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 СИМУЛЯТОРА 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.

ПРОГРАММИРОВАНИЕ, ШИФРОВАНИЕ, C++, ЭНИГМА, VISUAL STUDIO, WINDOWSFORMS, ШИФРАТОР ДЖЕФФЕРСОНА, ШИФР ЦЕЗАРЯ

**Оглавление**

[Введение 4](#_Toc43761524)

[Глава 1 Постановка задачи 5](#_Toc43761525)

[1.1 Цель проекта: 5](#_Toc43761526)

[1.2 Аналоги такого проекта: 5](#_Toc43761527)

[1.3 Техническая часть 5](#_Toc43761528)

[1.3.1 Требования к данному симулятору: 5](#_Toc43761529)

[1.3.2 Требования к алгоритмам шифрования: 5](#_Toc43761530)

[1.3.3 Требования к параметрам запуска данного симулятора: 5](#_Toc43761531)

[Глава 2 Программная реализация симулятора 6](#_Toc43761532)

[2.1 Анализ используемых инструментов 6](#_Toc43761533)

[2.2 Использованные фреймворки (платформы для написания кода): 6](#_Toc43761534)

[2.3 Описание алгоритма шифрования: 6](#_Toc43761535)

[Глава 3 Дальнейшее развитие проекта 8](#_Toc43761536)

[3.1 Перспективы развития в техническом направлении: 8](#_Toc43761537)

[Заключение 9](#_Toc43761538)

[Литература 10](#_Toc43761539)

# **Введение**

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.

Целью данного проекта является получение навыков по работе с методами шифрования а также изучение методов визуализации с помощью c++.

Задачи которые необходимо решить для разработки:

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

# **Глава 1 Постановка задачи**

## **1.1 Цель проекта:**

Конечная программа сможет зашифровать текст предложенный пользователем достаточно сильным алгоритмом, для взлома которого понадобиться достаточное время, прежде чем можно будет прочитать изначальное сообщение.

## **1.2 Аналоги такого проекта:**

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

## **1.3 Техническая часть**

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

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

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

* Алгоритм шифрования должен быть такой-же как и в физическом аналоге машины Энигма.
* Возможность менять ключ для шифровки.

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

* Операционная система Windows, с версией начиная от Windows 7.

# **Глава 2 Программная реализация симулятора**

## **2.1 Анализ используемых инструментов**

Языки программирования использованные для создания данного симулятора:

* С++, основной язык на котором написана большая часть работы, позволяет удобно реализовывать алгоритмы обработки данных
* Windows Forms, дополнительное ПО, позволяющее легко нарисовать интерфейс программы.

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

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

## **2.3 Описание алгоритма шифрования:**

Для шифрования текста используется шифратор Джефферсона - это несколько дисков на которых нанесены буквы алфавита идущие в случайном порядке, для шифровки сообщения, изначальный текст разбивается на части по 36 букв в каждой, после на первом диске выбирается первая буква из набора, после на втором диске ищется вторая буква из той-же части, и так-же 36 буквы, после выставления таким образом сообщения собеседнику передавали код который ему необходимо было выставить на цилиндрах, и после этого искать в остальных линиях осмысленное сообщение. Кроме шифратора Джефферсона используется шифр Цезаря который заключается в смещении букв, например, вместо буквы **А** будет буква **В**, таким образом смещение составляет 2 буквы, т.е. **Б** будет заменена на **Г** и так весь оставшийся текст.

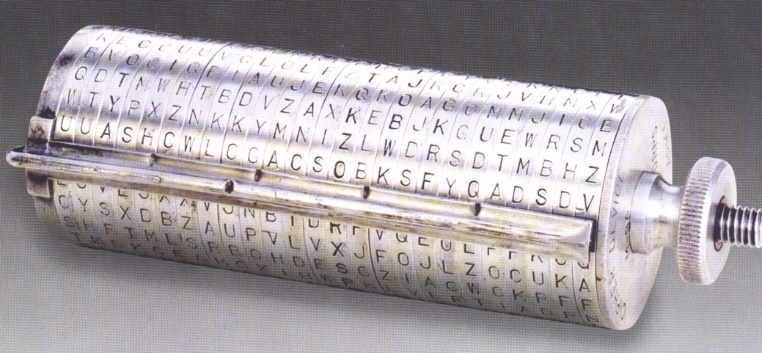


Рисунок 2.3.1 Шифратор Джефферсона

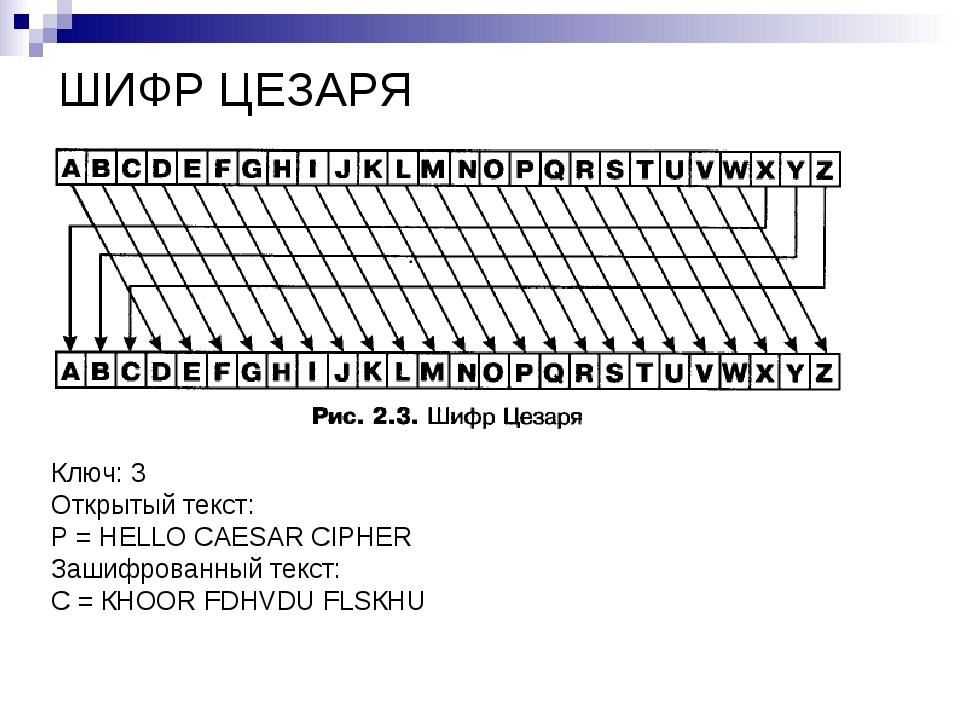


Рисунок 2.3.2 Шифрование Цезаря

# **Глава 3 Дальнейшее развитие проекта**

## **3.1 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 на свой ПК.
* Добавить возможность шифрования в реальном времени.
* При помощи сервера создать web-сайт для использования данного алгоритма в виде шифрования сообщений, для развлекательный целей, либо для передачи какой-либо важной информации.
* Усовершенствовать графический интерфейс.

При добавлении вышеперечисленных пунктов, симулятор сможет составить конкуренцию остальным приложениям. Возможно, больше людей заинтересуется способами шифрования текста 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.

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

Был разработан симулятор Энигмы позволяющий зашифровывать сообщения с достаточным уровнем защиты, который 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, невозможность заклинивания данной программы. 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.

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

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

# **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>]