

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

2 Задать кодовое представление идентификатора:

$$OID(h) \leftarrow \texttt{06092A70 00020022 651F51}_{16}.$$

3 Задать личный ключ:

$$d \leftarrow \begin{array}{l}\texttt{1F66B5B8 4B733967 4533F032 9C74F218}\\ \texttt{34281FED 0732429E 0C79235F C273E269}_{16}.\end{array}$$

4 Задать хэш-значение:

$$H \leftarrow \begin{array}{l}\texttt{ABEF9725 D4C5A835 97A367D1 4494CC25}\\ \texttt{42F20F65 9DDFECC9 61A3EC55 0CBA8C75}_{16}.\end{array}$$

5 Задать одноразовый личный ключ:

$$k \leftarrow \begin{array}{l}\texttt{829614D8 411DBBC4 E1F2471A 40045864}\\ \texttt{40FD8C95 53FAB6A1 A45CE417 AE97111E}_{16}.\end{array}$$

6 Испытуемой реализацией выполнить выработку ЭЦП и сохранить результат в S.

7 Если

$$S = \begin{array}{l}\texttt{19D32B7E 01E25BAE 4A70EB6B CA42602C}\\ \texttt{CA6A1394 4451BCC5 D4C54CFD 8737619C}\\ \texttt{328B8A58 FB9C68FD 17D569F7 D06495FB}_{16},\end{array}$$

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

Тест BIGN.ECS.2

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

2 Задать кодовое представление идентификатора:

$$OID(h) \leftarrow \texttt{06092A70 00020022 651F51}_{16}.$$

3 Задать открытый ключ:

$$x_Q \leftarrow \begin{array}{l}\texttt{BD1A5650 179D79E0 3FCEE49D 4C2BD5DD}\\ \texttt{F54CE46D 0CF11E4F F87BF7A8 90857FD0}_{16},\end{array}$$

$$y_Q \leftarrow \begin{array}{l}\texttt{7AC6A603 61E8C817 3491686D 461B2826}\\ \texttt{190C2EDA 5909054A 9AB84D2A B9D99A90}_{16}.\end{array}$$

4 Задать хэш-значение:

$$H \leftarrow \begin{array}{l}\texttt{9D02EE44 6FB6A29F E5C982D4 B13AF9D3}\\ \texttt{E90861BC 4CEF27CF 306BFB0B 174A154A}_{16}.\end{array}$$

5 Задать значение ЭЦП:

$$S \leftarrow \begin{array}{l}\texttt{47A63C8B 9C936E94 B5FAB3D9 CBD78366}\\ \texttt{290F3210 E163EEC8 DB4E921E 8479D413}\\ \texttt{8F112CC2 3E6DCE65 EC5FF21D F4231C28}_{16}.\end{array}$$

6 Испытуемой реализацией выполнить проверку ЭЦП S.
7 Если алгоритм проверки ЭЦП возвратил `НЕТ`, то возвратить `ОШИБКА`.
8 Задать значение ЭЦП:

$$S \leftarrow \begin{array}{l}\texttt{46A63C8B 9C936E94 B5FAB3D9 CBD78366}\\ \texttt{290F3210 E163EEC8 DB4E921E 8479D413}\\ \texttt{8F112CC2 3E6DCE65 EC5FF21D F4231C28}_{16}.\end{array}$$

9 Испытуемой реализацией выполнить проверку ЭЦП S.
10 Если алгоритм проверки ЭЦП возвратил `НЕТ`, то возвратить `УСПЕХ`, иначе — `ОШИБКА`.

Тест BIGN.ECS.3

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

$$OID(h) \leftarrow \texttt{06092A70 00020022 651F51}_{16}.$$

3 Задать личный ключ:

$$d \leftarrow \begin{array}{l}\texttt{1F66B5B8 4B733967 4533F032 9C74F218}\\ \texttt{34281FED 0732429E 0C79235F C273E269}_{16}.\end{array}$$

4 Задать открытый ключ:

$$x_Q \leftarrow \begin{array}{l}\texttt{BD1A5650 179D79E0 3FCEE49D 4C2BD5DD}\\ \texttt{F54CE46D 0CF11E4F F87BF7A8 90857FD0}_{16},\end{array}$$

$$y_Q \leftarrow \begin{array}{l}\texttt{7AC6A603 61E8C817 3491686D 461B2826}\\ \texttt{190C2EDA 5909054A 9AB84D2A B9D99A90}_{16}.\end{array}$$

5 Для $i = 1, 2, \ldots, 10000$ выполнить:
1) псевдослучайным методом сгенерировать хэш-значение H;
2) псевдослучайным методом сгенерировать одноразовый личный ключ k;
3) испытуемой реализацией выполнить выработку ЭЦП и сохранить результат в S;
4) испытуемой реализацией выполнить проверку ЭЦП S;
5) если алгоритм проверки ЭЦП возвращает `НЕТ`, то возвратить `ОШИБКА`.
6 Возвратить `УСПЕХ`.

Тест BIGN.ECS.4

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

$$OID(h) \leftarrow \texttt{06092A70 00020022 651F51}_{16}.$$

3 Задать личный ключ:

$$d \leftarrow \begin{array}{l}\texttt{1F66B5B8 4B733967 4533F032 9C74F218}\\ \texttt{34281FED 0732429E 0C79235F C273E269}_{16}.\end{array}$$

4 Для $i = 1, 2, \ldots, 10000$ выполнить:
1) псевдослучайным методом сгенерировать хэш-значение H;
2) псевдослучайным методом сгенерировать одноразовый личный ключ k;
3) испытуемой реализацией выполнить выработку ЭЦП и сохранить результат в S;
4) эталонной реализацией выполнить выработку ЭЦП и сохранить результат в S';
5) если $S \neq S'$, то возвратить `ОШИБКА`.
5 Возвратить `УСПЕХ`.

Тест BIGN.ECS.5

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

$$OID(h) \leftarrow \texttt{06092A70 00020022 654D0C}_{16}.$$

3 Задать личный ключ:

$$d \leftarrow \begin{array}{l}\texttt{84C21DBF 7B3C2372 DC21386C 216FA16C}\\ \texttt{9EF10AEA F9F96A87 2FD8058F 2780BA93}\\ \texttt{0F08BE3B EC804161 37E11A23 2D93B50E}_{16}.\end{array}$$

4 Задать хэш-значение:

$$H \leftarrow \begin{array}{l}\texttt{64334AF8 30D33F63 E9ACDFA1 84E32522}\\ \texttt{103FFF5C 6860110A 2CD369ED BC04387C}\\ \texttt{501D8F92 F749AE4D E15A8305 C353D64D}_{16}.\end{array}$$

5 Задать одноразовый личный ключ:

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

6 Испытуемой реализацией выполнить выработку ЭЦП и сохранить результат в S.
7 Если

$$S = \begin{array}{l}\texttt{A7FC9D62 B6859EBB 0A98AAE3 6BE47969}\\ \texttt{C362B666 95750DDD 2CA17532 1826D4BC}\\ \texttt{8F78EBF5 55A87121 3FEC6B50 A63D30C5}\\ \texttt{89733B0A 56F6C0C2 BC03A353 2969CDF0}\\ \texttt{11DC28D4 844E79EC}_{16},\end{array}$$

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

Тест BIGN.ECS.6

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

$$OID(h) \leftarrow \texttt{06092A70 00020022 654D0C}_{16}.$$

3 Задать открытый ключ:

$$x_Q \leftarrow \begin{array}{l}\texttt{212602EE 5589B84A 4585807A E8BFE371}\\ \texttt{8A52B675 8B05F644 05F9D371 6462B02D}\\ \texttt{334D51CF 27125637 37F63F5B 9BE7E4DA}_{16},\end{array}$$

$$y_Q \leftarrow \begin{array}{l}\texttt{8634E65F 71905CB7 204DC5BC 1229FB68}\\ \texttt{76ED4F60 EC299D49 9AB0641A 5F82F291}\\ \texttt{517F7631 4B50A0ED 389368A5 690EC3A5}_{16}.\end{array}$$

4 Задать хэш-значение:

$$H \leftarrow \begin{array}{l}\texttt{D06EFBC1 6FD6C088 0CBFC6A4 E3D65AB1}\\ \texttt{01FA8282 6934190F AABEBFBF FEDE93B2}\\ \texttt{2B85EA72 A7FB3147 A133A5A8 FEBD8320}_{16}.\end{array}$$

5 Задать значение ЭЦП:

$$S \leftarrow \begin{array}{l}\texttt{51D11ABB 6392D904 0685C4CC 3A87553B}\\ \texttt{AF474481 198602FC F180DD0E 0F0076B7}\\ \texttt{5A9B8752 69560930 80DA21AC FE73A70E}\\ \texttt{EF4E5CEA E8C07CDB A526CFA3 F6C50DFD}\\ \texttt{4E8E8817 C1AE624B}_{16}.\end{array}$$

6 Испытуемой реализацией выполнить проверку ЭЦП S.
7 Если алгоритм проверки ЭЦП возвратил `НЕТ`, то возвратить `ОШИБКА`.
8 Задать значение ЭЦП:

$$S \leftarrow \begin{array}{l}\texttt{50D11ABB 6392D904 0685C4CC 3A87553B}\\ \texttt{AF474481 198602FC F180DD0E 0F0076B7}\\ \texttt{5A9B8752 69560930 80DA21AC FE73A70E}\\ \texttt{EF4E5CEA E8C07CDB A526CFA3 F6C50DFD}\\ \texttt{4E8E8817 C1AE624B}_{16}.\end{array}$$

9 Испытуемой реализацией выполнить проверку ЭЦП S.
10 Если алгоритм проверки ЭЦП возвратил `НЕТ`, то возвратить `УСПЕХ`, иначе — `ОШИБКА`.

Тест BIGN.ECS.7

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

$$OID(h) \leftarrow \texttt{06092A70 00020022 654D0C}_{16}.$$

3 Задать личный ключ:

$$d \leftarrow \begin{array}{l}\texttt{84C21DBF 7B3C2372 DC21386C 216FA16C}\\ \texttt{9EF10AEA F9F96A87 2FD8058F 2780BA93}\\ \texttt{0F08BE3B EC804161 37E11A23 2D93B50E}_{16}.\end{array}$$

4 Задать открытый ключ:

$$x_Q \leftarrow \begin{array}{l}\texttt{212602EE 5589B84A 4585807A E8BFE371}\\ \texttt{8A52B675 8B05F644 05F9D371 6462B02D}\\ \texttt{334D51CF 27125637 37F63F5B 9BE7E4DA}_{16},\end{array}$$

$$y_Q \leftarrow \begin{array}{l}\texttt{8634E65F 71905CB7 204DC5BC 1229FB68}\\ \texttt{76ED4F60 EC299D49 9AB0641A 5F82F291}\\ \texttt{517F7631 4B50A0ED 389368A5 690EC3A5}_{16}.\end{array}$$

5 Для $i = 1, 2, \ldots, 10000$ выполнить:
1) псевдослучайным методом сгенерировать хэш-значение H;
2) псевдослучайным методом сгенерировать одноразовый личный ключ k;
3) испытуемой реализацией выполнить выработку ЭЦП и сохранить результат в S;
4) испытуемой реализацией выполнить проверку ЭЦП S;
5) если алгоритм проверки ЭЦП возвращает `НЕТ`, то возвратить `ОШИБКА`.

