МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ

РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное образовательное учреждение

Высшего образования

«КРЫМСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ им. В.И. ВЕРНАДСКОГО»

ФИЗИКО-ТЕХНИЧЕСКИЙ ИНСТИТУТ

Кафедра компьютерной инженерии и моделирования

**РАЗРАБОТКА ЭМУЛЯТОРА ШИФРОВАЛЬНОЙ МАШИНЫ «ЭНИГМА»**

Курсовая работа

По дисциплине программирование

Студента 1 курса группы ИВТ-б-о-191(2)

Тройслит Андрея Александровича

Направления подготовки 09.03.01 «Информатика и вычислительная техника»

|  |  |  |
| --- | --- | --- |
| Научный руководитель  Старший преподаватель кафедры  Компьютерной инженерии и моделирования | \_\_\_\_\_\_\_\_\_\_\_\_\_\_  (оценка)  \_\_\_\_\_\_\_\_\_\_\_\_\_\_  (подпись,дата) | Чабанов В.В. |

Симферополь 2020

# **Реферат**

Разработка симулятора шифровальной машины «Энигма» .- Симферополь: ФТИ КФУ им В.И.ВЕРНАДСКОГО, 2019, стр.,

*Объект разработки* – компьютерная программа создающая симуляцию шифровальной машины Энигма.

*Цель работы* – создать программу, дающую возможность шифрования сообщений по принципу шифрования Энигмы ,использующей принцип шифрования Джефферсона и шифра Цезаря.

Рассмотрены основные принципы шифрования Энигмы, изучены возможности для написания кода и его визуализации.

Ключевые слова: ПРОГРАММИРОВАНИЕ, ШИФРОВАНИЕ, C++, ЭНИГМА, VISUALSTUDIO, WINDOWSFORMS, ШИФРАТОР ДЖЕФФЕРСОНА, ШИФР ЦЕЗАРЯ

# **Оглавление**

[**Реферат** 2](#_Toc67573947)

[**Оглавление** 3](#_Toc67573948)

[**Введение** 4](#_Toc67573949)

[**Глава 1 Постановка задачи** 5](#_Toc67573950)

[**1.1 Цель проекта:** 5](#_Toc67573951)

[**1.2 Аналоги такого проекта:** 5](#_Toc67573952)

[**1.3 Техническая часть** 5](#_Toc67573953)

[**1.3.1 Требования к данному симулятору:** 5](#_Toc67573954)

[**1.3.2 Требования к алгоритмам шифрования:** 5](#_Toc67573955)

[**1.3.3 Требования к параметрам запуска данного симулятора:** 5](#_Toc67573956)

[**Глава 2 Программная реализация симулятора** 7](#_Toc67573957)

[**2.1 Анализ используемых инструментов** 7](#_Toc67573958)

[**2.2 Использованные фреймворки (платформы для написания кода):** 7](#_Toc67573959)

[**2.3 Описание алгоритма шифрования:** 7](#_Toc67573960)

[**Глава 3 Тестирование проекта** 9](#_Toc67573961)

[**3.1 Первое тестирование.** 9](#_Toc67573962)

[**Глава 4 Дальнейшее развитие проекта** 10](#_Toc67573963)

[**4.1 Перспективы развития в техническом направлении:** 10](#_Toc67573964)

[**Заключение** 11](#_Toc67573965)

[**Литература** 13](#_Toc67573966)

# **Введение**

Целью данной работы, как было уже сказано выше является закрепление навыков работы с языком программирования С++, получение навыки по работе с методами шифрования и дешифрования информации, изучение методов визуализации с помощью WindowsForms в среде разработки VisualStudio.

В настоящее время секретность информации играет большую роль. Для скрытия информации от посторонних глаз, люди часто прибегают к каким- либо методам шифрования.

Зашифрованная информация позволяет людям более безопасно общаться между собой, а также сохраняет данные пользователей. Проект симулятора шифровальной машины позволит людям взглянуть на один из способов шифрования информации, который был особенно популярен примерно половину века назад.

