МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«МОСКОВСКИЙ АВИАЦИОННЫЙ ИНСТИТУТ
(НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ)» (МАИ)

Кафедра 319 «Системы интеллектуального мониторинга»

Отчет

по лабораторной работе №3 по дисциплине:
«Защита информации»

Выполнил: Корнилов А. Н.

Студент группы: М3О-435Б-17

Проверил: Коновалов К.А.

Москва 2020

Оглавление

1. Постановка задачи 3
2. Описание алгоритма 4
3. Организация данных 6
3.1. Организация входных данных 6
3.2. Организация выходных данных 6
4. Технические и программные средства 6
4.1. Технические средства 6
4.2. Программные средствами 6
5. Результаты работы программы и их оценка 7
5.1. Объект испытаний 7
5.2. Цель испытаний 7
5.3. Требования к программе 7
5.4. Методы испытаний 7
5.5. Оценка результатов тестирования 9
Заключение 10
Список литературы 10
Ссылка на проект: 11

1. Постановка задачи

Разработать алгоритмы шифрования и дешифрования следующими методами:

- Скитала;
- Шифрующие таблицы;
- Двойная перестановка;
- Магический квадрат;
- Полибианский квадрат;
- Шифр Цезаря;
- Шифр Гронсфельда;
- Шифр Виженера;
- Шифр Уитстона.

Для реализации данной задачи необходимо:

- Реализовать графический интерфейс;
- предусмотреть возможные нарушения порядка эксплуатации и реализовать вывод аварийных сообщений;
- реализовать взаимодействие программы с пользователем, разработать и воплотить алгоритмы вывода полученного результата в удобной для пользователя форме.

2. Описание алгоритма

На Рисунке 1 представлен скриншот интерфейса запущенной программы.