6 Возвратить `УСПЕХ`.

Тест BIGN.ECS.8

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

$$OID(h) \leftarrow \texttt{06092A70 00020022 654D0C}_{16}.$$

3 Задать личный ключ:

$$d \leftarrow \begin{array}{l}\texttt{84C21DBF 7B3C2372 DC21386C 216FA16C}\\ \texttt{9EF10AEA F9F96A87 2FD8058F 2780BA93}\\ \texttt{0F08BE3B EC804161 37E11A23 2D93B50E}_{16}.\end{array}$$

4 Для $i = 1, 2, \ldots, 10000$ выполнить:
1) псевдослучайным методом сгенерировать хэш-значение H;
2) псевдослучайным методом сгенерировать одноразовый личный ключ k;
3) испытуемой реализацией выполнить выработку ЭЦП и сохранить результат в S;
4) эталонной реализацией выполнить выработку ЭЦП и сохранить результат в S';
5) если $S \neq S'$, то возвратить `ОШИБКА`.

5 Возвратить `УСПЕХ`.

Тест BIGN.ECS.9

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

2 Задать кодовое представление идентификатора:

$$OID(h) \leftarrow \texttt{06092A70 00020022 654D0D}_{16}.$$

3 Задать личный ключ:

$$d \leftarrow \begin{array}{l}\texttt{BEC09635 3EF4568A A417622A 95F2B563}\\ \texttt{33BF3A02 040B3137 2FD5737D E0F1A2BA}\\ \texttt{6090C1D1 A27155D8 711FFE5B 31027847}\\ \texttt{1B0B97CF 1B8FE821 C50205E5 D24AB9B8}_{16}.\end{array}$$

4 Задать хэш-значение:

$$H \leftarrow \begin{array}{l}\texttt{2A66C87C 189C12E2 55239406 123BDEDB}\\ \texttt{F19955EA F0808B2A D705E249 220845E2}\\ \texttt{0F4786FB 6765D0B5 C48984B1 B16556EF}\\ \texttt{19EA8192 B985E423 3D9C0950 8D6339E7}_{16}.\end{array}$$

5 Задать одноразовый личный ключ:

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

6 Испытуемой реализацией выполнить выработку ЭЦП и сохранить результат в S.

7 Если

$$S = \begin{array}{l}\texttt{F922D701 48C55AD5 47EB0A19 30E52CC5}\\ \texttt{52D928DC 76E4030C 9EE57DE8 DED1B5F9}\\ \texttt{5D4E33F4 7CD361DA CB1F26B2 0132E45D}\\ \texttt{4988FB86 AF1B5465 8FE2FE97 116177F5}\\ \texttt{D3117CE0 632DDFAA 8EDE10DA 7DF835D2}\\ \texttt{725E2B83 4CA96C8C 061BC831 DFA5B316}_{16},\end{array}$$

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

Тест BIGN.ECS.10

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

2 Задать кодовое представление идентификатора:

$$OID(h) \leftarrow \texttt{06092A70 00020022 654D0D}_{16}.$$

3 Задать открытый ключ:

$$x_Q \leftarrow \begin{array}{l}\texttt{C6255C65 515274CD 10E68B2F C13E16B2}\\ \texttt{2CB7AC00 D45ABE2A 2FD0CA5E 4E472895}\\ \texttt{43C20F62 56A5FAD3 3E862894 C15A477E}\\ \texttt{C4BBEE3C 139D9548 4243BA97 F200CA35}_{16},\end{array}$$

$$y_Q \leftarrow \begin{array}{l}\texttt{048521F7 AB27D7CF 81658CD7 D36018CE}\\ \texttt{B8FE6446 8F1E096A 0CB5638D 11C4697B}\\ \texttt{B7C9A1CA EAF5F243 A6477BE8 B306F20B}\\ \texttt{D45E5BB5 A8986FED 554509FD 5FDC39D6}_{16}.\end{array}$$

4 Задать хэш-значение:

$$H \leftarrow \begin{array}{l}\texttt{07ABBF85 80E7E5A3 21E9B940 F667AE20}\\ \texttt{9E2952CE F557978A E743DB08 6BAB4885}\\ \texttt{B708233C 3F5541DF 8AAFC361 1482FDE4}\\ \texttt{98E58B33 79A6622D AC2664C9 C118A162}_{16}.\end{array}$$

5 Задать значение ЭЦП:

$$S \leftarrow \begin{array}{l}\texttt{4B478B2B 28795A43 8C3F4A70 D7F302D3}\\ \texttt{D1B615E9 85CE22DA 7122AE1E AB0DD987}\\ \texttt{92399496 8A24BF15 C2E659B4 546F83CF}\\ \texttt{16493338 79D47954 C4AB7E41 046EB3D9}\\ \texttt{2787F785 C91230CD 7E65E455 26D45650}\\ \texttt{921D772D D42BD352 2CF7BD5F 7D79AB65}_{16}.\end{array}$$

6 Испытуемой реализацией выполнить проверку ЭЦП S.
7 Если алгоритм проверки ЭЦП возвратил `НЕТ`, то возвратить `ОШИБКА`.
8 Задать значение ЭЦП:

$$S \leftarrow \begin{array}{l}\texttt{4A478B2B 28795A43 8C3F4A70 D7F302D3}\\ \texttt{D1B615E9 85CE22DA 7122AE1E AB0DD987}\\ \texttt{92399496 8A24BF15 C2E659B4 546F83CF}\\ \texttt{16493338 79D47954 C4AB7E41 046EB3D9}\\ \texttt{2787F785 C91230CD 7E65E455 26D45650}\\ \texttt{921D772D D42BD352 2CF7BD5F 7D79AB65}_{16}.\end{array}$$

9 Испытуемой реализацией выполнить проверку ЭЦП S.
10 Если алгоритм проверки ЭЦП возвратил `НЕТ`, то возвратить `УСПЕХ`, иначе — `ОШИБКА`.

Тест BIGN.ECS.11

1 Задать параметры p, a, b, q, G из таблицы Б.3 СТБ 34.101.45.
2 Задать кодовое представление идентификатора:

$$OID(h) \leftarrow \texttt{06092A70 00020022 654D0D}_{16}.$$

3 Задать личный ключ:

$$d \leftarrow \begin{array}{l}\texttt{BEC09635 3EF4568A A417622A 95F2B563}\\ \texttt{33BF3A02 040B3137 2FD5737D E0F1A2BA}\\ \texttt{6090C1D1 A27155D8 711FFE5B 31027847}\\ \texttt{1B0B97CF 1B8FE821 C50205E5 D24AB9B8}_{16}.\end{array}$$

4 Задать открытый ключ:

$$x_Q \leftarrow \texttt{C6255C65 515274CD 10E68B2F C13E16B2}$$
$$\texttt{2CB7AC00 D45ABE2A 2FD0CA5E 4E472895}$$
$$\texttt{43C20F62 56A5FAD3 3E862894 C15A477E}$$
$$\texttt{C4BBEE3C 139D9548 4243BA97 F200CA35}_{16},$$

$$y_Q \leftarrow \texttt{048521F7 AB27D7CF 81658CD7 D36018CE}$$
$$\texttt{B8FE6446 8F1E096A 0CB5638D 11C4697B}$$
$$\texttt{B7C9A1CA EAF5F243 A6477BE8 B306F20B}$$
$$\texttt{D45E5BB5 A8986FED 554509FD 5FDC39D6}_{16}.$$

5 Для $i = 1, 2, \ldots, 10000$ выполнить:
1) псевдослучайным методом сгенерировать хэш-значение H;
2) псевдослучайным методом сгенерировать одноразовый личный ключ k;
3) испытуемой реализацией выполнить выработку ЭЦП и сохранить результат в S;
4) испытуемой реализацией выполнить проверку ЭЦП S;
5) если алгоритм проверки ЭЦП возвращает `НЕТ`, то возвратить `ОШИБКА`.
6 Возвратить `УСПЕХ`.

Тест BIGN.ECS.12

1 Задать параметры p, a, b, q, G из таблицы Б.3 СТБ 34.101.45.
2 Задать кодовое представление идентификатора:

$$OID(h) \leftarrow \texttt{06092A70 00020022 654D0D}_{16}.$$

3 Задать личный ключ:

$$d \leftarrow \texttt{BEC09635 3EF4568A A417622A 95F2B563}$$
$$\texttt{33BF3A02 040B3137 2FD5737D E0F1A2BA}$$
$$\texttt{6090C1D1 A27155D8 711FFE5B 31027847}$$
$$\texttt{1B0B97CF 1B8FE821 C50205E5 D24AB9B8}_{16}.$$

4 Для $i = 1, 2, \ldots, 10000$ выполнить:
1) псевдослучайным методом сгенерировать хэш-значение H;
2) псевдослучайным методом сгенерировать одноразовый личный ключ k;
3) испытуемой реализацией выполнить выработку ЭЦП и сохранить результат в S;
4) эталонной реализацией выполнить выработку ЭЦП и сохранить результат в S';
5) если $S \neq S'$, то возвратить `ОШИБКА`.
5 Возвратить `УСПЕХ`.

6.2.5 Алгоритмы транспорта ключа

При тестировании реализации алгоритмов транспорта ключа выполняются тесты BIGN.ECT.1 – BIGN.ECT.12.

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

ключ $X \in \{0,1\}^{8*}$, заголовок ключа $I \in \{0,1\}^{128}$, открытый ключ $Q \in E^*_{a,b}(\mathbb{F}_p)$, одноразовый личный ключ $k \in \{1,2,\ldots,q-1\}$, токен $Y \in \{0,1\}^*$, и личный ключ $d \in \{1,2,\ldots,q-1\}$.

В тестах для хранения результата создания токена ключа используются слова $Y, Y' \in \{0,1\}^{2l+|X|+128}$, а для хранения результата разбора токена ключа Y — слово $X' \in \{0,1\}^{|Y|-2l-128}$

Тест BIGN.ECT.1

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

2 Задать открытый ключ:

$$x_Q \leftarrow \texttt{BD1A5650 179D79E0 3FCEE49D 4C2BD5DD F54CE46D 0CF11E4F F87BF7A8 90857FD0}_{16},$$

$$y_Q \leftarrow \texttt{7AC6A603 61E8C817 3491686D 461B2826 190C2EDA 5909054A 9AB84D2A B9D99A90}_{16}.$$

3 Задать транспортируемый ключ:

$$X \leftarrow \texttt{B194BAC8 0A08F53B 366D008E 584A5DE4 8504}_{16}.$$

4 Задать заголовок ключа:

$$I \leftarrow \texttt{5BE3D612 17B96181 FE6786AD 716B890B}_{16}.$$

5 Задать одноразовый личный ключ:

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

6 Испытуемой реализацией выполнить создание токена ключа и сохранить результат в Y.