Задачи которые необходимо решить для разработки данного приложения:

* Изучение WindowsForms для создания интерфейса программы, и последующей визуализации.
* Изучение принципа шифратора Джефферсона и шифра Цезаря для создания шифратора Энигмы.
* Подробное изучения языка программирования C++.

# **Глава 1 Постановка задачи**

## **1.1 Цель проекта:**

Конечная версия программы сможет зашифровать текст, предложенный пользователем, достаточно сильным алгоритмом, для взлома которого, без известного ключа, понадобиться достаточно большое время, прежде чем можно будет прочитать изначально зашифрованное сообщение.

## **1.2 Аналоги такого проекта:**

* Сайт <https://cryptii.com/pipes/enigma-decoder> полностью реализующий шифровальную машину Энигма в онлайн формате.
* Физические аналоги шифровальной машины Энигмы.

## **1.3 Техническая часть**

### **1.3.1 Требования к данному симулятору:**

* Возможность зашифровать сообщения с известным ключом шифрования.
* Возможность зашифровать сообщения без известного ключа шифрования.
* Возможность расшифровать сообщения с известным ключом шифрования

### **1.3.2 Требования к алгоритмам шифрования:**

* Алгоритм шифрования программы должен быть аналогичным тому, который используется в физическом аналоге шифровальной машины Энигма.
* Возможность менять ключ для шифровки, не прибегая к перезапуску программы

### **1.3.3 Требования к параметрам запуска данного симулятора:**

* Операционная система Windows, с версией начиная от Windows 7.
* Оперативная память 512 Мб
* Физическая память – 10 Мб

# **Глава 2 Программная реализация симулятора**

## **2.1 Анализ используемых инструментов**

Языки программирования, которые были использованы для создания данного эмулятора:

* С++, основной язык программирования, на котором написана большая часть работы. Он позволяет удобно реализовывать алгоритмы обработки данных, что является первостепенной задачей в текущем проекте.
* WindowsForms, дополнительное программное обеспечение, позволяющее без особых усилий нарисовать интерфейс программы, который будет легко понятен пользователю.

## **2.2 Использованные фреймворки (платформы для написания кода):**

* VisualStudio 2019 –в ходе выбора платформы был выбор между VisualStudio и QT, однако в конечном итоге была выбрана именно VisualStudio из-за своего понятного интерфейса, возможности работы с разными языками, а также опыта работы с данной программой, что при написании большой и сложной работы играет немаловажную роль.

## **2.3 Описание алгоритма шифрования:**

Для шифрования текста, в шифровальной машине «Энигма», используется два принципа шифрования, один из них - шифратор Джефферсона, а другой называется шифром Цезаря. О принципах их шифрования, будет рассказано далее.

Для шифрования текста используется устройство шифратора Джефферсона(Рис.2.3.1) - это устройство представляло собой несколько дисков, на которых нанесены буквы алфавита, идущие в случайном порядке. Для проведения шифровки сообщения, изначальный текст разбивается на части по 36 букв в каждой, после этого, на первом диске выбирается первая буква из набора, которая не стоит прямо на цилиндрах, после на втором диске ищется вторая буква по той-же линии, и по такой аналогии выстраивались оставшиеся 34 буквы. После выставления, таким образом, набора букв сообщения, собеседнику передавали код, состоящий из набора букв, который ему необходимо было выставить на цилиндрах, и после этого искать в остальных линиях осмысленное сообщение.

Кроме шифратора Джефферсона, в шифровальной машине «Энигма», используется шифр Цезаря (Рис.2.3.2), смысл которого заключается в смещении каждой буквы. Например, вместо буквы А**,** будет идти буква **В**, таким образом, полученное смещение будет составлять 2 буквы, т.е. буква **Б** будет заменена на букву **Г,** и по такой аналогии, будет подвергаться шифровке весь оставшийся текст.

