Министерство образования Республики Беларусь

Учреждение образования

«Белорусский государственный университет информатики и радиоэлектроники»

Факультет компьютерных систем и сетей

Кафедра программного обеспечения информационных технологий Дисциплина «Теория информации»

## ОТЧЁТ

к лабораторной работе №1

## ПРОСТЕЙШИЕ ШИФРЫ

Вариант 2

Студент гр. 451001 Яркович Е.Р. Преподователь: Болтак С.В.

**СОДЕРЖАНИЕ**

1. [Задание к лабораторной работе 3](#_bookmark0)
2. [Тестирование программы 3](#_bookmark1)
3. [Скриншоты, подтверждающие работу программы с файлами 6](#_bookmark2)

# Задание к лабораторной работе

Вариант 2.

Написать программу, которая выполняет шифрование и дешифрование текстового файла любого размера, содержащего текст на заданном языке, используя следующие алгоритмы шифрования:

* метод **«железнодорожной изгороди»,** текст на русском языке;
* алгоритм **Виженера, прогрессивный ключ,** текст на русском языке. Для всех алгоритмов ключ задается с клавиатуры пользователем.

Программа должна игнорировать все символы, не являющиеся буквами заданного алфавита, и шифровать только текст на заданном языке. Все алгоритмы должны быть реализованы в одной программе. Программа не должна быть написана в консольном режиме. Результат работы программы – зашифрованный/расшифрованный файл/ы. Кроме работы с файлами программа должна предоставлять ввод/вывод шифруемого текста с клавиатуры/на экран.

# Тестирование программы

* 1. Метод “Железнодорожной изгороди”

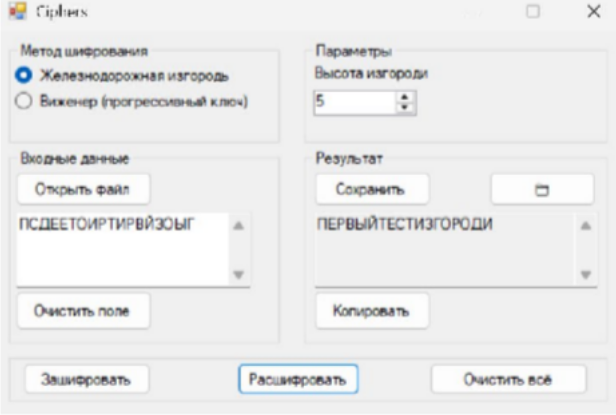
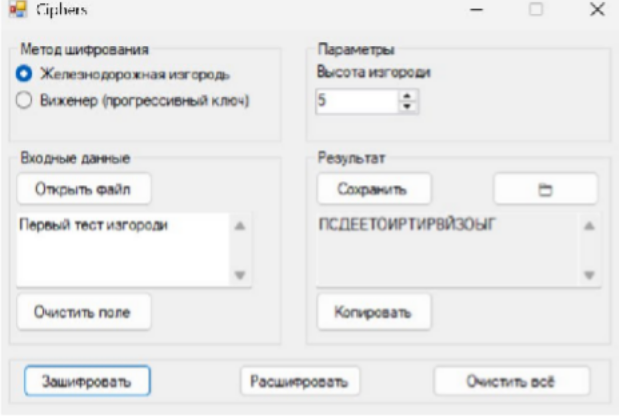


Рисунок 1.1 – тест №1

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| П |  |  |  |  |  |  |  | С |  |  |  |  |  |  |  | Д |  |
|  | Е |  |  |  |  |  | Е |  | Т |  |  |  |  |  | О |  | И |
|  |  | Р |  |  |  | Т |  |  |  | И |  |  |  | Р |  |  |  |
|  |  |  | В |  | Й |  |  |  |  |  | З |  | О |  |  |  |  |
|  |  |  |  | Ы |  |  |  |  |  |  |  | Г |  |  |  |  |  |

Исходный текст = “Первый тест изгороди” Высота изгороди = 5

Получаем следующий шифротекст = “ПСДЕЕТОИРТИРВЙЗОЫГ”