7 Если

$$Y = \texttt{9B4EA669 DABDF100 A7D4B6E6 EB76EE52 51912531 F426750A AC8A9DBB 51C54D8D EB9289B5 0A46952D 0531861E 45A8814B 008FDC65 DE9FF1FA 2A1F16B6 A280E957 A814}_{16},$$

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

Тест BIGN.ECT.2

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

2 Задать личный ключ:

$$d \leftarrow \texttt{1F66B5B8 4B733967 4533F032 9C74F218 34281FED 0732429E 0C79235F C273E269}_{16}.$$

3 Задать токен ключа:

$$Y \leftarrow \begin{array}{l}\texttt{4856093A 0F6C1301 5FC8E15F 1B23A762}\\ \texttt{02D2F4BA 6E5EC52B 78658477 F6486DE6}\\ \texttt{87AFAEEA 0EF7BC13 26A7DCE7 A10BA10E}\\ \texttt{3F91C012 6044B222 67BF30BD 6F1DA29E}\\ \texttt{0647CF39 C1D59A56 BB0194E0 F4F8A2BB}_{16}.\end{array}$$

4 Задать заголовок ключа:

$$I \leftarrow \texttt{E12BDC1A E28257EC 703FCCF0 95EE8DF1}_{16}.$$

5 Испытуемой реализацией выполнить разбор токена ключа и сохранить результат в X.

6 Если алгоритм разбора токена ключа не возвратил `ОШИБКА` и

$$X = \begin{array}{l}\texttt{B194BAC8 0A08F53B 366D008E 584A5DE4}\\ \texttt{8504FA9D 1BB6C7AC 252E72C2 02FDCE0D}_{16},\end{array}$$

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

Тест BIGN.ECT.3

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

2 Задать открытый ключ:

$$x_Q \leftarrow \begin{array}{l}\texttt{BD1A5650 179D79E0 3FCEE49D 4C2BD5DD}\\ \texttt{F54CE46D 0CF11E4F F87BF7A8 90857FD0}_{16},\end{array}$$

$$y_Q \leftarrow \begin{array}{l}\texttt{7AC6A603 61E8C817 3491686D 461B2826}\\ \texttt{190C2EDA 5909054A 9AB84D2A B9D99A90}_{16}.\end{array}$$

3 Задать личный ключ:

$$d \leftarrow \begin{array}{l}\texttt{1F66B5B8 4B733967 4533F032 9C74F218}\\ \texttt{34281FED 0732429E 0C79235F C273E269}_{16}.\end{array}$$

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

1) псевдослучайным методом сгенерировать транспортируемый ключ X длины 32 октета;

2) псевдослучайным методом сгенерировать заголовок ключа I;

3) псевдослучайным методом сгенерировать одноразовый личный ключ k;

4) испытуемой реализацией выполнить создание токена ключа и сохранить результат в Y;

5) испытуемой реализацией выполнить разбор токена ключа Y и сохранить результат в X';

6) если алгоритм проверки ЭЦП возвращает `ОШИБКА` или $X \neq X'$, то возвратить `ОШИБКА`.

5 Возвратить `УСПЕХ`.

Тест BIGN.ECT.4

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

$$x_Q \leftarrow \texttt{BD1A5650 179D79E0 3FCEE49D 4C2BD5DD}\ \texttt{F54CE46D 0CF11E4F F87BF7A8 90857FD0}_{16},$$

$$y_Q \leftarrow \texttt{7AC6A603 61E8C817 3491686D 461B2826}\ \texttt{190C2EDA 5909054A 9AB84D2A B9D99A90}_{16}.$$

3 Для $i = 1, 2, \ldots, 10000$ выполнить:
1) псевдослучайным методом сгенерировать транспортируемый ключ X длины 32 октета;
2) псевдослучайным методом сгенерировать заголовок ключа I;
3) псевдослучайным методом сгенерировать одноразовый личный ключ k;
4) испытуемой реализацией выполнить создание токена ключа и сохранить результат в Y;
5) эталонной реализацией выполнить создание токена ключа и сохранить результат в Y';
6) если $Y \neq Y'$, то возвратить `ОШИБКА`.
4 Возвратить `УСПЕХ`.

Тест BIGN.ECT.5

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

$$x_Q \leftarrow \texttt{212602EE 5589B84A 4585807A E8BFE371}\ \texttt{8A52B675 8B05F644 05F9D371 6462B02D}\ \texttt{334D51CF 27125637 37F63F5B 9BE7E4DA}_{16},$$

$$y_Q \leftarrow \texttt{8634E65F 71905CB7 204DC5BC 1229FB68}\ \texttt{76ED4F60 EC299D49 9AB0641A 5F82F291}\ \texttt{517F7631 4B50A0ED 389368A5 690EC3A5}_{16}.$$

3 Задать транспортируемый ключ:

$$X \leftarrow \texttt{94BAC80A 08F53B36 6D008E58 4A5DE485 04FA}_{16}.$$

4 Задать заголовок ключа:

$$I \leftarrow \texttt{E3D61217 B96181FE 6786AD71 6B890B5C}_{16}.$$

5 Задать одноразовый личный ключ:

$$k \leftarrow \texttt{2B4F71DB D8E70AA1 17BFA307 65AFA934}\ \texttt{69D31615 09B10406 A2A0860F 9DC98C50}\ \texttt{91CFDD4E 4B3B6462 B6B2EFCB 9B1FED44}_{16}.$$

6 Испытуемой реализацией выполнить создание токена ключа и сохранить результат в Y.

7 Если

$$Y = \texttt{BBADA0BA 582EEB29 C794544A AE2D212B}$$
$$\texttt{B4A97B11 9A70EB1A 58975C25 B0AE4CE2}$$
$$\texttt{C18AF138 158EB347 1945D9B9 A6BEEA96}$$
$$\texttt{8E4D0BC6 96566FE4 464406AF 5EB4CCCB}$$
$$\texttt{35A7E5F9 6B1819FE CA94DA5F C139366B}$$
$$\texttt{C894}_{16},$$

то возвратить УСПЕХ, иначе — ОШИБКА.

Тест BIGN.ECT.6

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

$$d \leftarrow \texttt{84C21DBF 7B3C2372 DC21386C 216FA16C}$$
$$\texttt{9EF10AEA F9F96A87 2FD8058F 2780BA93}$$
$$\texttt{0F08BE3B EC804161 37E11A23 2D93B50E}_{16}.$$

3 Задать токен ключа:

$$Y \leftarrow \texttt{E3DF6E76 38A80D5F 0B49AA4C 2EC98F10}$$
$$\texttt{0A8A8F92 18F3DC8A 6DBAFC23 F798E889}$$
$$\texttt{2BD2D64D B361D605 2797A0CB F8B0F44B}$$
$$\texttt{1AE13222 DE3F6410 EB0A0382 0B545E06}$$
$$\texttt{B230B0BE B19E2701 DA7330DB 8B62C3A9}$$
$$\texttt{37B5F3E2 D375F687 8BBF87BC B43EEBCA}_{16}.$$

4 Задать заголовок ключа:

$$I \leftarrow \texttt{2BDC1AE2 8257EC70 3FCCF095 EE8DF1C1}_{16}.$$

5 Испытуемой реализацией выполнить разбор токена ключа и сохранить результат в X.
6 Если алгоритм разбора токена ключа не возвратил ОШИБКА и

$$X = \texttt{94BAC80A 08F53B36 6D008E58 4A5DE485}$$
$$\texttt{04FA9D1B B6C7AC25 2E72C202 FDCE0D5B}_{16},$$

то возвратить УСПЕХ, иначе — ОШИБКА.

Тест BIGN.ECT.7

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

$$x_Q \leftarrow \texttt{212602EE 5589B84A 4585807A E8BFE371}$$
$$\texttt{8A52B675 8B05F644 05F9D371 6462B02D}$$
$$\texttt{334D51CF 27125637 37F63F5B 9BE7E4DA}_{16},$$

$$y_Q \leftarrow \begin{array}{l}\texttt{8634E65F 71905CB7 204DC5BC 1229FB68}\\ \texttt{76ED4F60 EC299D49 9AB0641A 5F82F291}\\ \texttt{517F7631 4B50A0ED 389368A5 690EC3A5}_{16}.\end{array}$$

3 Задать личный ключ:

$$d \leftarrow \begin{array}{l}\texttt{84C21DBF 7B3C2372 DC21386C 216FA16C}\\ \texttt{9EF10AEA F9F96A87 2FD8058F 2780BA93}\\ \texttt{0F08BE3B EC804161 37E11A23 2D93B50E}_{16}.\end{array}$$

4 Для $i = 1, 2, \ldots, 10000$ выполнить:
1) псевдослучайным методом сгенерировать транспортируемый ключ X длины 32 октета;
2) псевдослучайным методом сгенерировать заголовок ключа I;
3) псевдослучайным методом сгенерировать одноразовый личный ключ k;
4) испытуемой реализацией выполнить создание токена ключа и сохранить результат в Y;
5) испытуемой реализацией выполнить разбор токена ключа Y и сохранить результат в X';
6) если алгоритм проверки ЭЦП возвращает `ОШИБКА` или $X \neq X'$, то возвратить `ОШИБКА`.
5 Возвратить `УСПЕХ`.

Тест BIGN.ECT.8

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

$$x_Q \leftarrow \begin{array}{l}\texttt{212602EE 5589B84A 4585807A E8BFE371}\\ \texttt{8A52B675 8B05F644 05F9D371 6462B02D}\\ \texttt{334D51CF 27125637 37F63F5B 9BE7E4DA}_{16},\end{array}$$

$$y_Q \leftarrow \begin{array}{l}\texttt{8634E65F 71905CB7 204DC5BC 1229FB68}\\ \texttt{76ED4F60 EC299D49 9AB0641A 5F82F291}\\ \texttt{517F7631 4B50A0ED 389368A5 690EC3A5}_{16}.\end{array}$$

3 Для $i = 1, 2, \ldots, 10000$ выполнить:
1) псевдослучайным методом сгенерировать транспортируемый ключ X длины 32 октета;
2) псевдослучайным методом сгенерировать заголовок ключа I;
3) псевдослучайным методом сгенерировать одноразовый личный ключ k;
4) испытуемой реализацией выполнить создание токена ключа и сохранить результат в Y;
5) эталонной реализацией выполнить создание токена ключа и сохранить результат в Y';
6) если $Y \neq Y'$, то возвратить `ОШИБКА`.
4 Возвратить `УСПЕХ`.

