Петрозаводский государственный университет
Институт математики и информационных технологий
Кафедра Информатики и Математического Обеспечения

09.03.04 - Программная инженерия

Отчет о проектной работе по курсу «Основы информатики и программирования»

Приложение «Desktop crypto tool»

Выполнила:
студентка 1 курса группы 22107

Т. Д. Квист _____
подпись

Руководитель:
А. В. Бородин, старший преподаватель

Петрозаводск — 2021

Содержание

Введение **3**

1 Требования к приложению **4**

2 Проектирование приложения **5**

3 Релизация приложения **6**

Заключение **7**

Введение

Цель проекта: разработать приложение для решения основных криптографических задач.

Задачи проекта:

1. Разработать модуль для подбора строки, которой соответствует заданный хеш.
2. Разработать модуль для дешифровки RSA.
3. Разработать модуль для перевода кодировки из UTF-8 в base16, base32 и base64.
4. Разработать графический интерфейс пользователя.
5. Реализовать приложение с использованием разработанных модулей и QtQuick.

В мире криптографии часто приходится решать какие-то задачи, которые человек может выполнять несколько часов, а то и дней. Для этого создаются приложения, автоматизирующие эти процессы: вычисление сложных математических операций, brute-force (метод перебора грубой силы) и т.п. Случаются ситуации, когда нет доступа к сети Интернет, в связи с этим создаются оффлайн приложения. Основная цель этого проекта: разработать оффлайн приложение, которое поможет решить некоторые базовые задачи криптографии (подбор хеша, дешифровка RSA, перевод из одной кодировки в другую). Для достижения этой цели необходимо разработать соответствующие модули.

1 Требования к приложению

- Подбор MD5 хеша методом грубой силы.
- Дешифровка криптографического алгоритма RSA.
- Перевод строки из UTF-8 в base16 (другими словами hex), base32, base64.

2 Проектирование приложения

Модули приложения:

1. hash.cpp — работа с хешем. Основная функция модуля:
    - check_hash() — проверка наличия строки в словаре (rockyou.txt), для которой хеш будет совпадать с заданной строкой.
2. rsa.cpp — работа с RSA. Основные функции модуля:
    - solve_rsa() — подготовка всех необходимых переменных для дешифровки RSA.
    - calculateD() — подсчёт числа d, для которого будет выполняться следующее условие: $d \cdot e = 1 \; mod \; phi$
    - decrypt() — дешифровка сообщения со всеми необходимыми переменными.
3. bases.cpp — работа с кодировками. Основная функция модуля:
    - bases_encode() — перевод строки из UTF-8 в следующие кодировки: base16, base32 и base64. Используется сторонняя библиотека для подсчёта base32 и base64: `https://github.com/tplgy/cppcodec`.
4. Page1Form.ui.qml — графический интерфейс главной страницы.
5. Page2Form.ui.qml — графический интерфейс для работы с хешами.
6. Page3Form.ui.qml — графический интерфейс для работы с RSA.
7. Page4Form.ui.qml — графический интерфейс для работы с кодировками.
8. main.qml — главный модуль графического интерфейсаю
9. main.cpp — главный модуль для работы с фунциями на языке «C++», в котором инициализируются экземпляры классов Hash, RSA и Bases.

3 Релизация приложения

Для реализации приложения были использованы языки «C++» и «QML».

- Количество модулей: 5.
- Количество классов: 3.
- Количество «C++» функций: 5.
- Количество «QML» сигналов: 6.
- Количество строк «C++» кода: 227.
- Количество строк «QML» кода: 661.

Заключение

В результате проекта было разработано приложение для решения основных криптографических задач. Пользователь может узнать для какой строке соответствует заданный хеш, дешифровать RSA и поменять кодировку у заданной строки.

Получен опыт работы с криптографическими библиотеками языка «C++», а также опыт работы с «QtQuick».