Министерство образования Республики Беларусь
Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники»

Факультет компьютерных систем и сетей

Кафедра информатики

Дисциплина: Информационные сети. Основы безопасности

ОТЧЁТ
к лабораторной работе №2
на тему

ШИФРЫ ЦЕЗАРЯ И ВИЖЕНЕРА

Выполнил: студент гр.253504
Фроленко К.Ю.
Проверил: ассистент кафедры информатики
Герчик А.В.

Минск 2025

СОДЕРЖАНИЕ

1 ФОРМУЛИРОВКА ЗАДАЧИ

В данной работе необходимо разработать программное средство для шифрования и дешифрования текстовых файлов с использованием Шифра Цезаря и Шифра Виженера. Реализация должна обеспечивать возможность обработки текстовых данных в удобной форме, позволяя пользователю выбирать метод шифрования, указывать параметры кодирования и получать результат в наглядном виде.

Шифр Цезаря должен позволять задавать величину сдвига, которая определяет, на сколько позиций будет смещен каждый символ исходного текста в алфавите. Для Шифра Виженера необходимо реализовать механизм работы с ключом, который определяет последовательность сдвигов для шифрования и расшифрования текста. Оба метода должны поддерживать работу с русским и английским алфавитами, учитывать регистр символов и корректно обрабатывать неалфавитные символы, оставляя их без изменений.

Программа должна обеспечивать возможность загрузки текста из файлов и сохранения обработанных данных, что позволит избежать необходимости ввода текста вручную. Графический интерфейс должен предоставлять удобные средства выбора алгоритма, задания параметров и управления процессом обработки данных. Важно, чтобы пользователь мог интуитивно взаимодействовать с приложением, легко переключаясь между методами шифрования и дешифрования, а также выбирать необходимые параметры без сложных настроек.

Дополнительно необходимо предусмотреть обработку ошибок, связанных с некорректными входными данными, и реализовать систему уведомлений для информирования пользователя о ходе выполнения операций. Реализация должна быть удобной, надежной и обеспечивать корректную работу алгоритмов в различных сценариях использования.

2 ХОД РАБОТЫ

Для реализации программного средства шифрования и дешифрования текстовых файлов разработано графическое приложение, позволяющее пользователю выбирать метод шифрования, задавать параметры, загружать текстовые файлы и сохранять обработанные данные. Приложение поддерживает два алгоритма: Шифр Цезаря и Шифр Виженера, а также работу с текстами на русском и английском языках.

Графический интерфейс включает элементы для выбора метода шифрования, переключения между режимами шифрования и дешифрования, задания параметров, загрузки входного файла и сохранения результата. Визуальное представление интерфейса программы приведено на Рисунке 1.

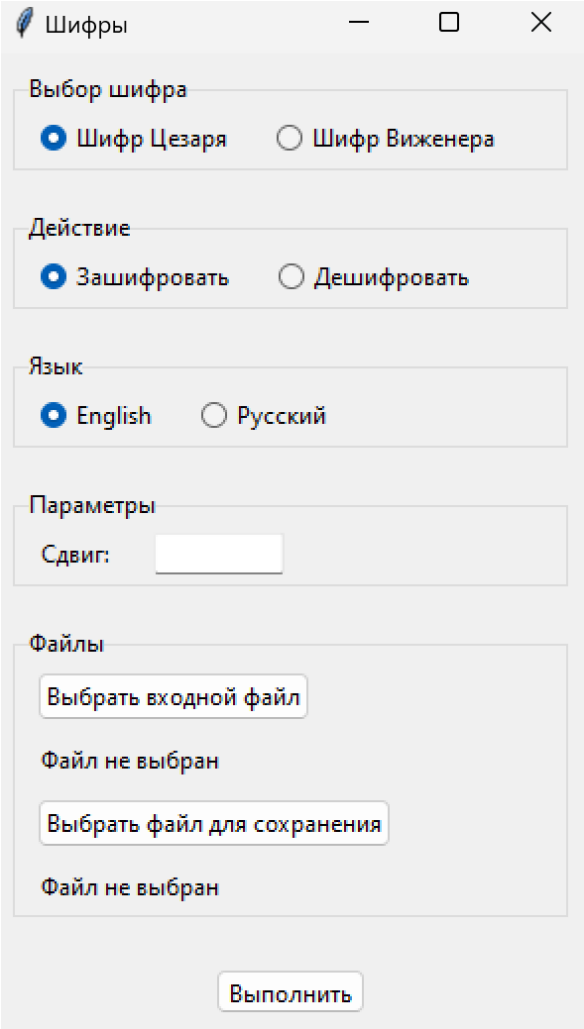

Рисунок 1 – Интерфейс программы для работы с шифрами

В основе работы Шифра Цезаря лежит сдвиг символов входного текста на указанное пользователем количество позиций в пределах выбранного алфавита. Для шифрования и дешифрования текста разработаны функции *caesar_encrypt* и *caesar_decrypt*, выполняющие преобразование символов. В

процессе обработки текста символы латинского или кириллического алфавита изменяются в соответствии с указанным сдвигом, а остальные символы, такие как цифры, пробелы и знаки препинания, остаются неизменными.