Тест BIGN.ECT.9

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

2 Задать открытый ключ:

$$x_Q \leftarrow \texttt{C6255C65 515274CD 10E68B2F C13E16B2}$$
$$\texttt{2CB7AC00 D45ABE2A 2FD0CA5E 4E472895}$$
$$\texttt{43C20F62 56A5FAD3 3E862894 C15A477E}$$
$$\texttt{C4BBEE3C 139D9548 4243BA97 F200CA35}_{16},$$

$$y_Q \leftarrow \texttt{048521F7 AB27D7CF 81658CD7 D36018CE}$$
$$\texttt{B8FE6446 8F1E096A 0CB5638D 11C4697B}$$
$$\texttt{B7C9A1CA EAF5F243 A6477BE8 B306F20B}$$
$$\texttt{D45E5BB5 A8986FED 554509FD 5FDC39D6}_{16}.$$

3 Задать транспортируемый ключ:

$$X \leftarrow \texttt{BAC80A08 F53B366D 008E584A 5DE48504}$$
$$\texttt{FA9D}_{16}.$$

4 Задать заголовок ключа:

$$I \leftarrow \texttt{D61217B9 6181FE67 86AD716B 890B5CB0}_{16}.$$

5 Задать одноразовый личный ключ:

$$k \leftarrow \texttt{52BD3326 96B49E33 79F15D73 6AC05F39}$$
$$\texttt{27B8A02A 5577642C 39E5DA84 8D0C4BE6}$$
$$\texttt{DFA5DFCB 0BBBF7DC D7232EEA 5F50E18C}$$
$$\texttt{AC8A94A1 B5C55F69 DB08C56C E06053AA}_{16}.$$

6 Испытуемой реализацией выполнить создание токена ключа и сохранить результат в Y.

7 Если

$$Y = \texttt{6F50014D 62076605 391205E1 DDD61115}$$
$$\texttt{50ED6190 563C93D9 8AEEDC2B E9A7B846}$$
$$\texttt{2C156F77 9F78B5A9 9D8AC7DC 84DFFFB7}$$
$$\texttt{450DF15A 4D44970E ED577A30 864B2A1C}$$
$$\texttt{12D44891 676D8110 8F57277F 4E66E106}$$
$$\texttt{3552E36C B2282563 8711548E 701A22F6}$$
$$\texttt{5835}_{16},$$

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

Тест BIGN.ECT.10

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

2 Задать личный ключ:

$$d \leftarrow \texttt{BEC09635 3EF4568A A417622A 95F2B563}$$
$$\texttt{33BF3A02 040B3137 2FD5737D E0F1A2BA}$$
$$\texttt{6090C1D1 A27155D8 711FFE5B 31027847}$$
$$\texttt{1B0B97CF 1B8FE821 C50205E5 D24AB9B8}_{16}.$$

3 Задать токен ключа:

$$Y \leftarrow \texttt{C09D3FEA AE61571C DB0056C6 4EE46A14}$$
$$\texttt{0814278F 1D9B9449 8CA5B904 2A4BAE14}$$
$$\texttt{3E9CD0D6 DC2C5F1A 663368FE C3165611}$$
$$\texttt{9354F1D7 766FF7BB 2040FC7F 8C8A026B}$$
$$\texttt{C26FC267 ACBF2EC3 D4AC9DB5 A4452225}$$
$$\texttt{33E4B86A D2618DE8 0B8B94F8 EC5B7711}$$
$$\texttt{C5B2D55B 0FCBC416 FF3E11DF 5E17683F}_{16}.$$

4 Задать заголовок ключа:

$$I \leftarrow \texttt{DC1AE282 57EC703F CCF095EE 8DF1C1AB}_{16}.$$

5 Испытуемой реализацией выполнить разбор токена ключа и сохранить результат в X.

6 Если алгоритм разбора токена ключа не возвратил `ОШИБКА` и

$$X = \texttt{BAC80A08 F53B366D 008E584A 5DE48504}$$
$$\texttt{FA9D1BB6 C7AC252E 72C202FD CE0D5BE3}_{16},$$

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

Тест BIGN.ECT.11

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

2 Задать открытый ключ:

$$x_Q \leftarrow \texttt{C6255C65 515274CD 10E68B2F C13E16B2}$$
$$\texttt{2CB7AC00 D45ABE2A 2FD0CA5E 4E472895}$$
$$\texttt{43C20F62 56A5FAD3 3E862894 C15A477E}$$
$$\texttt{C4BBEE3C 139D9548 4243BA97 F200CA35}_{16},$$

$$y_Q \leftarrow \texttt{048521F7 AB27D7CF 81658CD7 D36018CE}$$
$$\texttt{B8FE6446 8F1E096A 0CB5638D 11C4697B}$$
$$\texttt{B7C9A1CA EAF5F243 A6477BE8 B306F20B}$$
$$\texttt{D45E5BB5 A8986FED 554509FD 5FDC39D6}_{16}.$$

3 Задать личный ключ:

$$d \leftarrow \texttt{BEC09635 3EF4568A A417622A 95F2B563}$$
$$\texttt{33BF3A02 040B3137 2FD5737D E0F1A2BA}$$
$$\texttt{6090C1D1 A27155D8 711FFE5B 31027847}$$
$$\texttt{1B0B97CF 1B8FE821 C50205E5 D24AB9B8}_{16}.$$

4 Для $i = 1, 2, \ldots, 10000$ выполнить:
1) псевдослучайным методом сгенерировать транспортируемый ключ X длины 32 октета;
2) псевдослучайным методом сгенерировать заголовок ключа I;
3) псевдослучайным методом сгенерировать одноразовый личный ключ k;
4) испытуемой реализацией выполнить создание токена ключа и сохранить результат в Y;
5) испытуемой реализацией выполнить разбор токена ключа Y и сохранить результат в X';
6) если алгоритм проверки ЭЦП возвращает `ОШИБКА` или $X \neq X'$, то возвратить `ОШИБКА`.
5 Возвратить `УСПЕХ`.

Тест BIGN.ECT.12

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

$$x_Q \leftarrow \begin{array}{l}\texttt{C6255C65 515274CD 10E68B2F C13E16B2}\\ \texttt{2CB7AC00 D45ABE2A 2FD0CA5E 4E472895}\\ \texttt{43C20F62 56A5FAD3 3E862894 C15A477E}\\ \texttt{C4BBEE3C 139D9548 4243BA97 F200CA35}_{16},\end{array}$$

$$y_Q \leftarrow \begin{array}{l}\texttt{048521F7 AB27D7CF 81658CD7 D36018CE}\\ \texttt{B8FE6446 8F1E096A 0CB5638D 11C4697B}\\ \texttt{B7C9A1CA EAF5F243 A6477BE8 B306F20B}\\ \texttt{D45E5BB5 A8986FED 554509FD 5FDC39D6}_{16}.\end{array}$$

3 Для $i = 1, 2, \ldots, 10000$ выполнить:
1) псевдослучайным методом сгенерировать транспортируемый ключ X длины 32 октета;
2) псевдослучайным методом сгенерировать заголовок ключа I;
3) псевдослучайным методом сгенерировать одноразовый личный ключ k;
4) испытуемой реализацией выполнить создание токена ключа и сохранить результат в Y;
5) эталонной реализацией выполнить создание токена ключа и сохранить результат в Y';
6) если $Y \neq Y'$, то возвратить `ОШИБКА`.
4 Возвратить `УСПЕХ`.

6.2.6 Алгоритмы идентификационной цифровой подписи

При тестировании реализации алгоритмов идентификационной ЭЦП (ИЭЦП) выполняются тесты BIGN.IBS.1 – BIGN.IBS.15.

Входными данными тестов являются параметры p, a, b, q, G, которые описывают группу точек эллиптической кривой и определяют уровень стойкости l, кодовое представление идентификатора алгоритма хэширования $OID(h) \in \{0,1\}^*$, хэш-значение $h(Id) \in \{0,1\}^{2l}$ идентификатора.

Кроме общих параметров входными данными тестов BIGN.IDS.1, BIGN.IDS.6, BIGN.IDS.11 являются подпись $S \in \{0,1\}^*$ идентификатора, выработанная доверенной стороной, и открытый ключ $Q = (x_Q, y_Q) \in E^*_{a,b}(\mathbb{F}_p)$ доверенной стороны.

Кроме общих параметров входными данными тестов BIGN.IDS.2 – BIGN.IDS.5, BIGN.IDS.7 – BIGN.IDS.10, BIGN.IDS.12 – BIGN.IDS.15 являются личный ключ $e \in \{0,1,\ldots,q-1\}$, одноразовый личный ключ $k \in \{0,1,\ldots,q-1\}$, хэш-значение сообщения $h(X) \in \{0,1\}^{2l}$, идентификационная подпись $S \in \{0,1\}^*$, открытый ключ $R = (x_R, y_R)$, где x_R, y_R — целые числа, и открытый ключ $Q \in E^*_{a,b}(\mathbb{F}_p)$ доверенной стороны.

В тестах для хранения результата извлечения личного ключа используется $e \in \{0,1,\ldots,q-1\}$, для хранения результата извлечения открытого ключа — $R \in E^*_{a,b}(\mathbb{F}_p)$, а для хранения результата выработки ИЭЦП используются слова $S, S' \in \{0,1\}^{3l}$.

Тест BIGN.IBS.1

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

2 Задать кодовое представление идентификатора алгоритма хэширования:

$$OID(h) \leftarrow \texttt{06092A70 00020022 651F51}_{16}.$$

3 Задать хэш-значение идентификатора:

$$h(Id) \leftarrow \begin{array}{l}\texttt{ABEF9725 D4C5A835 97A367D1 4494CC25}\\ \texttt{42F20F65 9DDFECC9 61A3EC55 0CBA8C75}_{16}.\end{array}$$

4 Задать открытый ключ доверенной стороны:

$$x_Q \leftarrow \begin{array}{l}\texttt{BD1A5650 179D79E0 3FCEE49D 4C2BD5DD}\\ \texttt{F54CE46D 0CF11E4F F87BF7A8 90857FD0}_{16},\end{array}$$

$$y_Q \leftarrow \begin{array}{l}\texttt{7AC6A603 61E8C817 3491686D 461B2826}\\ \texttt{190C2EDA 5909054A 9AB84D2A B9D99A90}_{16}.\end{array}$$

5 Задать подпись идентификатора:

$$S \leftarrow \begin{array}{l}\texttt{E36B7F03 77AE4C52 4027C387 FADF1B20}\\ \texttt{CE72F153 0B71F2B5 FD3A8C58 4FE2E1AE}\\ \texttt{D20082E3 0C8AF650 11F4FB54 649DFD3D}_{16}.\end{array}$$

6 Испытуемой реализацией выполнить извлечения пары ключей и сохранить результат в e, $R = (x_R, y_R)$.