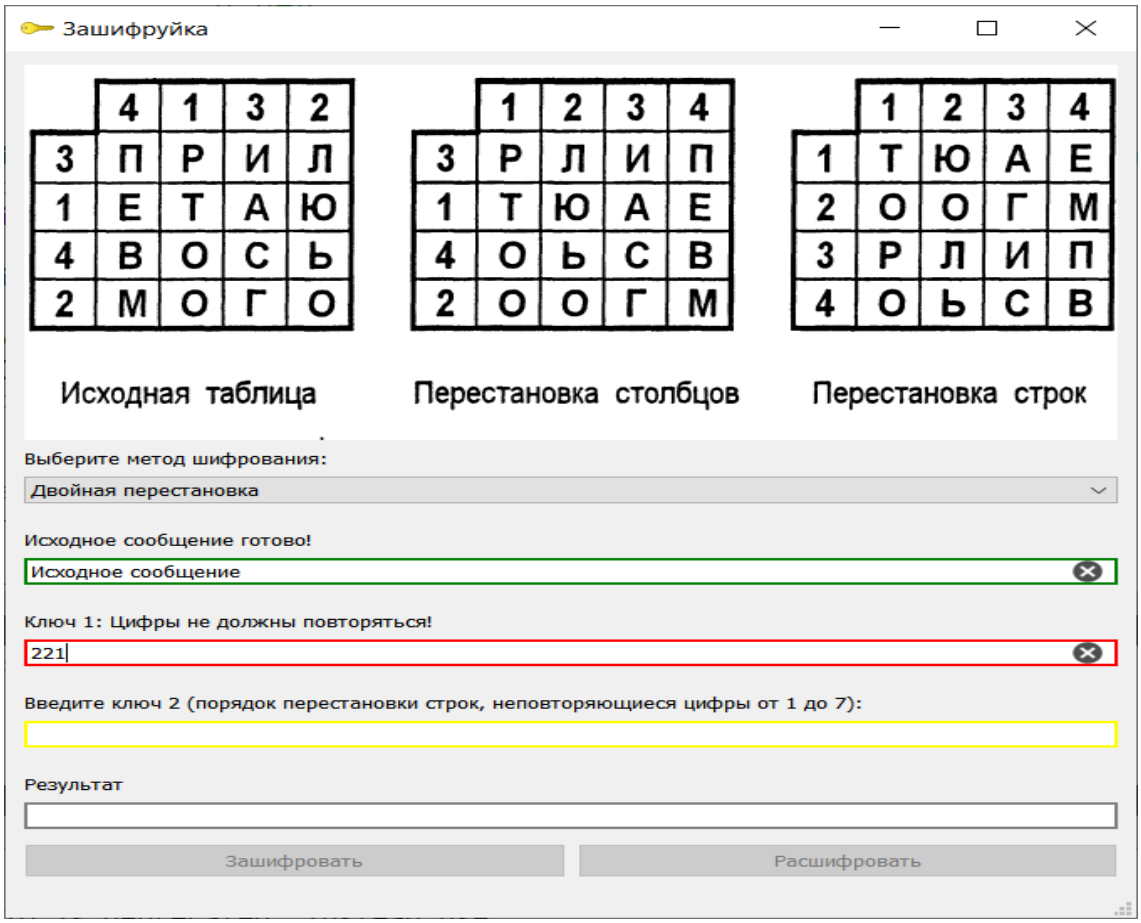

Рисунок 1 – скриншот работоспособности программы

В поле «Метод шифрования» необходимо выбрать один из методов. Каждая картинка соответствует определенному методу (на скриншоте картинка показывает пример работы двойной перестановки).

В поле «Исходное сообщение» необходимо ввести исходное сообщение. Минимальный и максимальный размер исходного сообщения зависят от выбранного метода. Поле подсвечивается зеленым цветом, если кол-во символов не меньше минимальной длины и желтым, если таковых недостаточно.

В поле «Ключ 1» необходимо ввести ключ для шифрования или дешифрования. В зависимости от выбранного метода длина ключа и кол-во допустимых символов могут отличаться. По этой же причине поле «Ключ 1» может быть не всегда доступно для введения символов (к примеру, для метода с использованием магического квадрата ключ не требуется). Поле подсвечивается зеленым цветом, если введенный ключ соответствует необходимым условиям, желтым, если кол-во символов меньше минимальной длины и красным, если не соответствует необходимым условиям помимо длины (например, в методе с использованием Шифрующих таблиц может быть пропущена цифра, либо вписана дважды).

Поле «Ключ 2» доступно только в том случае, если был выбран метод с использованием двойной перестановки, работает аналогично полю «Ключ 1».

Поле «Результат» содержит зашифрованное или расшифрованное сообщение. После нажатия кнопок «Расшифровать» или «Расшифровать» поле выводит результат работы выбранного метода, а также подсвечивается зеленым цветом на полторы секунды, чтобы сакцентировать внимание пользователя.

В полях «Исходное сообщение», «Ключ 1» и «Ключ 2» имеется возможность полностью удалить введенные символы. Для этого в соответствующем поле необходимо нажать на крестик в правой части.

Кнопки «Зашифровать» и «Расшифровать» доступны только тогда, когда введенные исходные данные соответствуют условиям выбранного метода.

В программе «Зашифруйка» поддерживается возможность изменить размеры своего окна. При изменении ширины окна также изменится ширина самих элементов. При изменении высоты окна изменится лишь высота картинки. Также доступен развернутый режим. Минимальный размер окна программы зависит от минимального размера картинки, соответствующей выбранному методу.

3. Организация данных

3.1. Организация входных данных

В качестве входных данных в программе используются целочисленные, буквенные и символьные значения, вводимые пользователем.

3.2. Организация выходных данных

Выходными данными в программе являются:

- Пользовательский интерфейс, а также пояснения на русском языке для упрощения навигации пользователя;
- Результат шифрования или дешифрования.

4. Технические и программные средства

4.1. Технические средства

Техническими средствами, необходимыми для запуска и штатного функционирования программы, являются:

- процессор с тактовой частотой не ниже 1,8 ГГц;
- не менее 512 Мб оперативной памяти;
- монитор SVGA с минимальным разрешением 800x600 пикселей;
- манипулятор типа «мышь» и клавиатура.

4.2. Программные средствами

Для разработки программы «Зашифруйка» необходим следующий инструментарий:

- Среда разработки Qt Creator 4.13.2 и комплект для сборки Qt 5.15.1 MSVC 2019 32 bit – платформа выбрана для использования языка C++ и библиотек Qt;
- операционная система MS Windows 7 или выше.

