Лабораторные работы по курсу «КриптоПротоколы»

Оглавление

[Общие положения для всех лабораторных работ 3](#_Toc82791290)

[Лабораторная работа 1 4](#_Toc82791291)

[Задание: 4](#_Toc82791292)

[Содержание отчета: 4](#_Toc82791293)

[Лабораторная работа 2. Электронная подпись и хэш-функция 5](#_Toc82791294)

[Задание 5](#_Toc82791295)

[Содержание отчета: 5](#_Toc82791296)

[Лабораторная работа №3. Программный датчик случайных чисел и алгоритм диверсификации ключа 6](#_Toc82791297)

[Задание 6](#_Toc82791298)

[Содержание отчета: 6](#_Toc82791299)

[Лабораторная работа №4. Протокол взаимной аутентификации с помощью доверенной третьей стороны. Протокол защищённого обмена сообщениями 8](#_Toc82791300)

[Задание 8](#_Toc82791301)

[Содержание отчета: 8](#_Toc82791302)

# **Общие положения** для всех лабораторных работ

1. При разработке ориентироваться на документ: «Р 1323565.1.012-2017 Информационная технология. Криптографическая защита информации. Принципы разработки и модернизации шифровальных (криптографических) средств защиты информации». В качестве класса принять КС3.
2. Процедуры дополнения до блока реализоваться согласно ГОСТ 34.13.2018
3. Коллективное выполнение не допускается.
4. Допустимые языки программирования для реализации: любой компилируемый язык (например С/С++).
5. После реализации необходимо составить «Отчет по лабораторной работе».
6. К отчету прилагаются исходные тексты и описание программы. Описание рекомендуется выполнять в соответствии с ГОСТ 19.402-78 Единая система программной документации. Описание программы.
7. Для тестирования необходимо привести артефакты тестирования в виде лог-файлов, скриншотов или каких-либо их аналогов, подтверждающих выполнение тестирования.

# Лабораторная работа 1.

## Задание:

1. Реализовать алгоритм шифрования и режим работы блочного шифра согласно ГОСТ 34.13-2018 и рекомендациям ТК-26, согласно варианту, зависящему от порядкового номера студента в списке группы.
2. Провести тестирование реализованного алгоритма и режимов его работы.
3. Написать отчет о лабораторной работе.

Содержание отчета:

1. Общее описание алгоритма. Длина блока. Длина ключа. Количество раундов
2. Описание криптографических свойств алгоритма и принципов его построения. Максимальная теоретическая стойкость для тотального перебора. Известные оценки стойкости по открытым источникам
3. Вычислительная сложность алгоритма, как временная, так и по памяти.
4. Общее описание программной реализации алгоритма
5. Отчет о скорости выполнения тестового задания.
   1. Шифрование и расшифрование произвольных файлов размером: 1 Мб, 100 Мб, 1000 Мб для каждого из режимов.
   2. Шифрование и расшифрование 106 произвольных блоков открытого текста со сменой ключа каждые 10, 100, 1000 блоков для каждого из режимов.
6. Описание тестового стенда
7. Фиксацию нагрузки на ОЗУ и ЦП во время выполнения тестового задания.
8. Проверку встречной работы с таким же алгоритмом, реализованным другим автором.

## Варианты:

1. «Кузнечик» OFB

2. «Магма» OFB

3. «Магма» OMAC

4. «Магма» CTR-ACPKM

5. «Магма» MGM

6. «Кузнечик» CBC

7. «Магма» CBC

8. «Кузнечик» CTR-ACPKM

9. «Кузнечик» OMAC

10. «Кузнечик» MGM

11. «Кузнечик» РСВС (данный режим не описан в методических документах, перечисленных в пункте 1 задания на данную лабораторную работу).

# Лабораторная работа 2. Алгоритм диверсификации ключа

## Задание

1. Реализовать алгоритм диверсификации ключа. Исходить из предположения, что существует мастер-ключ надлежащего качества. Алгоритм генерации согласно варианту, зависящему от порядкового номера студента в списке группы.
2. Провести тестирование реализованного алгоритма и режимов его работы.
3. Написать отчет о лабораторной работе.

Содержание отчета:

1. Общее описание алгоритма.
2. Описание криптографических свойств алгоритма и принципов его построения.
3. Вычислительная сложность алгоритма, как временная, так и по памяти.
4. Общее описание программной реализации алгоритма
5. Отчет о скорости выполнения тестового задания. Генерация некоторого случайного количества ключей в интервале 104 -106 штук.
6. Описание тестового стенда
7. Фиксацию нагрузки на ОЗУ и ЦП во время выполнения тестового задания.

## Варианты

1. Алгоритм описанный в «Р 50.1.113 ― 2016 Информационная технология. Криптографическая защита информации. Криптографические алгоритмы, сопутствующие. Применению алгоритмов электронной цифровой подписи и функции хэширования». (KDF\_GOSTR3411\_2012\_256)
2. Алгоритм описанный в «Р 1323565.1.022-2018 Информационная технология (ИТ). Криптографическая защита информации. Функции выработки производного ключа»
3. Алгоритм описанный в «Р 50.1.113 ― 2016 Информационная технология. Криптографическая защита информации. Криптографические алгоритмы, сопутствующие. Применению алгоритмов электронной цифровой подписи и функции хэширования». (KDF\_TREE\_GOSTR3411\_2012\_256)

# Лабораторная работа №3. Программный датчик случайных чисел и

## Задание

1. Реализовать алгоритм программного датчика случайных чисел. Исходить из предположения, что существует источник начальной энтропии надлежащего качества. Алгоритм генерации выбрать самостоятельно, с учетом имеющихся знаний в профессиональной области.
2. Провести проверку качества выходной последовательности при помощи батареи тестов NIST.

Содержание отчета:

1. Общее описание алгоритма программного датчика случайных чисел по следующему ряду параметров. Описание криптографических свойств алгоритма и принципов его построения. Количество раундов (шагов, циклов).
2. Вычислительная сложность алгоритма, как временная, так и по памяти.
3. Известные оценки качества выходной последовательности по открытым источникам
4. Обоснование выбора данного алгоритма
5. Описание
6. Отчет о скорости выполнения тестового задания.
   1. Генерация случайного файла размером. 1 Мб, 100 Мб, 1000 Мб
   2. Генерация некоторого случайного количества ключей в интервале: 103-104 штук.
7. Общее описание программной реализации алгоритма
8. Описание тестового стенда
9. Фиксация нагрузки на ОЗУ и ЦП во время выполнения тестового задания.

# Лабораторная работа №4.

## Задание:

1. Реализовать протокол «CRISP» согласно: «Р 1323565.1.029— 2019 Информационная технология. Криптографическая защита информации. Протокол защищенного обмена для индустриальных систем.»
2. Крипто примитивы использовать из предыдущих лабораторных работ.

Содержание отчета:

1. Общее описание протокола.
2. Описание криптографических свойств протокол и принципов его построения. Количество раундов (шагов, циклов).
3. Вычислительная сложность протокола, как временная, так и по памяти.
4. Обоснование выбора данного протокола
5. Общее описание программной реализации алгоритма
6. Отчет о скорости выполнения тестового задания.
   1. Прохождение некоторого случайного количества процедур аутентификации в интервале: 104-106 раз.
   2. Прохождение некоторого случайного количества сеансов обмена сообщениями с аутентификациями и сменами ключа: 102-103 раз.
   3. Фиксация нагрузки на ОЗУ и ЦП во время выполнения тестового задания.
7. Проверка встречной работы.