7 Если

$$e = \begin{array}{l}\texttt{79628979 DF369BEB 94DEF329 9476AED4}\\ \texttt{14F39148 AA69E31A 7397E8AA 70578AB3}_{16},\end{array}$$

$$x_R = \begin{array}{l}\texttt{CCEEF1A3 13A40664 9D15DA0A 851D486A}\\ \texttt{695B641B 20611776 252FFDCE 39C71060}_{16},\end{array}$$

$$y_R = \begin{array}{l}\texttt{7C9EA1F3 3C23D20D FCB8485A 88BE6523}\\ \texttt{A28ECC32 15B47FA2 89D6C9BE 1CE837C0}_{16},\end{array}$$

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

Тест BIGN.IBS.2

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

2 Задать кодовое представление идентификатора алгоритма хэширования:

$$OID(h) \leftarrow \texttt{06092A70 00020022 651F51}_{16}.$$

3 Задать хэш-значение идентификатора:

$$h(Id) \leftarrow \begin{array}{l}\texttt{ABEF9725 D4C5A835 97A367D1 4494CC25}\\ \texttt{42F20F65 9DDFECC9 61A3EC55 0CBA8C75}_{16}.\end{array}$$

4 Задать личный ключ:

$$e \leftarrow \begin{array}{l}\texttt{79628979 DF369BEB 94DEF329 9476AED4}\\ \texttt{14F39148 AA69E31A 7397E8AA 70578AB3}_{16}.\end{array}$$

5 Задать хэш-значение сообщения:

$$X \leftarrow \begin{array}{l}\texttt{9D02EE44 6FB6A29F E5C982D4 B13AF9D3}\\ \texttt{E90861BC 4CEF27CF 306BFB0B 174A154A}_{16}.\end{array}$$

6 Задать одноразовый личный ключ:

$$k \leftarrow \begin{array}{l}\texttt{0BA66DA6 214E48A7 01F22695 BA9CD6D5}\\ \texttt{67DE17A1 C6010624 88728ED8 BBF48ED0}_{16}.\end{array}$$

7 Испытуемой реализацией выполнить выработку ИЭЦП и сохранить результат в S.

8 Если

$$S = \begin{array}{l}\texttt{FF050E47 EB1CC116 A4524EF3 17E84429}\\ \texttt{F4057FFF 7725BF7A 605EDDCE 63B89A1B}\\ \texttt{322509D8 EA993039 52C90674 D718CA02}_{16},\end{array}$$

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

Тест BIGN.IBS.3

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

2 Задать кодовое представление идентификатора алгоритма хэширования:

$$OID(h) \leftarrow \texttt{06092A70 00020022 651F51}_{16}.$$

3 Задать хэш-значение идентификатора:

$$h(Id) \leftarrow \begin{array}{l}\texttt{ABEF9725 D4C5A835 97A367D1 4494CC25}\\ \texttt{42F20F65 9DDFECC9 61A3EC55 0CBA8C75}_{16}.\end{array}$$

4 Задать открытый ключ доверенной стороны:

$$x_Q \leftarrow \begin{array}{l}\texttt{BD1A5650 179D79E0 3FCEE49D 4C2BD5DD}\\ \texttt{F54CE46D 0CF11E4F F87BF7A8 90857FD0}_{16},\end{array}$$

$$y_Q \leftarrow \begin{array}{l}\texttt{7AC6A603 61E8C817 3491686D 461B2826}\\ \texttt{190C2EDA 5909054A 9AB84D2A B9D99A90}_{16}.\end{array}$$

5 Задать открытый ключ:

$$x_R \leftarrow \texttt{CCEEF1A3 13A40664 9D15DA0A 851D486A}\ \texttt{695B641B 20611776 252FFDCE 39C71060}_{16},$$

$$y_R \leftarrow \texttt{7C9EA1F3 3C23D20D FCB8485A 88BE6523}\ \texttt{A28ECC32 15B47FA2 89D6C9BE 1CE837C0}_{16}.$$

6 Задать хэш-значение сообщения:

$$X \leftarrow \texttt{ABEF9725 D4C5A835 97A367D1 4494CC25}\ \texttt{42F20F65 9DDFECC9 61A3EC55 0CBA8C75}_{16}.$$

7 Задать ИЭЦП:

$$S \leftarrow \texttt{BE54F0EC 2DDBA581 0440E140 D8A587ED}\ \texttt{55D5C3C3 10F91679 F804A35C 9C3C21C6}\ \texttt{2A0EBED9 022D81AB DE62FB83 BB5E6304}_{16}.$$

8 Испытуемой реализацией выполнить проверку ИЭЦП.
9 Если алгоритм проверки ИЭЦП возвратил `НЕТ`, то возвратить `ОШИБКА`.
10 Задать ИЭЦП:

$$S \leftarrow \texttt{BF54F0EC 2DDBA581 0440E140 D8A587ED}\ \texttt{55D5C3C3 10F91679 F804A35C 9C3C21C6}\ \texttt{2A0EBED9 022D81AB DE62FB83 BB5E6304}_{16}.$$

11 Испытуемой реализацией выполнить проверку ИЭЦП.
12 Если алгоритм проверки ИЭЦП возвратил `НЕТ`, то возвратить `УСПЕХ`, иначе — `ОШИБКА`.

Тест BIGN.IBS.4

1 Задать параметры p, a, b, q, G из таблицы Б.1 СТБ 34.101.45.
2 Задать кодовое представление идентификатора алгоритма хэширования:

$$OID(h) \leftarrow \texttt{06092A70 00020022 651F51}_{16}.$$

3 Задать хэш-значение идентификатора:

$$h(Id) \leftarrow \texttt{ABEF9725 D4C5A835 97A367D1 4494CC25}\ \texttt{42F20F65 9DDFECC9 61A3EC55 0CBA8C75}_{16}.$$

4 Задать открытый ключ доверенной стороны:

$$x_Q \leftarrow \texttt{BD1A5650 179D79E0 3FCEE49D 4C2BD5DD}\ \texttt{F54CE46D 0CF11E4F F87BF7A8 90857FD0}_{16},$$

$$y_Q \leftarrow \texttt{7AC6A603 61E8C817 3491686D 461B2826}\ \texttt{190C2EDA 5909054A 9AB84D2A B9D99A90}_{16}.$$

5 Задать личный ключ:

$$e \leftarrow \texttt{79628979 DF369BEB 94DEF329 9476AED4}\ \texttt{14F39148 AA69E31A 7397E8AA 70578AB3}_{16}.$$

6 Задать открытый ключ:

$$x_R \leftarrow \texttt{CCEEF1A3 13A40664 9D15DA0A 851D486A 695B641B 20611776 252FFDCE 39C71060}_{16},$$

$$y_R \leftarrow \texttt{7C9EA1F3 3C23D20D FCB8485A 88BE6523 A28ECC32 15B47FA2 89D6C9BE 1CE837C0}_{16}.$$

7 Для $i = 1, 2, \ldots, 10000$ выполнить:
1) псевдослучайным методом сгенерировать хэш-значение сообщения $h(X)$;
2) псевдослучайным методом сгенерировать одноразовый личный ключ k;
3) испытуемой реализацией выполнить выработку ИЭЦП и сохранить результат в S;
4) испытуемой реализацией выполнить проверку ИЭЦП S;
5) если алгоритм проверки ИЭЦП возвращает `НЕТ`, то возвратить `ОШИБКА`.
8 Возвратить `УСПЕХ`.

Тест BIGN.IBS.5

1 Задать параметры p, a, b, q, G из таблицы Б.1 СТБ 34.101.45.
2 Задать кодовое представление идентификатора алгоритма хэширования:

$$OID(h) \leftarrow \texttt{06092A70 00020022 651F51}_{16}.$$

3 Задать хэш-значение идентификатора:

$$h(Id) \leftarrow \texttt{ABEF9725 D4C5A835 97A367D1 4494CC25 42F20F65 9DDFECC9 61A3EC55 0CBA8C75}_{16}.$$

4 Задать личный ключ:

$$e \leftarrow \texttt{79628979 DF369BEB 94DEF329 9476AED4 14F39148 AA69E31A 7397E8AA 70578AB3}_{16}.$$

5 Для $i = 1, 2, \ldots, 10000$ выполнить:
1) псевдослучайным методом сгенерировать хэш-значение сообщения $h(X)$;
2) псевдослучайным методом сгенерировать одноразовый личный ключ k;
3) испытуемой реализацией выполнить выработку ИЭЦП и сохранить результат в S;
4) эталонной реализацией выполнить выработку ИЭЦП и сохранить результат в S';
5) если $S \neq S'$, то возвратить `ОШИБКА`.
6 Возвратить `УСПЕХ`.

Тест BIGN.IBS.6

1 Задать параметры p, a, b, q, G из таблицы Б.2 СТБ 34.101.45.
2 Задать кодовое представление идентификатора алгоритма хэширования:

$$OID(h) \leftarrow \texttt{06092A70 00020022 654D0C}_{16}.$$

3 Задать хэш-значение идентификатора:

$$h(Id) \leftarrow \texttt{A5DCA107 22EEB92A 7C245688 2C730119}$$
$$\texttt{EA58115C 8DF9068C 9C26D33D 18AB8CDC}$$
$$\texttt{A84A03C2 B872F147 22F3F568 0234EB28}_{16}.$$

4 Задать открытый ключ доверенной стороны:

$$x_Q \leftarrow \texttt{212602EE 5589B84A 4585807A E8BFE371}$$
$$\texttt{8A52B675 8B05F644 05F9D371 6462B02D}$$
$$\texttt{334D51CF 27125637 37F63F5B 9BE7E4DA}_{16},$$

$$y_Q \leftarrow \texttt{8634E65F 71905CB7 204DC5BC 1229FB68}$$
$$\texttt{76ED4F60 EC299D49 9AB0641A 5F82F291}$$
$$\texttt{517F7631 4B50A0ED 389368A5 690EC3A5}_{16}.$$

5 Задать подпись идентификатора:

$$S \leftarrow \texttt{7FD0BFFA D6A63069 20602AA8 464781AC}$$
$$\texttt{0F83BDF2 38A4B59E 5F049057 E3C9B13B}$$
$$\texttt{B15B3C81 A99D4BCF E804A02D 6ED54473}$$
$$\texttt{4AD0F8A0 6C1ED447 87E2118C 3F35FDA8}$$
$$\texttt{940A34BE 868F3C04}_{16}.$$

6 Испытуемой реализацией выполнить извлечения пары ключей и сохранить результат в e, $R = (x_R, y_R)$.

