Федеральное государственное автономное
образовательное учреждение
высшего образования
«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

ИНСТИТУТ КОСМИЧЕСКИХ И ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА

ОТЧЕТ ПО ПРАКТИЧЕСКОЙ РАБОТЕ
по дисциплине «Информационная безопасность и защита информации»
Современные симметричные шифры. AES-128/AES-256.
Вариант 6

Преподаватель _____ А. А. Сидарас
подпись, дата инициалы, фамилия

Студент КИ19-07Б, 031941597 _____ А. А. Горбацевич
номер группы, зачётной книжки подпись, дата инициалы, фамилия

Красноярск 2021

Содержание

1 Цель работы

Освоить принципы работы современного симметричного шифра AES-128/ AES-256.

2 Задание

Разработать алгоритм шифрования AES-128/AES-256; реализовать программу использующую данный шифр для шифрования/расшифрования данных; протестировать алгоритм.

3 Выполнение работы

3.1 Реализация метода шифрования на ЯП

Для реализации был выбрал ЯП Dart с фреймворком графического интерфейса Flutter.

Исходный код проекта выложен в репозиторий на GitHub: https://github.com/NuarkNoir/UPC/blob/master/4sem/isaip/03/AESCryptor/aes_cryptor.

3.2 Тестирование

Бали написаны автоматические тесты с использованием возможностей языка Dart, исходные коды теста находятся в директории https://github.com/NuarkNoir/UPC/blob/master/4sem/isaip/03/AESCryptor/aes_cryptor/test.

Также имеется возможность ручного тестирования, при условии открытия проекта через Android Studio/InteliJ IDEA с плагинами для Flutter и Dart.