Шифр Виженера использует заданное пользователем ключевое слово, определяющее последовательность сдвигов для каждого символа текста. Реализованы функции *vigenere_encrypt* и *vigenere_decrypt*, которые выполняют кодирование и декодирование с учетом ключа. Данный метод позволяет использовать более сложный способ шифрования, так как каждый символ текста заменяется другим символом с учетом соответствующего сдвига, вычисляемого на основе ключевого слова.

Для удобства работы с текстовыми файлами в программу добавлены функции загрузки входного текста из файла и сохранения обработанного текста в новый файл. Это позволяет пользователю работать с шифрованием и дешифрованием без необходимости ввода текста вручную.

На Рисунке 2 представлен пример работы программы. Исходный текст был зашифрован с помощью Шифра Виженера с заданным ключевым словом, а затем успешно расшифрован обратно, что подтверждает корректность работы алгоритмов.

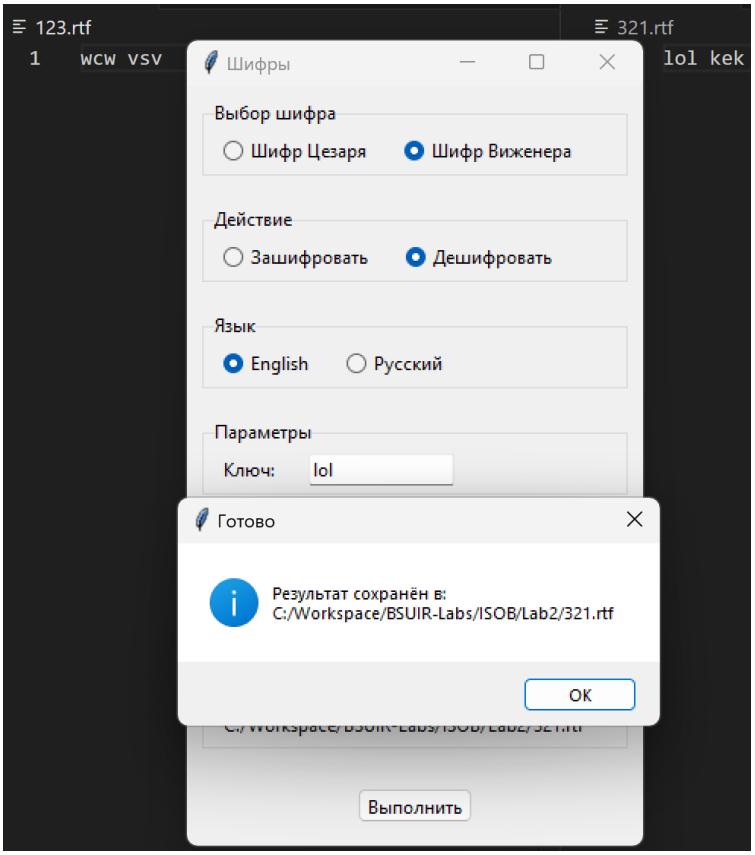

Рисунок 2 – Пример работы программы

ЗАКЛЮЧЕНИЕ

В ходе данной работы было разработано программное средство для шифрования и дешифрования текстовых файлов с использованием Шифра Цезаря и Шифра Виженера. Реализация обеспечила возможность выбора метода шифрования, задания параметров, загрузки и сохранения текстовых данных, а также интуитивно понятное управление процессом обработки.

На первом этапе была определена архитектура программы, выбраны основные алгоритмы и реализован графический интерфейс, позволяющий пользователю взаимодействовать с программой без необходимости работы с командной строкой. Далее был разработан алгоритм Шифра Цезаря, который выполняет сдвиг символов в пределах алфавита на заданное пользователем число позиций, а затем добавлена поддержка Шифра Виженера, использующего ключевое слово для формирования последовательности сдвигов. Оба метода корректно работают с русским и английским языками, учитывают регистр символов и сохраняют неизменными неалфавитные символы.

Для удобства работы реализована возможность загрузки входного текста из файла и сохранения результата в отдельный файл. В процессе тестирования проверена работоспособность обоих методов шифрования и дешифрования, корректность обработки различных языков и символов, а также работоспособность программы при вводе различных параметров. Дополнительно была добавлена система уведомлений, позволяющая информировать пользователя об ошибках и ходе выполнения операций.

Таким образом, поставленная задача была успешно выполнена. Программа позволяет эффективно выполнять шифрование и расшифровку текстовых данных, корректно обрабатывает входные параметры и обеспечивает удобство работы за счет графического интерфейса. Полученные результаты подтверждают надежность реализации и соответствие требованиям, предъявленным к функционалу программного средства.