7 Если

$$e = \texttt{04E1315F 05B86B66 2D809209 D6104DE8}$$
$$\texttt{D25DB189 FBCE4BFF E6F6CBDE 84C96024}$$
$$\texttt{302D154E F8A7EEF0 B6FD2927 89C3272D}_{16},$$

$$x_R = \texttt{96FF522D B94308E0 0B438E8B C2BAFB07}$$
$$\texttt{94BA4269 88E464F6 9DAB96B0 C7DB7FBB}$$
$$\texttt{48588D83 1F4751F4 1E7454C4 6193EE36}_{16},$$

$$y_R = \texttt{5B8622B1 155DA785 6E8E643F 0B5BA937}$$
$$\texttt{2479ABFC DB1AA7C9 3CE0E1A8 2D2EEF33}$$
$$\texttt{6C8FE65D 2447F78D 3B7780C6 6E0892BA}_{16},$$

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

Тест BIGN.IBS.7

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

2 Задать кодовое представление идентификатора алгоритма хэширования:

$$OID(h) \leftarrow \texttt{06092A70 00020022 654D0C}_{16}.$$

3 Задать хэш-значение идентификатора:

$$h(Id) \leftarrow \texttt{A5DCA107 22EEB92A 7C245688 2C730119}$$
$$\texttt{EA58115C 8DF9068C 9C26D33D 18AB8CDC}$$
$$\texttt{A84A03C2 B872F147 22F3F568 0234EB28}_{16}.$$

4 Задать личный ключ:

$$e \leftarrow \texttt{04E1315F 05B86B66 2D809209 D6104DE8}$$
$$\texttt{D25DB189 FBCE4BFF E6F6CBDE 84C96024}$$
$$\texttt{302D154E F8A7EEF0 B6FD2927 89C3272D}_{16}.$$

5 Задать хэш-значение сообщения:

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

6 Задать одноразовый личный ключ:

$$k \leftarrow \texttt{01629612 C7A5A6B6 92279ABA 89230FA9}$$
$$\texttt{6D60FB47 EA099428 6F954878 8DDB8C9E}$$
$$\texttt{4E91BF81 984AC850 02E7727D 0D6FB060}_{16}.$$

7 Испытуемой реализацией выполнить выработку ИЭЦП и сохранить результат в S.

8 Если

$$S = \texttt{BEF7D5AA 29B4B3F1 5719703A 2F1671D5}$$
$$\texttt{FC61A63D 1EDC6B1F 44921EC0 4C963740}$$
$$\texttt{88BC2905 148D692D AA463EBD 966463C7}$$
$$\texttt{C0E3A5C7 F37CF60D FFEED22A E18E667D}$$
$$\texttt{D8B66448 316F8D5B}_{16},$$

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

Тест BIGN.IBS.8

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

2 Задать кодовое представление идентификатора алгоритма хэширования:

$$OID(h) \leftarrow \texttt{06092A70 00020022 654D0C}_{16}.$$

3 Задать хэш-значение идентификатора:

$$h(Id) \leftarrow \texttt{A5DCA107 22EEB92A 7C245688 2C730119}$$
$$\texttt{EA58115C 8DF9068C 9C26D33D 18AB8CDC}$$
$$\texttt{A84A03C2 B872F147 22F3F568 0234EB28}_{16}.$$

4 Задать открытый ключ доверенной стороны:

$$x_Q \leftarrow \texttt{212602EE 5589B84A 4585807A E8BFE371}$$
$$\texttt{8A52B675 8B05F644 05F9D371 6462B02D}$$
$$\texttt{334D51CF 27125637 37F63F5B 9BE7E4DA}_{16},$$

$$y_Q \leftarrow \texttt{8634E65F 71905CB7 204DC5BC 1229FB68}$$
$$\texttt{76ED4F60 EC299D49 9AB0641A 5F82F291}$$
$$\texttt{517F7631 4B50A0ED 389368A5 690EC3A5}_{16}.$$

5 Задать открытый ключ:

$$x_R \leftarrow \texttt{96FF522D B94308E0 0B438E8B C2BAFB07}$$
$$\texttt{94BA4269 88E464F6 9DAB96B0 C7DB7FBB}$$
$$\texttt{48588D83 1F4751F4 1E7454C4 6193EE36}_{16},$$

$$y_R \leftarrow \texttt{5B8622B1 155DA785 6E8E643F 0B5BA937}$$
$$\texttt{2479ABFC DB1AA7C9 3CE0E1A8 2D2EEF33}$$
$$\texttt{6C8FE65D 2447F78D 3B7780C6 6E0892BA}_{16}.$$

6 Задать хэш-значение сообщения:

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

7 Задать ИЭЦП:

$$S \leftarrow \texttt{7BC4568E 6527C478 F4B0D1F3 11095C6B}$$
$$\texttt{2ED8574B 22D26978 001DA821 76E83684}$$
$$\texttt{BE4FA282 238AD5A1 CB81A244 12A15AAB}$$
$$\texttt{7B774D98 78C43038 3638C439 40964436}$$
$$\texttt{4D095EE6 FC11E243}_{16}.$$

8 Испытуемой реализацией выполнить проверку ИЭЦП.
9 Если алгоритм проверки ИЭЦП возвратил `НЕТ`, то возвратить `ОШИБКА`.
10 Задать ИЭЦП:

$$S \leftarrow \texttt{7A568E 6527C478 F4B0D1F3 11095C6B}$$
$$\texttt{2ED8574B 22D26978 001DA821 76E83684}$$
$$\texttt{BE4FA282 238AD5A1 CB81A244 12A15AAB}$$
$$\texttt{7B774D98 78C43038 3638C439 40964436}$$
$$\texttt{4D095EE6 FC11E243}_{16}.$$

11 Испытуемой реализацией выполнить проверку ИЭЦП.
12 Если алгоритм проверки ИЭЦП возвратил `НЕТ`, то возвратить `УСПЕХ`, иначе — `ОШИБКА`.

Тест BIGN.IBS.9

1 Задать параметры p, a, b, q, G из таблицы Б.2 СТБ 34.101.45.
2 Задать кодовое представление идентификатора алгоритма хэширования:

$$OID(h) \leftarrow \texttt{06092A70 00020022 654D0C}_{16}.$$

3 Задать хэш-значение идентификатора:

$$h(Id) \leftarrow \texttt{A5DCA107 22EEB92A 7C245688 2C730119}$$
$$\texttt{EA58115C 8DF9068C 9C26D33D 18AB8CDC}$$
$$\texttt{A84A03C2 B872F147 22F3F568 0234EB28}_{16}.$$

4 Задать открытый ключ доверенной стороны:

$$x_Q \leftarrow \begin{array}{l}\texttt{212602EE 5589B84A 4585807A E8BFE371}\\ \texttt{8A52B675 8B05F644 05F9D371 6462B02D}\\ \texttt{334D51CF 27125637 37F63F5B 9BE7E4DA}_{16},\end{array}$$

$$y_Q \leftarrow \begin{array}{l}\texttt{8634E65F 71905CB7 204DC5BC 1229FB68}\\ \texttt{76ED4F60 EC299D49 9AB0641A 5F82F291}\\ \texttt{517F7631 4B50A0ED 389368A5 690EC3A5}_{16}.\end{array}$$

5 Задать личный ключ:

$$e \leftarrow \begin{array}{l}\texttt{04E1315F 05B86B66 2D809209 D6104DE8}\\ \texttt{D25DB189 FBCE4BFF E6F6CBDE 84C96024}\\ \texttt{302D154E F8A7EEF0 B6FD2927 89C3272D}_{16}.\end{array}$$

6 Задать открытый ключ:

$$x_R \leftarrow \begin{array}{l}\texttt{96FF522D B94308E0 0B438E8B C2BAFB07}\\ \texttt{94BA4269 88E464F6 9DAB96B0 C7DB7FBB}\\ \texttt{48588D83 1F4751F4 1E7454C4 6193EE36}_{16},\end{array}$$

$$y_R \leftarrow \begin{array}{l}\texttt{5B8622B1 155DA785 6E8E643F 0B5BA937}\\ \texttt{2479ABFC DB1AA7C9 3CE0E1A8 2D2EEF33}\\ \texttt{6C8FE65D 2447F78D 3B7780C6 6E0892BA}_{16}.\end{array}$$

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

1) псевдослучайным методом сгенерировать хэш-значение сообщения $h(X)$;
2) псевдослучайным методом сгенерировать одноразовый личный ключ k;
3) испытуемой реализацией выполнить выработку ИЭЦП и сохранить результат в S;
4) испытуемой реализацией выполнить проверку ИЭЦП S;
5) если алгоритм проверки ИЭЦП возвращает `НЕТ`, то возвратить `ОШИБКА`.

8 Возвратить `УСПЕХ`.

Тест BIGN.IBS.10

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

2 Задать кодовое представление идентификатора алгоритма хэширования:

$$OID(h) \leftarrow \texttt{06092A70 00020022 654D0C}_{16}.$$

3 Задать хэш-значение идентификатора:

$$h(Id) \leftarrow \begin{array}{l}\texttt{A5DCA107 22EEB92A 7C245688 2C730119}\\ \texttt{EA58115C 8DF9068C 9C26D33D 18AB8CDC}\\ \texttt{A84A03C2 B872F147 22F3F568 0234EB28}_{16}.\end{array}$$

4 Задать личный ключ:

$$e \leftarrow \begin{array}{l}\texttt{04E1315F 05B86B66 2D809209 D6104DE8}\\ \texttt{D25DB189 FBCE4BFF E6F6CBDE 84C96024}\\ \texttt{302D154E F8A7EEF0 B6FD2927 89C3272D}_{16}.\end{array}$$

5 Для $i = 1, 2, \ldots, 10000$ выполнить:
1) псевдослучайным методом сгенерировать хэш-значение сообщения $h(X)$;
2) псевдослучайным методом сгенерировать одноразовый личный ключ k;
3) испытуемой реализацией выполнить выработку ИЭЦП и сохранить результат в S;
4) эталонной реализацией выполнить выработку ИЭЦП и сохранить результат в S';
5) если $S \neq S'$, то возвратить `ОШИБКА`.
6 Возвратить `УСПЕХ`.