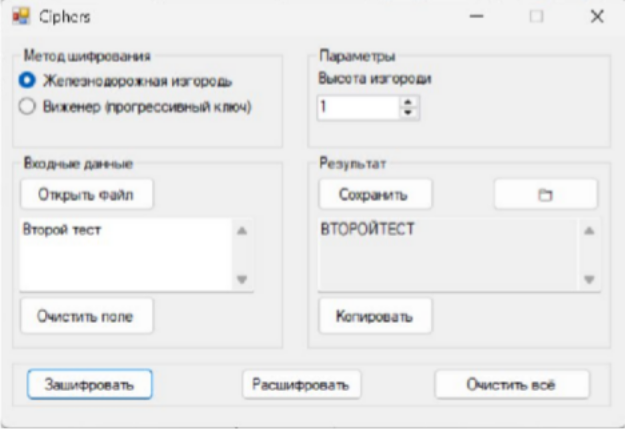
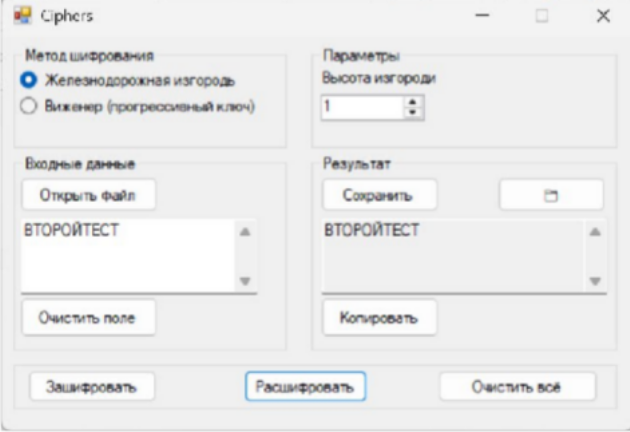
 

Рисунок 1.2 – тест №2

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| В | Т | О | Р | О | Й | Т | Е | С | Т |

Исходный текст = “Второй тест” Высота изгороди = 1

Получаем следующий шифротекст = “ВТОРОЙТЕСТ”

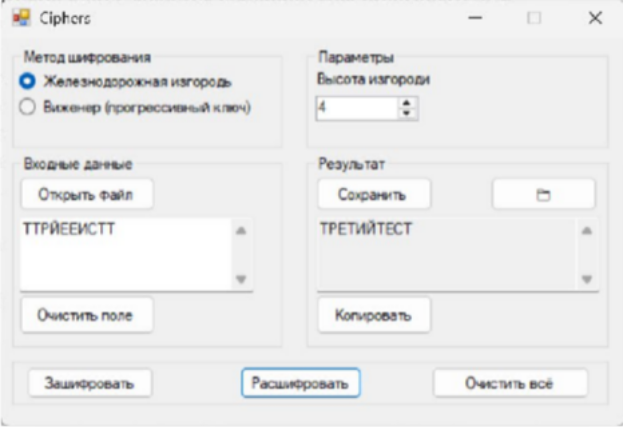
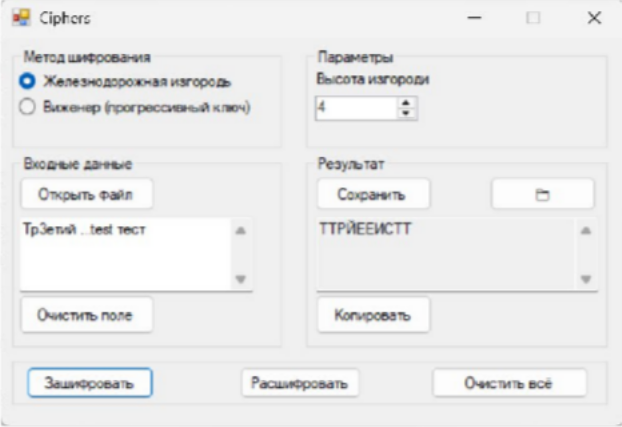


Рисунок 1.3 – тест №3

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Т |  |  |  |  |  | Т |  |  |  |
|  | Р |  |  |  | Й |  | Е |  |  |
|  |  | Е |  | И |  |  |  | С |  |
|  |  |  | Т |  |  |  |  |  | Т |