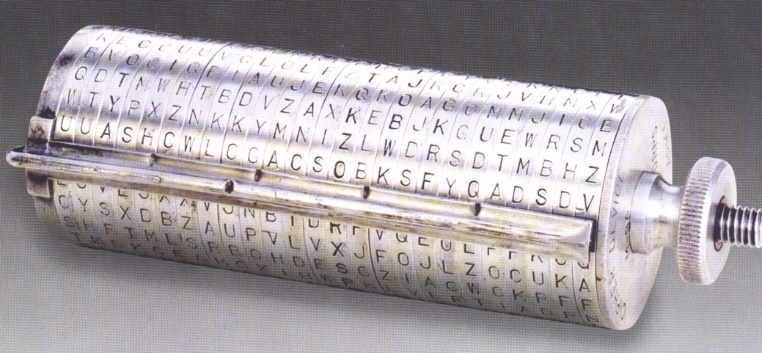


Рисунок 2.3.1 Шифратор Джефферсона

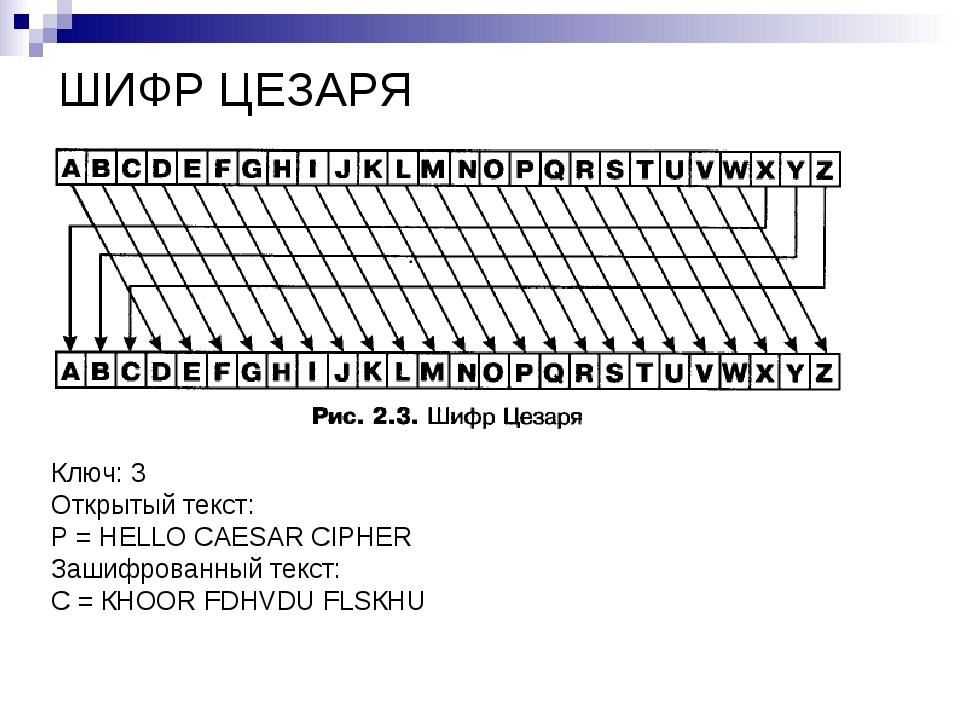


Рисунок 2.3.2 Шифрование Цезаря

# **Глава 3 Тестирование проекта**

## **3.1 Первое тестирование.**

Первое версия программы шифровальной машины была отправлена на тестирование 12.04.2020. На следующий день, 13.04.2020, был получен следующий отчет:

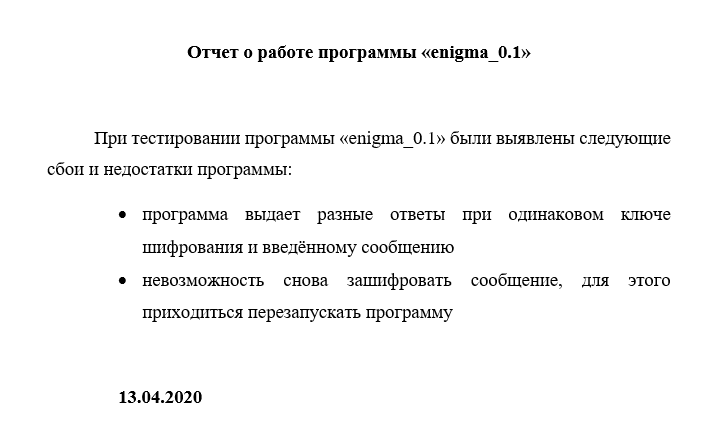


Рис.3.1.1 отчет по первому тестированию

Исходя из полученного отчета, были проведены работы по улучшению программы, в частности была добавлена возможность вновь зашифровать сообщение, без необходимости перезапуска программы.

## **3.2 Второе тестирование**

Вторая версия программы с исправленным способом повторного шифрования была отправлена на тестирование 20.04.2020. Через несколько дней, 23.04.2020, был получен новый отчет о работе программы:

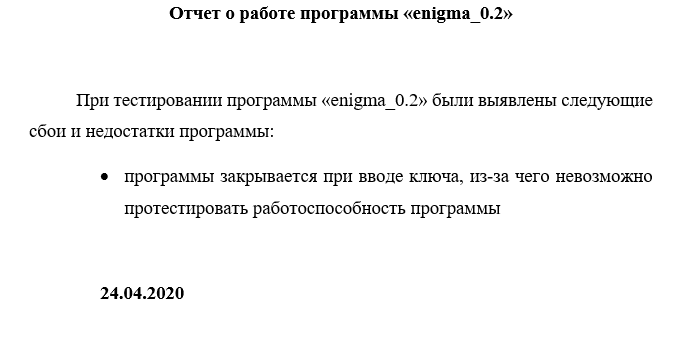


Рис.3.2.1 отчет по второму тестированию программы

Исходя из полученного ответа, была проведена работа по восстановлению работоспособности программы. После восстановления работоспособности, программа была отправлена на повторное тестирование.

Результат повторного тестирования:

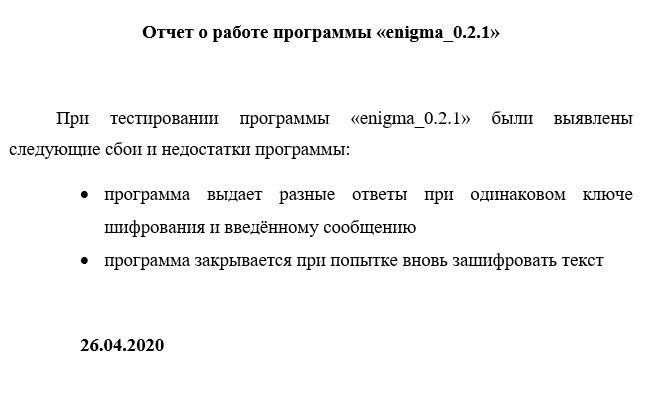


Рис.3.2.2 отчет по повторному тестирования второй версии программы

Исходя из полученных результатов, была устранена ошибка, при которой программа каждый раз выдавала разный шифрованный текст, при одинаковом ключе шифрования и введенному тексту.

## **3.3 Третье тестирование программы**

Третья версия программы была отправлена на тестирование 1.05.2020. Через несколько дней, 4.05.2020 был получен следующий отчет:

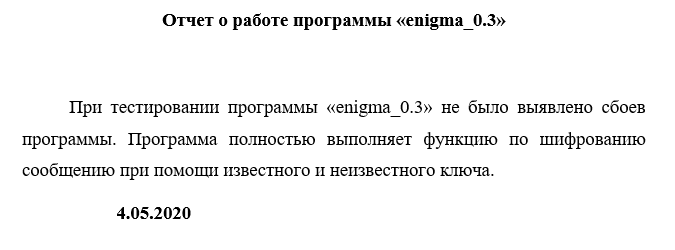


Рис.3.3.1 третье тестирование программы

Как видно из результатов тестирования программа оказалось полностью готова.