5. Результаты работы программы и их оценка

5.1. Объект испытаний

Объектом испытаний является программа «Зашифруйка».

Для проверки работоспособности была разработана система тестов, проверяющая основной функционал данной программы.

5.2. Цель испытаний

Целью испытаний данной программы является проверка работоспособности при ее эксплуатации пользователем с набором базовых навыков обращения с компьютером.

5.3. Требования к программе

Программа должна обладать достаточной степенью надежности, удобства визуальной части и тестируемостью.

5.4. Методы испытаний

Результаты тестирования программы приведены в Таблице 1.

Таблица 1 - Система испытаний работы программы

Назначение теста	Входные данные	Метод	Фактическая реакция программы
Проверка реакции программы на ввод пользователем исходного сообщения недостаточной длины	Рыбак	Скитала	Вывод предупреждения
Проверка реакции программы на ввод пользователем исходного сообщения, соответствующего условиям выбранного метода	Рыбаки	Скитала	Ожидание следующих действий

Продолжение Таблицы 1

Проверка реакции программы на ввод пользователем ключа, не соответствующего условию выбранного метода	314	Шифрующие таблицы	Вывод предупреждения
Проверка реакции программы на ввод пользователем ключа, соответствующего условию выбранного метода	312	Шифрующие таблицы	Ожидание следующих действий
Проверка реакции программы на ввод пользователем ключа, не соответствующего условию выбранного метода	55312	Двойная перестановка	Вывод предупреждения
Проверка реакции программы на ввод пользователем ключа, соответствующего условиям выбранного метода	14352	Двойная перестановка	Ожидание следующих действий
Проверка реакции программы на ввод пользователем исходного сообщения недостаточной длины	Рыба	Магический квадрат	Вывод предупреждения
Проверка реакции программы на ввод пользователем исходного сообщения, соответствующего условиям выбранного метода	Рыбак	Магический квадрат	Ожидание следующих действий
Проверка реакции программы на ввод пользователем исходного сообщения недостаточной длины	фильм	Полибианский квадрат	Вывод предупреждения
Проверка реакции программы на ввод пользователем исходного сообщения, соответствующего условиям выбранного метода	фильмы	Полибианский квадрат	Ожидание следующих действий
Проверка реакции программы на ввод пользователем исходного сообщения недостаточной длины	камни	Цезаря	Вывод предупреждения

Продолжение Таблицы 1

Проверка реакции программы на ввод пользователем исходного сообщения, соответствующего условиям выбранного метода	камень	Цезаря	Ожидание следующих действий
Проверка реакции программы на ввод пользователем ключа, не соответствующего условию выбранного метода	8	Гронсфельда	Вывод предупреждения
Проверка реакции программы на ввод пользователем ключа, соответствующего условию выбранного метода	89	Гронсфельда	Ожидание следующих действий
Проверка реакции программы на ввод пользователем ключа, не соответствующего условию выбранного метода	мы	Виженера	Вывод предупреждения
Проверка реакции программы на ввод пользователем ключа, соответствующего условию выбранного метода	мыши	Вижинера	Ожидание следующих действий
Проверка реакции программы на ввод пользователем исходного сообщения недостаточной длины	Я	Уитстона	Вывод предупреждения
Проверка реакции программы на ввод пользователем исходного сообщения, соответствующего условиям выбранного метода	я и ты	Уитстона	Ожидание следующих действий

5.5.Оценка результатов тестирования

Все испытания проведены успешно, результаты работы программы соответствуют ожидаемым.

Заключение

Программа выполнена в полном соответствии с поставленной задачей, была проверена и отлажена. Эксперименты показали состоятельность алгоритма. Программа полностью работоспособна.

Выполнение лабораторной работы помогло закрепить материал и знания, полученные на лекциях, а также были получены практические навыки в написании программной реализации простейших алгоритмов шифрования.

Список литературы

- Курс лекций по дисциплине «Защита информации» Коновалов К. А.;
- Руководство по «Qt Creator»

Ссылка на проект:

https://github.com/Akornilov1999/Trash/blob/master/Documents.7z