Исходный текст = “Тр3етий …test тест” Высота изгороди = 4

Получаем следующий шифротекст = “ТТРЙЕЕИСТТ”

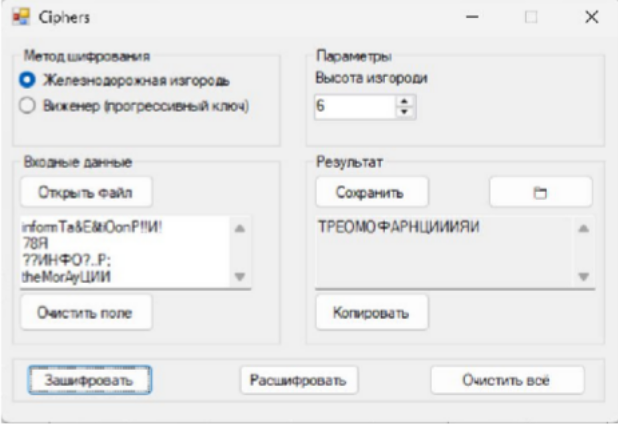
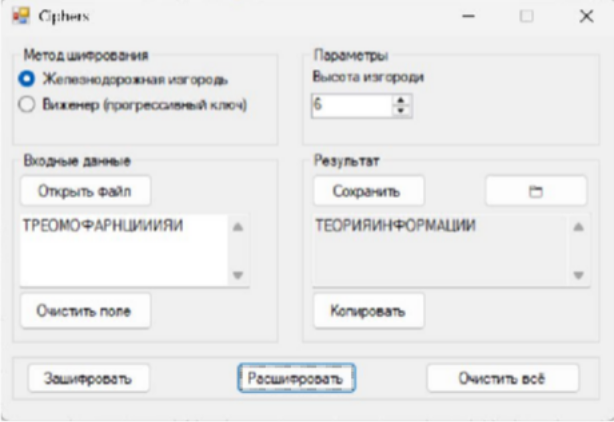
 

Рисунок 1.4 – тест №4

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Т |  |  |  |  |  |  |  |  |  | Р |  |  |  |  |  |
|  | Е |  |  |  |  |  |  |  | О |  | М |  |  |  |  |
|  |  | О |  |  |  |  |  | Ф |  |  |  | А |  |  |  |
|  |  |  | Р |  |  |  | Н |  |  |  |  |  | Ц |  |  |
|  |  |  |  | И |  | И |  |  |  |  |  |  |  | И |  |
|  |  |  |  |  | Я |  |  |  |  |  |  |  |  |  | И |

Исходный текст = “informТa&Е&tiОonР!!И!

## 78Я

## ??ИНФО?..Р;

theМorАyЦИИ” Высота изгороди = 6

Получаем следующий шифротекст = “ТРЕОМОФАРНЦИИИЯИ”

* 1. Алгоритм Виженера (прогрессивный ключ)