Тест BIGN.IBS.11

1 Задать параметры p, a, b, q, G из таблицы Б.3 СТБ 34.101.45.
2 Задать кодовое представление идентификатора алгоритма хэширования:

$$OID(h) \leftarrow \texttt{06092A70 00020022 654D0D}_{16}.$$

3 Задать хэш-значение идентификатора:

$$h(Id) \leftarrow \begin{array}{l}\texttt{3C329B13 ECD6EFA9 D12E8455 E3EDF1A4}\\ \texttt{0B674700 7A0FF468 EDB2B911 2A68AF3B}\\ \texttt{8949D974 B57D002B BA8D934F 0B1E9E2B}\\ \texttt{951CCF83 26DB4FE3 064B590F E2D07E79}_{16}.\end{array}$$

4 Задать открытый ключ доверенной стороны:

$$x_Q \leftarrow \begin{array}{l}\texttt{C6255C65 515274CD 10E68B2F C13E16B2}\\ \texttt{2CB7AC00 D45ABE2A 2FD0CA5E 4E472895}\\ \texttt{43C20F62 56A5FAD3 3E862894 C15A477E}\\ \texttt{C4BBEE3C 139D9548 4243BA97 F200CA35}_{16},\end{array}$$

$$y_Q \leftarrow \begin{array}{l}\texttt{048521F7 AB27D7CF 81658CD7 D36018CE}\\ \texttt{B8FE6446 8F1E096A 0CB5638D 11C4697B}\\ \texttt{B7C9A1CA EAF5F243 A6477BE8 B306F20B}\\ \texttt{D45E5BB5 A8986FED 554509FD 5FDC39D6}_{16}.\end{array}$$

5 Задать подпись идентификатора:

$$S \leftarrow \begin{array}{l}\texttt{1F24FEBC 3C92B31B 26871E05 C24CA257}\\ \texttt{0025FA99 07BCCFB4 5E637773 9C44F514}\\ \texttt{5E5EF3CD 477FE5E6 8085227E 04BE397C}\\ \texttt{DA045442 9A09F411 1BE3FD2A 971D11E3}\\ \texttt{CC304748 C1B7B8D4 4835710E D2BAA727}\\ \texttt{3F680FC1 7521B668 534B6FBE 7A1990B9}_{16}.\end{array}$$

6 Испытуемой реализацией выполнить извлечения пары ключей и сохранить результат в e, $R = (x_R, y_R)$.
7 Если

$$e = \begin{array}{l}\texttt{A90188D4 EAA8D5B3 1FD54F3E 02E10FEB}\\ \texttt{F1577A14 642D7C88 B9951F3B 957C006C}\\ \texttt{567A20BD 7635B9FF 02C3045E DDD84553}\\ \texttt{D484DE44 9CFC054C 5A96C8CD 5CEA0E33}_{16},\end{array}$$

$$x_R = \begin{array}{l}\texttt{11516758 2A97B4DB F51A1B59 3DDF44D3}\\ \texttt{0B84D8E2 74B31553 7402CFE9 4B0251F6}\\ \texttt{586B3287 809DB27B 4076F54D D3FB8D89}\\ \texttt{8B96204A DD543F38 191A9256 95DB5367}_{16},\end{array}$$

$$y_R = \begin{array}{l}\texttt{FD0A3195 F06A4A84 DF5940AB 113BC817}\\ \texttt{98392F87 0EEDFFDF CBC76EDD C0F74544}\\ \texttt{793B93E6 B4AED5E6 D005FAB5 3DABAD75}\\ \texttt{AE86F361 4F3CDC4C D5FEF99D 122A743A}_{16},\end{array}$$

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

Тест BIGN.IBS.12

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

2 Задать кодовое представление идентификатора алгоритма хэширования:

$$OID(h) \leftarrow \texttt{06092A70 00020022 654D0D}_{16}.$$

3 Задать хэш-значение идентификатора:

$$h(Id) \leftarrow \begin{array}{l}\texttt{3C329B13 ECD6EFA9 D12E8455 E3EDF1A4}\\ \texttt{0B674700 7A0FF468 EDB2B911 2A68AF3B}\\ \texttt{8949D974 B57D002B BA8D934F 0B1E9E2B}\\ \texttt{951CCF83 26DB4FE3 064B590F E2D07E79}_{16}.\end{array}$$

4 Задать личный ключ:

$$e \leftarrow \begin{array}{l}\texttt{A90188D4 EAA8D5B3 1FD54F3E 02E10FEB}\\ \texttt{F1577A14 642D7C88 B9951F3B 957C006C}\\ \texttt{567A20BD 7635B9FF 02C3045E DDD84553}\\ \texttt{D484DE44 9CFC054C 5A96C8CD 5CEA0E33}_{16}.\end{array}$$

5 Задать хэш-значение сообщения:

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

6 Задать одноразовый личный ключ:

$$k \leftarrow \begin{array}{l}\texttt{E023B431 F73B2531 B078E36D C34D5C9F}\\ \texttt{463F2CB7 444BD4D3 6E272F6C EAE30C7A}\\ \texttt{FA63E6E2 86726514 F905489C 70ED0B58}\\ \texttt{891EA8A3 6726D14C 911DE939 0859D37E}_{16}.\end{array}$$

7 Испытуемой реализацией выполнить выработку ИЭЦП и сохранить результат в S.

8 Если

$$S = \texttt{C8B750EE 1248526B F21495D7 9650BE09}$$
$$\texttt{1EBA4F30 52B4F192 38CA6E37 84099DF7}$$
$$\texttt{6E068BB0 3E25479E B305C672 6F48A27A}$$
$$\texttt{5A2AFCC1 A3B505A5 FE2CF41B C1F3117F}$$
$$\texttt{A1B5C032 5DA88D54 9EE4CA3B DBCFCECF}$$
$$\texttt{02A3D8B1 6B76F3C0 6259E65F 12628761}_{16},$$

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

Тест BIGN.IBS.13

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

2 Задать кодовое представление идентификатора алгоритма хэширования:

$$OID(h) \leftarrow \texttt{06092A70 00020022 654D0D}_{16}.$$

3 Задать хэш-значение идентификатора:

$$h(Id) \leftarrow \texttt{3C329B13 ECD6EFA9 D12E8455 E3EDF1A4}$$
$$\texttt{0B674700 7A0FF468 EDB2B911 2A68AF3B}$$
$$\texttt{8949D974 B57D002B BA8D934F 0B1E9E2B}$$
$$\texttt{951CCF83 26DB4FE3 064B590F E2D07E79}_{16}.$$

4 Задать открытый ключ доверенной стороны:

$$x_Q \leftarrow \texttt{C6255C65 515274CD 10E68B2F C13E16B2}$$
$$\texttt{2CB7AC00 D45ABE2A 2FD0CA5E 4E472895}$$
$$\texttt{43C20F62 56A5FAD3 3E862894 C15A477E}$$
$$\texttt{C4BBEE3C 139D9548 4243BA97 F200CA35}_{16},$$

$$y_Q \leftarrow \texttt{048521F7 AB27D7CF 81658CD7 D36018CE}$$
$$\texttt{B8FE6446 8F1E096A 0CB5638D 11C4697B}$$
$$\texttt{B7C9A1CA EAF5F243 A6477BE8 B306F20B}$$
$$\texttt{D45E5BB5 A8986FED 554509FD 5FDC39D6}_{16}.$$

5 Задать открытый ключ:

$$x_R \leftarrow \texttt{11516758 2A97B4DB F51A1B59 3DDF44D3}$$
$$\texttt{0B84D8E2 74B31553 7402CFE9 4B0251F6}$$
$$\texttt{586B3287 809DB27B 4076F54D D3FB8D89}$$
$$\texttt{8B96204A DD543F38 191A9256 95DB5367}_{16},$$

$$y_R \leftarrow \texttt{FD0A3195 F06A4A84 DF5940AB 113BC817}$$
$$\texttt{98392F87 0EEDFFDF CBC76EDD C0F74544}$$
$$\texttt{793B93E6 B4AED5E6 D005FAB5 3DABAD75}$$
$$\texttt{AE86F361 4F3CDC4C D5FEF99D 122A743A}_{16}.$$

6 Задать хэш-значение сообщения:

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

7 Задать ИЭЦП:

$$S \leftarrow \texttt{E40C57F4 4E0BC8F9 0B7AB110 0B5448E5}$$
$$\texttt{3B3D2117 B51F0048 9452E478 8E8B142A}$$
$$\texttt{B8A84BBA CE08E781 9A699374 76785490}$$
$$\texttt{502614C8 9F0818CC 79763717 7F2956C9}$$
$$\texttt{52836EA8 91FDB83C 4F043AEB 42293481}$$
$$\texttt{4322C573 41D9B56F 3E574BAA 3481C844}_{16}.$$

8 Испытуемой реализацией выполнить проверку ИЭЦП.
9 Если алгоритм проверки ИЭЦП возвратил `НЕТ`, то возвратить `ОШИБКА`.
10 Задать ИЭЦП:

$$S \leftarrow \texttt{E5C57F4 4E0BC8F9 0B7AB110 0B5448E5}$$
$$\texttt{3B3D2117 B51F0048 9452E478 8E8B142A}$$
$$\texttt{B8A84BBA CE08E781 9A699374 76785490}$$
$$\texttt{502614C8 9F0818CC 79763717 7F2956C9}$$
$$\texttt{52836EA8 91FDB83C 4F043AEB 42293481}$$
$$\texttt{4322C573 41D9B56F 3E574BAA 3481C844}_{16}.$$

11 Испытуемой реализацией выполнить проверку ИЭЦП.
12 Если алгоритм проверки ИЭЦП возвратил `НЕТ`, то возвратить `УСПЕХ`, иначе — `ОШИБКА`.

Тест BIGN.IBS.14

1 Задать параметры p, a, b, q, G из таблицы Б.3 СТБ 34.101.45.
2 Задать кодовое представление идентификатора алгоритма хэширования:

$$OID(h) \leftarrow \texttt{06092A70 00020022 654D0D}_{16}.$$

3 Задать хэш-значение идентификатора:

$$h(Id) \leftarrow \texttt{3C329B13 ECD6EFA9 D12E8455 E3EDF1A4}$$
$$\texttt{0B674700 7A0FF468 EDB2B911 2A68AF3B}$$
$$\texttt{8949D974 B57D002B BA8D934F 0B1E9E2B}$$
$$\texttt{951CCF83 26DB4FE3 064B590F E2D07E79}_{16}.$$

4 Задать открытый ключ доверенной стороны:

$$x_Q \leftarrow \texttt{C6255C65 515274CD 10E68B2F C13E16B2}$$
$$\texttt{2CB7AC00 D45ABE2A 2FD0CA5E 4E472895}$$
$$\texttt{43C20F62 56A5FAD3 3E862894 C15A477E}$$
$$\texttt{C4BBEE3C 139D9548 4243BA97 F200CA35}_{16},$$

$$y_Q \leftarrow \texttt{048521F7 AB27D7CF 81658CD7 D36018CE}$$
$$\texttt{B8FE6446 8F1E096A 0CB5638D 11C4697B}$$
$$\texttt{B7C9A1CA EAF5F243 A6477BE8 B306F20B}$$
$$\texttt{D45E5BB5 A8986FED 554509FD 5FDC39D6}_{16}.$$

5 Задать личный ключ:

$$e \leftarrow \begin{array}{l}\texttt{A90188D4 EAA8D5B3 1FD54F3E 02E10FEB}\\ \texttt{F1577A14 642D7C88 B9951F3B 957C006C}\\ \texttt{567A20BD 7635B9FF 02C3045E DDD84553}\\ \texttt{D484DE44 9CFC054C 5A96C8CD 5CEA0E33}_{16}.\end{array}$$

6 Задать открытый ключ:

$$x_R \leftarrow \begin{array}{l}\texttt{11516758 2A97B4DB F51A1B59 3DDF44D3}\\ \texttt{0B84D8E2 74B31553 7402CFE9 4B0251F6}\\ \texttt{586B3287 809DB27B 4076F54D D3FB8D89}\\ \texttt{8B96204A DD543F38 191A9256 95DB5367}_{16},\end{array}$$

$$y_R \leftarrow \begin{array}{l}\texttt{FD0A3195 F06A4A84 DF5940AB 113BC817}\\ \texttt{98392F87 0EEDFFDF CBC76EDD C0F74544}\\ \texttt{793B93E6 B4AED5E6 D005FAB5 3DABAD75}\\ \texttt{AE86F361 4F3CDC4C D5FEF99D 122A743A}_{16}.\end{array}$$

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

1) псевдослучайным методом сгенерировать хэш-значение сообщения $h(X)$;

2) псевдослучайным методом сгенерировать одноразовый личный ключ k;

3) испытуемой реализацией выполнить выработку ИЭЦП и сохранить результат в S;

4) испытуемой реализацией выполнить проверку ИЭЦП S;

5) если алгоритм проверки ИЭЦП возвращает `НЕТ`, то возвратить `ОШИБКА`.

