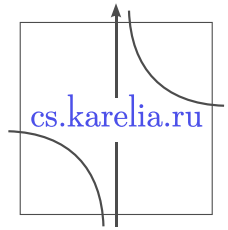
Петрозаводский государственный университет
Кафедра информатики и математического обеспечения



Татьяна Денисовна Квист

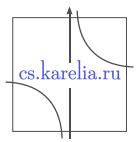
Приложение «Desktop crypto tool»

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

Научный руководитель: ст. преп., А. В. Бородин

Проблема автоматизации

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.



Цель и задачи

Цель работы

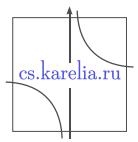
Разработать приложение для решения основных криптографических задач.

Задачи

- разработать модуль для подбора строки, которой соответствует заданный хеш;
- разработать модуль для дешифровки RSA;
- разработать модуль для перевода кодировки из UTF-8 в base16, base32 и base64;
- разработать графический интерфейс пользователя;
- реализовать приложение с использованием разработанных модулей и QtQuick.

Этапы разработки приложения

1. Разработка модуля для подбора хеша.
2. Разработка модуля для дешифровки RSA.
3. Разработка перевода из одной кодировки в другие.
4. Разработка графического интерфейса пользователя.



Hash.cpp

Модуль, позволяющий подобрать строку, MD5-хеш которой будет соответствовать заданной строке. Подбор осуществляется методом грубой силы по словарю rockyou.txt. В классе содержится одна функция: check_hash().

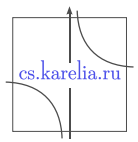
RSA.cpp

Модуль, позволяющий дешифровать криптографический алгоритм RSA. Пользователь вводит переменные p, q, e и само зашифрованное сообщение. В классе содержится три функции:

- 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.

Bases.cpp

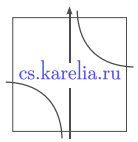
Модуль, позволяющий перевести заданную пользователем строку в base16, base32 и base64. Используется сторонняя библиотека для подсчёта base32 и base64: `https://github.com/tplgy/cppcodec`. Функция модуля: bases_encode().



Заключение

Реализованные функции:

- Подбор MD5-хеша.
- Дешифровка RSA.
- Перевод строки из UTF-8 в base16 (hex), base32 и base64



Заключение

В результате проекта было разработано приложение для решения основных криптографических задач.
Предлагаемые дополнения для реализации:

- определение кодировки для последующего перевода в другую кодировку;
- добавление шифров (например Цезарь, Атбаш и т.д.)

Спасибо за внимание!