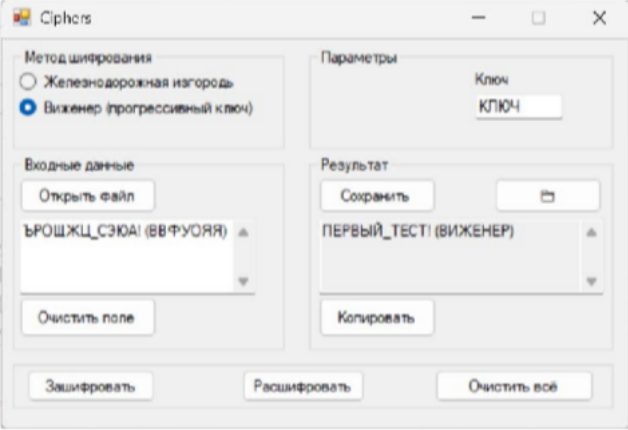
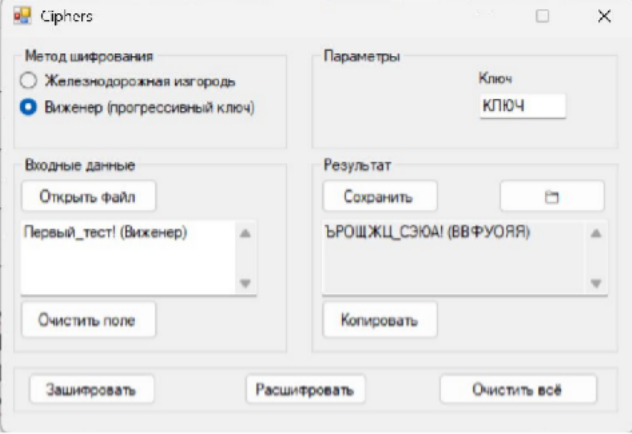
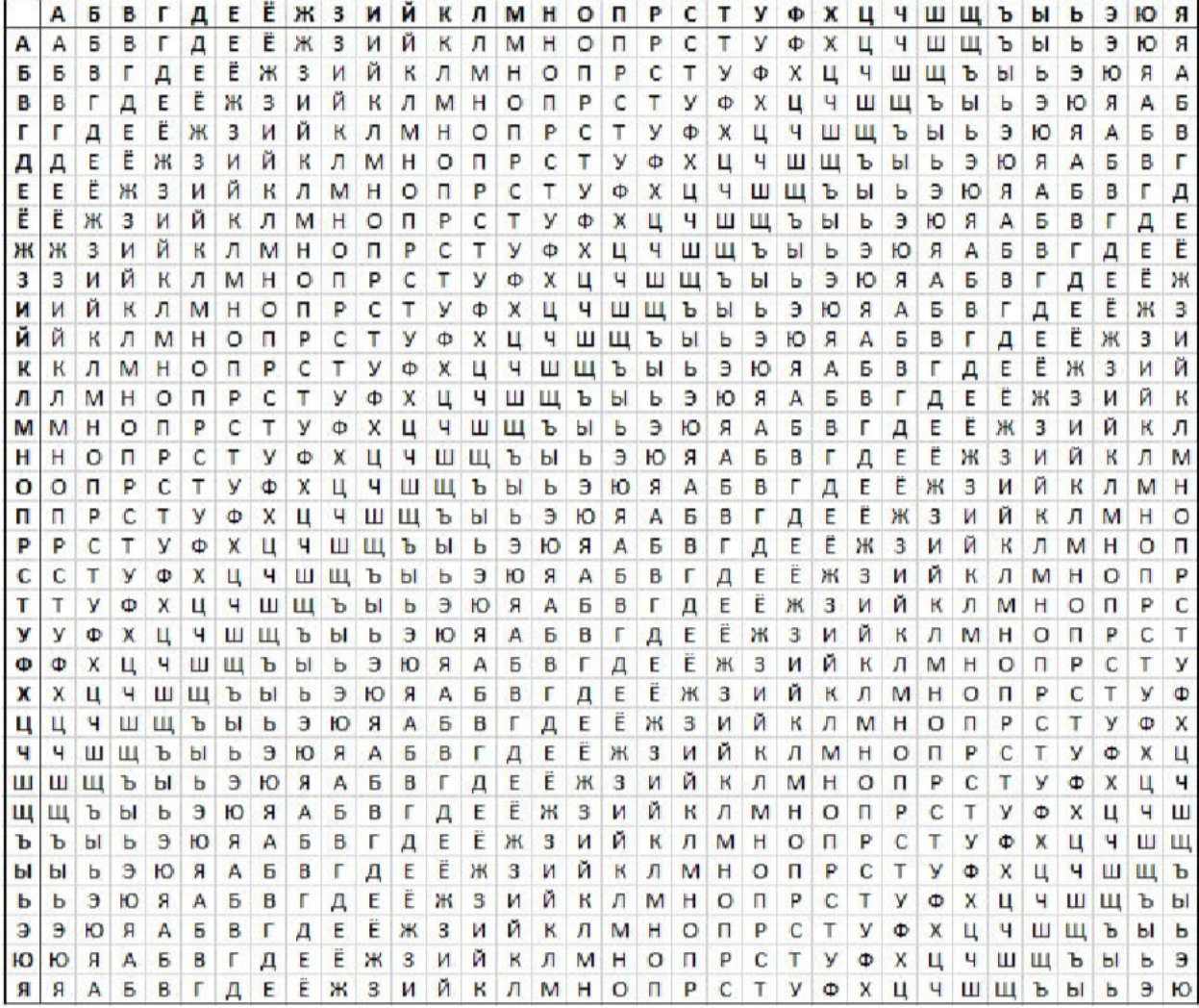