8 Возвратить `УСПЕХ`.

Тест BIGN.IBS.15

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

2 Задать кодовое представление идентификатора алгоритма хэширования:

$$OID(h) \leftarrow \texttt{06092A70 00020022 654D0D}_{16}.$$

3 Задать хэш-значение идентификатора:

$$h(Id) \leftarrow \begin{array}{l}\texttt{3C329B13 ECD6EFA9 D12E8455 E3EDF1A4}\\ \texttt{0B674700 7A0FF468 EDB2B911 2A68AF3B}\\ \texttt{8949D974 B57D002B BA8D934F 0B1E9E2B}\\ \texttt{951CCF83 26DB4FE3 064B590F E2D07E79}_{16}.\end{array}$$

4 Задать личный ключ:

$$e \leftarrow \begin{array}{l}\texttt{A90188D4 EAA8D5B3 1FD54F3E 02E10FEB}\\ \texttt{F1577A14 642D7C88 B9951F3B 957C006C}\\ \texttt{567A20BD 7635B9FF 02C3045E DDD84553}\\ \texttt{D484DE44 9CFC054C 5A96C8CD 5CEA0E33}_{16}.\end{array}$$

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

1) псевдослучайным методом сгенерировать хэш-значение сообщения $h(X)$;

2) псевдослучайным методом сгенерировать одноразовый личный ключ k;
3) испытуемой реализацией выполнить выработку ИЭЦП и сохранить результат в S;
4) эталонной реализацией выполнить выработку ИЭЦП и сохранить результат в S';
5) если $S \neq S'$, то возвратить `ОШИБКА`.
6 Возвратить `УСПЕХ`.

6.2.7 Алгоритм построения ключа защиты по паролю

При тестировании реализации алгоритма построения ключа защиты по паролю выполняются тесты BIGN.PBK.1 – BIGN.PBK.3.

Входными данными тестов являются пароль $P \in \{0,1\}^{8*}$, число итераций $c \in \{1,2,\ldots\}$ и синхропосылка $S \in \{0,1\}^{8*}$.

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

Тест BIGN.PBK.1

1 Задать пароль:

$$I \leftarrow \texttt{42313934 42414338 30413038 46353342}_{16}.$$

2 Задать число итераций: $c \leftarrow 10000$.
3 Задать синхропосылку:

$$S \leftarrow \texttt{BE329713 43FC9A48 A02A885F 194B09A1}_{16}.$$

4 Испытуемой реализацией выполнить построения ключа защиты по паролю и сохранить результат в K.
5 Если

$$K = \begin{array}{l}\texttt{D9024724 82130F3B 77D09303 03DD7E4E}\\ \texttt{68630CC0 2B56A8B2 AFA74F09 6BCAC971}_{16},\end{array}$$

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

Тест BIGN.PBK.2

1 Задать пароль:

$$I \leftarrow \begin{array}{l}\texttt{E9DEE72C 8F0C0FA6 2DDB49F4 6F739647}\\ \texttt{06075316 ED247A37 39CBA383 03A98BF6}_{16}.\end{array}$$

2 Задать число итераций: $c \leftarrow 10000$.
3 Задать синхропосылку:

$$S \leftarrow \begin{array}{l}\texttt{BE329713 43FC9A48 A02A885F 194B09A1}\\ \texttt{7ECDA4D0 1544AF8C A58450BF 66D2E88A}_{16}.\end{array}$$

4 Испытуемой реализацией выполнить построения ключа защиты по паролю и сохранить результат в K.
5 Если

$$K = \begin{array}{l}\texttt{ADFB258D 3FFE73C9 2109CBAB 3BD3EA77}\\ \texttt{0ADE798E ABB71D6B FE16DE00 1F23D22A}_{16},\end{array}$$

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

Тест BIGN.PBK.3

1 Задать пароль:

$$I \leftarrow \texttt{1F66B5B8 4B733967 4533F032 9C74F218}\ \texttt{34281FED 0732429E 0C79235F C273E269}\ \texttt{4C0E74B2 CD5811AD}_{16}.$$

2 Задать число итераций: $c \leftarrow 10000$.

3 Задать синхропосылку:

$$S \leftarrow \texttt{BE329713 43FC9A48 A02A885F 194B09A1}\ \texttt{7ECDA4D0 1544AF8C}_{16}.$$

4 Испытуемой реализацией выполнить построения ключа защиты по паролю и сохранить результат в K.

5 Если

$$K = \texttt{DED0E547 959760ED 4DE9258B 6912F4D3}\ \texttt{EB6F3961 57E0CC86 83B31932 B6E62F02}_{16},$$

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

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 следующие константы:

– значения кодового представления идентификатора алгоритма хэширования $\mathrm{OID}(h)$ (шаг 2 п. 6.3.3, шаг 4 п. 7.1.3, шаг 7 п. 7.1.4, шаг 8 п. В.2.3, шаг 5 п. В.2.4 СТБ 34.101.45);

– 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 константы 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 34.101.45 вспомогательное преобразование, являющееся композиционной частью некоторого криптографического алгоритма.

В СТБ 34.101.45 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);

– алгоритм вычисления порядка группы точек (п. 6.1.2 СТБ 34.101.45). В случае реализации данного алгоритма необходимо провести его проверку в соответствии с документацией на реализованный алгоритм;

– алгоритм проверки простоты (п. 6.1.2 СТБ 34.101.45). При реализации алгоритма, отличного от указанного в п. Ж.1 СТБ 34.101.45, необходимо провести проверку реализации в соответствии с документацией на алгоритм. Алгоритм должен быть математически обоснован;

– тест на квадратичный вычет (п. 6.1.2 СТБ 34.101.45). При реализации алгоритма, отличного от указанного в п. Ж.2 СТБ 34.101.45, необходимо провести проверку реализации в соответствии с документацией на алгоритм. Алгоритм должен быть математически обоснован;

– алгоритм хэширования `belt-hash` (п. 6.1.2, 6.3.2, 7.1.2, В.2.2 СТБ 34.101.45). Проверка должна проводиться по согласованной с Органом по сертификации методике испытаний программы, реализующей функцию хэширования согласно СТБ 34.101.31. Проверка может не проводиться, если реализации `belt-hash` уже прошла испытания по указанной методике. В таких случаях эксперт может зачесть результаты испытаний реализации `belt-hash` предварительно проверив совпадение испытанной ранее реализации с проверяемой;

– функция хэширования h (п. 7.1.2, В.2.2 СТБ 34.101.45). Алгоритм хэширования, который определяет действие h, должен быть задан в ТНПА. Проверка должна проводиться

по согласованной с Органом по сертификации методике испытаний программы, реализующей функцию хэширования согласно заданному ТНПА. Проверка может не проводиться, если реализация h уже прошла испытания по указанной методике. В таких случаях эксперт может зачесть результаты испытаний реализации h предварительно проверив совпадение испытанной ранее реализации с проверяемой;

– алгоритмы `belt-block` (п. 6.3.2 СТБ 34.101.45), `belt-kwp` (п. 7.2.2, Е.3 СТБ 34.101.45) и $\texttt{belt-kwp}^{-1}$ (п. 7.2.2, Е.3 СТБ 34.101.45). Проверка должна проводиться по согласованной с Органом по сертификации методике испытаний программы, реализующей алгоритмы шифрования согласно СТБ 34.101.31. Проверка может не проводиться, если реализации `belt-block`, `belt-kwp` и $\texttt{belt-kwp}^{-1}$ уже прошли испытания по указанной методике. В таких случаях эксперт может зачесть результаты испытаний реализаций `belt-block`, `belt-kwp` и $\texttt{belt-kwp}^{-1}$ предварительно проверив совпадение испытанных ранее реализаций с проверяемыми;

– алгоритм `hmac[belt-hash]` (п. Е.2.2 СТБ 34.101.45). Проверка должна проводиться по согласованной с Органом по сертификации методике испытаний программы, реализующей алгоритм выработки имитовставки согласно СТБ 34.101.47. Проверка может не проводиться, если реализации `hmac[belt-hash]` уже прошла испытания по указанной методике. В таких случаях эксперт может зачесть результаты испытаний реализации `hmac[belt-hash]` предварительно проверив совпадение испытанной ранее реализации с проверяемой.

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

В СТБ 34.101.45 определены следующие криптографические алгоритмы:

– алгоритмы генерации и проверки параметров эллиптической кривой (п. 6.1 СТБ 34.101.45);

– алгоритмы генерации и проверки ключей (п. 6.2 СТБ 34.101.45);

– алгоритм генерации одноразового личного ключа (п. 6.3 СТБ 34.101.45);

– алгоритмы выработки и проверки ЭЦП (п. 7.1 СТБ 34.101.45);

– алгоритмы транспорта ключа (п. 7.2 СТБ 34.101.45);

– алгоритмы извлечения пары ключей, выработки и проверки ИЭЦП (прил. В СТБ 34.101.45);

– алгоритм построения ключа защиты по паролю (п. Е.2 СТБ 34.101.45).

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.

6.3.10 Корректность управления секретными данными

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

Секретными данными СТБ 34.101.45 являются:

– личные ключи;

– одноразовые личные ключи;

– секретный ключ, используемый в алгоритмах транспорта ключа;

– транспортируемый ключ;

– сообщение и его хэш-значение, если в соответствии с документацией реализации алгоритмов выработки и проверки ЭЦП/ИЭЦП могут использоваться для контроля целостности и подлинности сообщений, которые должны быть защищены от раскрытия;

– пароль и сформированный ключ защиты, используемые в алгоритме построения ключа защиты по паролю.

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
согласно СТБ 34.101.45-2013

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 согласно СТБ 34.101.45-2013.

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 согласно СТБ 34.101.45. 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
согласно СТБ 34.101.45-2013

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	BIGN.ECS.1	{Поле 8}
2	BIGN.ECS.2	{Поле 8}
...	...	...

3. Заключение по результатам тестирования: объект испытаний {Поле 4} соответствует (не соответствует) требованиям, установленным в СТБ 34.101.45–2013.

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 34.101.45. 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

Экз. {Поле 1}

Протокол № {Поле 2} **от** {Поле 3}
результатов анализа исходных текстов программ
объекта испытаний {Поле 4}, реализующего криптографические алгоритмы
согласно СТБ 34.101.45-2013

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	{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 34.101.45-2013.

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 34.101.45. 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.