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

**ЭЛЕМЕНТЫ КРИПТОГРАФИИ**

Выполнил: студент гр.253504 Давыдовский Д.В.

Проверил: ассистент кафедры информатики Герчик А.В.

Минск 2025

**СОДЕРЖАНИЕ**

[1 Цель работы 3](#_Toc188986632)

[2 Ход работы 4](#_Toc188986633)

[Заключение 5](#_Toc188986634)

# 1 ЦЕЛЬ РАБОТЫ

Цель работы – реализовать программные средства шифрования и дешифрования текстовых файлов при помощи шифра Цезаря (шифра сдвига, кода Цезаря) и шифра Виженера, а также сделать данный продукт удобным для эксплуатации пользователями.

В ходе работы необходимо разработать приложение, позволяющее пользователям безопасно шифровать и расшифровывать текстовые файлы. Основной акцент будет сделан на использовании классических методов шифрования – шифра Цезаря и шифра Виженера, что обеспечит простоту реализации и понимания принципов работы алгоритмов. Разработка программного продукта должна учитывать удобство интерфейса и интуитивно понятное управление, что сделает его доступным даже для пользователей без специальных технических знаний.

На первом этапе необходимо детально изучить алгоритмы шифра Цезаря и шифра Виженера, их принципы работы, сильные и слабые стороны. Затем следует разработка архитектуры программы, включающей модули для шифрования, дешифрования, обработки текстовых данных и управления ключами. Также важно реализовать гибкие настройки, позволяющие пользователю выбирать метод шифрования, задавать параметры сдвига или ключа, а также работать с различными текстовыми файлами.

Следующим этапом является непосредственная реализация программы, включающая написание кода, тестирование на различных входных данных, отладку и оптимизацию. Программа должна корректно обрабатывать символы различных алфавитов, поддерживать работу с разными типами кодировок и обеспечивать надежную защиту данных.

# 2 ХОД РАБОТЫ

В ходе выполнения поставленной задачи, было реализовано три метода шифрования и дешифрования, которые соответствуют условию задачи. Разберём каждый из них.

Шифр сдвига представляет собой алгоритм шифрования при которой каждая буква заменяется буквой, стоящей через *n* позиций от текущей. В программном продукте была реализована поддержка русского языка, поэтому основополагающей задачей для реализации этого алгоритма, являлось определение принадлежности к одному из языков (русскому или английскому), в добавок стоило также проверять является ли буква заглавной или строчной. Чтобы найти какой символ, соответствует текущему в зашифрованном виде, мы находили позицию текущего символа в алфавите (для этого мы и определяли является ли буква заглавной или нет), после нахождения позиции мы добавляли к ней смещение и брали остаток от деления на 26(в случае же с русским языком, остаток от деления на 32), чтобы оставаться в пределах алфавита, и далее, полученное значение, преобразовывали в символ.

Код Цезаря представляет собой частный случай шифра сдвига. В нём каждая буква заменяется буквой, стоящей в 3 позициях от текущей. Алгоритм вычисления зашифрованного символа остаётся таким же, как и в случае с шифром сдвига.

Шифр Виженера представляет собой более продвинутый метод шифрования по сравнению с шифром Цезаря, поскольку использует многоалфавитную замену. В отличие от простого шифра сдвига, где каждая буква заменяется на одну и ту же сдвинутую букву, Виженер применяет ключевое слово, которое определяет последовательность сдвигов. Без учета шифрования с использованием ключевого слова, алгоритм нахождения зашифрованного символа, соответствующему текущему, остался почти неизменным. На рисунке 1 представлен результат работы программы.

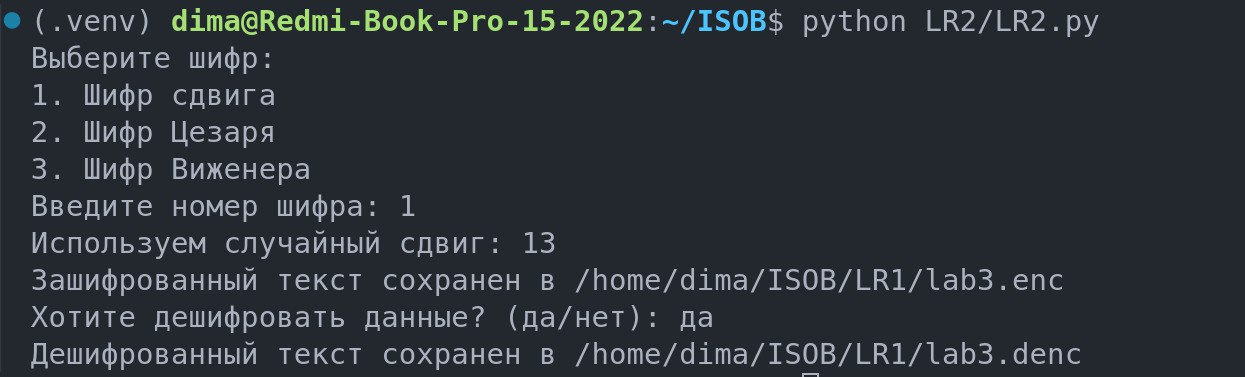


Рисунок 1 – Результат работы программы

# ЗАКЛЮЧЕНИЕ

В ходе работы был выяснен принцип работы шифра Цезаря и шифра Виженера, что позволило реализовать программу для шифрования и дешифрования текстовых файлов с использованием этих подходов. Подробное изучение алгоритмов дало возможность учесть их особенности, такие как чувствительность к регистру, работу с пробелами, специальными символами и поддержку различных языков. Реализованные методы шифрования обеспечивают корректную обработку текста, сохраняя исходную структуру и читабельность.

Также были разработаны вспомогательные функции, значительно повышающие удобство использования программы. Среди них – интерактивное окно для открытия и сохранения файлов, позволяющее пользователям быстро загружать и сохранять зашифрованные или расшифрованные документы в удобном формате. Данная функция поддерживает выбор директорий, фильтрацию файлов по расширениям и отображение последних открытых файлов для ускоренного доступа.

Дополнительно было реализовано интерактивное меню, которое предоставляет пользователю возможность выбора способа шифрования с удобным вводом ключевых переменных. Например, для шифра Цезаря предусмотрен механизм установки значения сдвига, а для шифра Виженера – удобный ввод ключевого слова с проверкой его корректности. Пользователь может в режиме реального времени увидеть изменения текста, что позволяет оценить результат шифрования перед сохранением.

Таким образом, в ходе выполнения работы была создана программа, обеспечивающая надежное шифрование и дешифрование текстовых файлов с использованием шифра Цезаря и шифра Виженера. Реализованные вспомогательные функции делают продукт удобным для использования, а система обработки ошибок и интерактивный интерфейс повышают его надежность и функциональность. Итоговая версия программы готова к эксплуатации и может быть использована как для личных целей, так и в образовательных процессах для изучения основ криптографии.