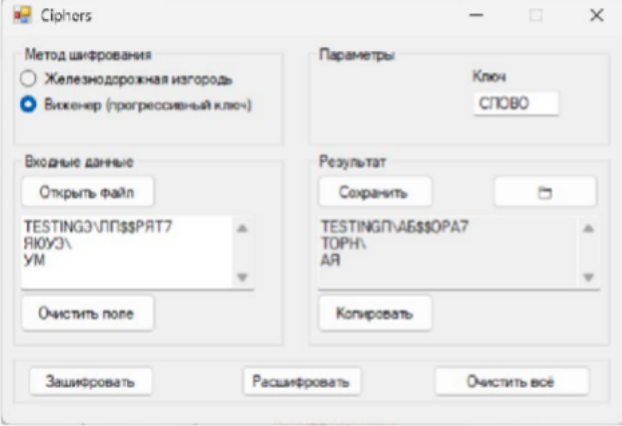
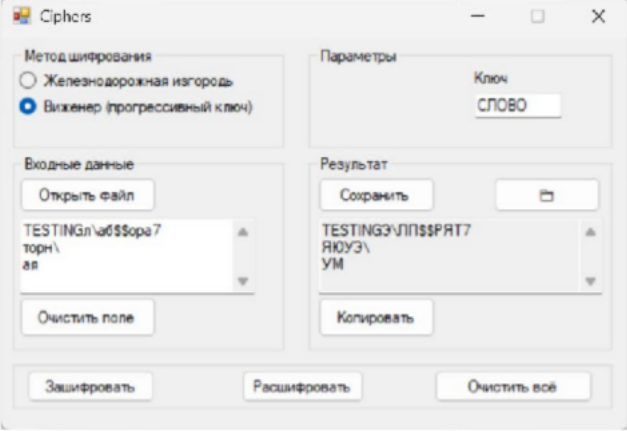
Рисунок 2.1 – тест №1

Исходный текст = “Первый\_тест! (Виженер)” Ключ = “КЛЮЧ”

Полученный прогрессивный ключ = “ КЛЮЧЛМ ЯШМН АЩНОБЪО” Получаем следующий шифротекст = “ ЪРОЩЖЦ\_СЭЮА! (ВВФУОЯЯ)”

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| текс т | П | Е | Р | В | Ы | Й | \_ | Т | Е | С | Т | ! | ( | В | И | Ж | Е | Н | Е | Р | ) |
| клю ч | К | Л | Ю | Ч | Л | М |  | Я | Ш | М | Н |  |  | А | Щ | Н | О | Б | Ъ | О |  |
| итог | Ъ | Р | О | Щ | Ж | Ц | \_ | С | Э | Ю | А | ! | ( | В | В | Ф | У | О | Я | Я | ) |

Таблица Виженера (русский язык)

Рисунок 2.2 – тест №2 Исходный текст = “ TESTINGл\аб$$ора7

торн\ ая”

Ключ = “СЛОВО”

Полученный прогрессивный ключ = “ С ЛО ВОТ МПГП УН” Получаем следующий шифротекст = “ TESTINGЭ\ЛП$$РЯТ7

## ЯЮУЭ\ УМ”

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| текс т | T | E | S | T | I | N | G | л | \ | а | б | $ | $ | о | р | а | 7 | т | о | р | н | \ | а | я |
| клю ч |  |  |  |  |  |  |  | С |  | Л | О |  |  | В | О | Т |  | М | П | Г | П |  | У | Н |
| ито г | T | E | S | T | I | N | G | Э | \ | Л | П | $ | $ | Р | Я | Т | 7 | Я | Ю | У | Э | \ | У | М |