# **Глава 4 Дальнейшее развитие проекта**

## **4.1 Перспективы развития в техническом направлении:**

* Добавить дополнительные роторы для большего качества шифрования информации.
* Добавить другие языки, на которых может осуществляться шифрование.
* Реализовать приложение в виде web-сайта, для возможности использования шифратора без необходимости скачивания программы на свой ПК.
* Добавить возможность шифрования в реальном времени, т.е. при каждая буква будет сразу шифроваться без необходимости ввода полноценного предложения.
* Создать клиент-серверную систему для использования данного алгоритма в виде шифрования сообщений, для развлекательных целей, либо для передачи какой-либо важной информации.
* Усовершенствовать графический интерфейс.

При добавлении вышеперечисленных пунктов, эмулятор сможет составить полноценную конкуренцию остальным электронным приложениям в Web-среде. Возможно, больше людей заинтересуется способами шифрования и защиты информации, и смогут расширить свои знания о криптографии – науки о шифровании сообщений.

# **Заключение**

В ходе выполнения курсовой работы были получены навыки работы с C++, визуализации программ с помощью WindowsForms и их кастомизации в произвольной форме.

Был изучен принцип шифрования реальных аналогов Энигмы, и возможность воссоздать симулятор такой машины с аналогичным принципом шифрования.

Был разработан симулятор Энигмы, который позволяет зашифровывать сообщения с достаточным уровнем защиты, и предусматривает реальный прототип, т.е. получатель не сможет быстро расшифровать сообщения, не имея специального ключа.

При создании данного симулятора я обращал внимание на недостатки реального аналога, например, возможность заклинивания механизма шифрования. На практике могла бы получиться неловкая ситуация, когда необходимо срочно зашифровать сообщение, но устройство вышло из строя. В случае программы, можно просто перезапустить приложение, что займет гораздо меньше времени, чем починка шифровальной машины. Также программа не подвержена износу, что также является большим преимуществом перед физической копией.

Однако программа не может быть идеальна, данный случай не исключение. Например, для замены роторов необходимо дописывать дополнительный код, в то время как в механизме можно потратить гораздо меньше времени, и данная проблема должна быть решена быстрее всего.

Разработанный симулятор выполняет базовые функции реального механизма, а именно – шифрование и дешифрование информации. Однако данной программе еще далеко до полноценного эмулятора, который бы выполнял все функции, которые может предложить реальный механизм.

В ближайшем будущем, планируется добавить возможность шифрования на разных языках, дополнительные роторы для надежности шифрования.

В конечном виде программа должна будет принять вид небольшого окна, в котором можно будет с легкостью зашифровать сообщение на разных языках,

# **Литература**

1. Уроки по программирования с помощью WindowsForms с YouTube канала «FPS FirePlanetStudio» [Электронный ресурс  
<https://www.youtube.com/watch?v=WHF8mtnJnl0>]

2.Статья о принципе шифрования Энигмы [Электронный ресурс <https://habr.com/ru/post/217331/>]

3.Курс уроков по C++ [Электронный ресурс <https://www.youtube.com/watch?v=kRcbYLK3OnQ&list=PLQOaTSbfxUtCrKs0nicOg2npJQYSPGO9r>]

4.Объяснение принципа работы шифратора Джефферсона [Электронный ресурс <http://hijos.ru/2014/01/15/dzhefferson-shifrovalshhik/>]

5.Обзор других методов шифрования информации [Электронный ресурс <https://scienceforum.ru/2016/article/2016019504>]

6. Объяснение принципа совместной работы шифратора Джефферсона и кода Цезаря в машине «Энигма» [Электронный ресурс <https://oyla.xyz/article/kod-enigmy> ]