Правительство Российской Федерации

Федеральное государственное автономное образовательное учреждение
высшего образования «Национальный исследовательский университет

«Высшая школа экономики»
Кафедра «Компьютерная безопасность»

Прототип системы с использованием кодовой криптографии на основе криптосистем МакЭлиса и Нидеррайтера как консольное приложение

ТЕХНИЧЕСКОЕ ЗАДАНИЕ

Москва 2022

Введение

Консольное приложение с использованием кодовой криптографии на основе криптосистем МакЭлиса и Нидеррайтера реализует алгоритмы, являющимися кандидатами для постквантовой криптографии - актуальной части криптографии при появлении квантовых компьютеров и квантовых атак. Данное приложение является прототипом для последующей разработки криптографической системы с использованием реализованных алгоритмов.

Основание для разработки

Первичным документом на основании которого ведется разработка алгоритма МакЭлиса является статья Роберта МакЭлиса “A public key cryptosystem based on algebraic coding theory” (1978). Для алгоритма Нидеррайтера таковым является документ Харальда Нидеррайтера "Knapsack-type cryptosystems and algebraic coding theory" (1986).

Поиск дополнительных источников информации по вышеупомянутым системам является одним из этапов разработки программного продукта.

Назначение разработки

Данное консольное приложение должно содержать функциональность шифрования и расшифрования входных данных в соответствии с алгоритмами МакЭлиса и Нидеррайтера.

Программный продукт является прототипом для последующей разработки криптографической системы с использованием реализованных алгоритмов.

Требование к программе или программному изделию

Прототип системы с использованием кодовой криптографии на основе криптосистем МакЭлиса и Нидеррайтера должен быть реализован на языке программирования C\C++. Возможна дополнительная реализация на языке программирования Python.

Требование к программной документации

Для создания и поддержки актуальной документации по кодовой базе проекта будет использовано средство автоматической генерации документации разработчика “Doxygen”. Требуется реализовать полное покрытие документацией разработанных алгоритмов.

Стадии и этапы разработки

Этап 1

Поиск обзорных статей по системам МакЭлиса и Нидеррайтера.

Этап 2

Поиск существующих библиотек для работы с конечными полями и блочными кодами исправляющими ошибки, при возможности планируется собственная реализация.

Этап 3

Поиск реализаций алгоритма перемножения матриц над конечными полями, при возможности планируется собственная реализация.

Этап 4

Реализация консольного приложение, осуществляющее шифрование по схемам МакЭлиса.

Этап 5

Реализация алгоритма шифрования по схемам Нидеррайтера.

Этап 6

Реализация модульных (unit), интеграционных и нагрузочных тестов.

Этап 7

Проведение оценки скорости работы алгоритмов.

Этап 8

Анализ возможности использовании схем для электронной подписи.

Этап 9

Создание технического отчета.

Этап 10

Написание документации для пользователей и разработчиков.

Порядок контроля и приемки

Результатом работы является программный продукт (консольное приложение) с документацией разработчика и техническим отчетом.

Состав группы разработчиков

Студенты группы СКБ181 кафедры «Компьютерной безопасности» МИЭМ НИУ ВШЭ:

- Щебетов Андрей
- Шабаев Сергей
- Щелканова Екатерина
- Юровских Ясмин