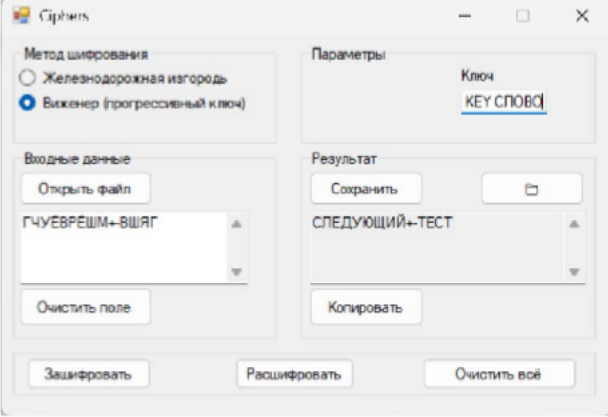
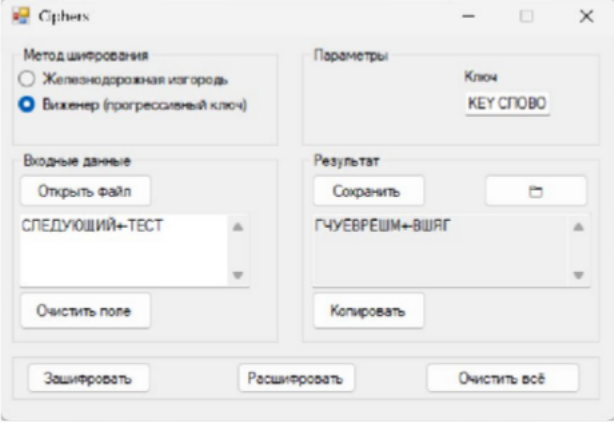


Рисунок 2.3 – тест №3 Исходный текст = “ СЛЕДУЮЩИЙ+-ТЕСТ”

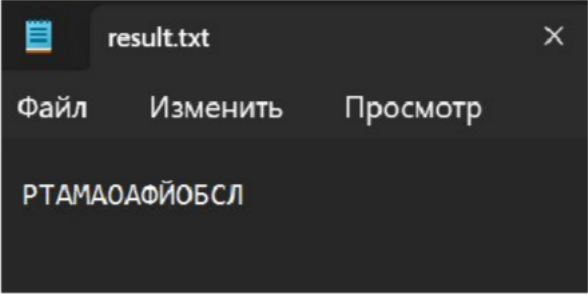
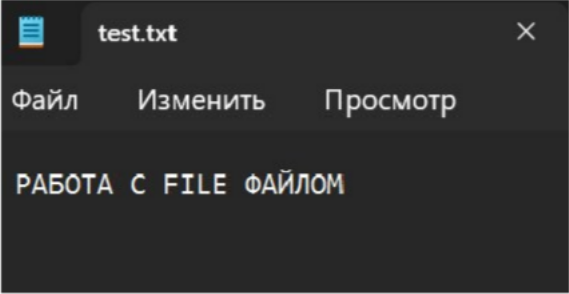
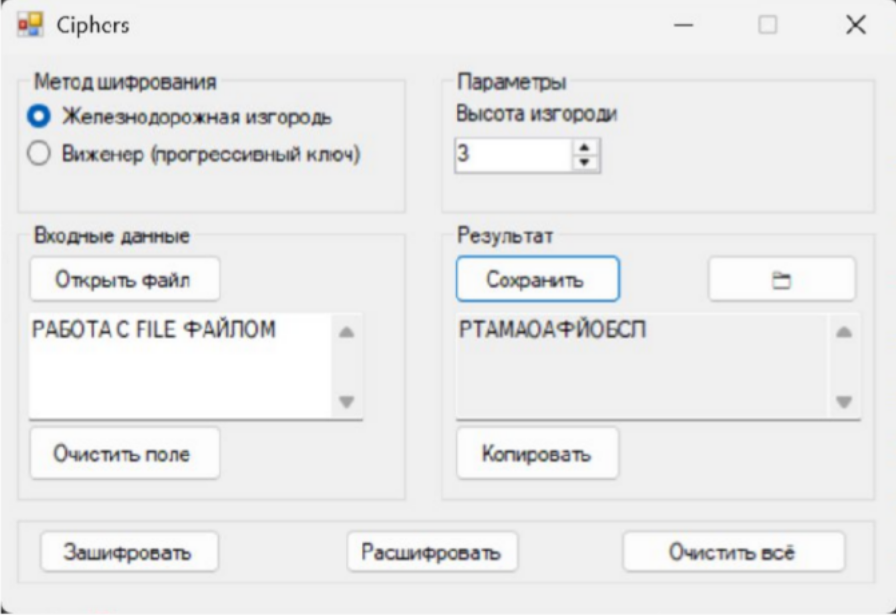
Ключ = “KEY СЛОВО”

Полученный прогрессивный ключ = “СЛОВОТМПГ ПУНР” Получаем следующий шифротекст = “ГЧУЁВРЁШМ+-ВШЯГ”

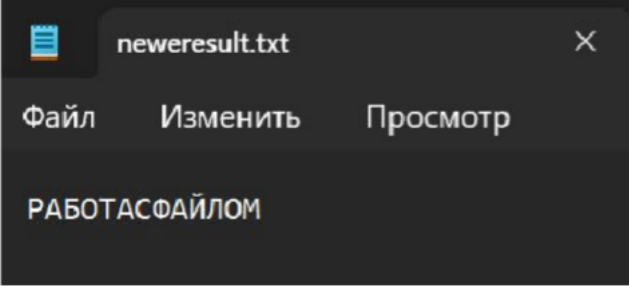
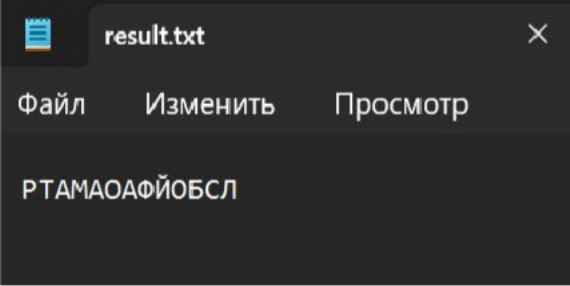
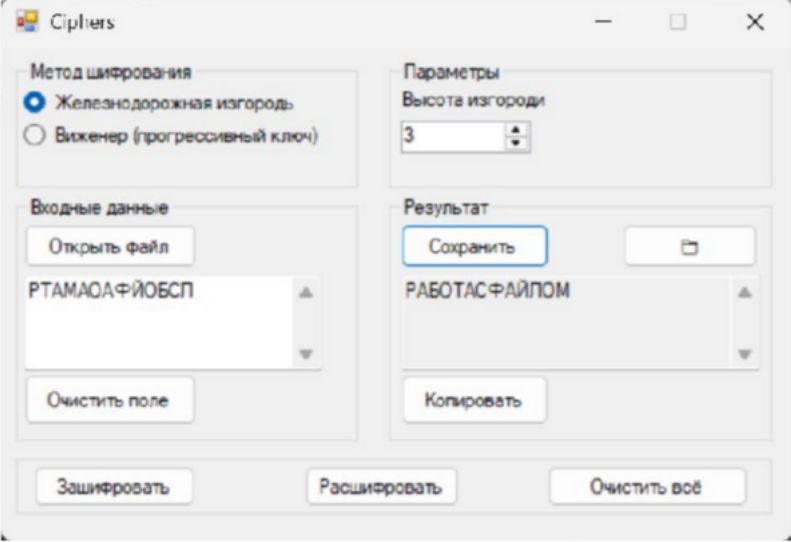
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| текст | С | Л | Е | Д | У | Ю | Щ | И | Й | + | - | Т | Е | С | Т |
| ключ | С | Л | О | В | О | Т | М | П | Г |  |  | П | У | Н | Р |
| итог | Г | Ч | У | Ё | В | Р | Ё | Ш | М | + | - | В | Ш | Я | Г |

# Скриншоты, подтверждающие работу программы с файлами

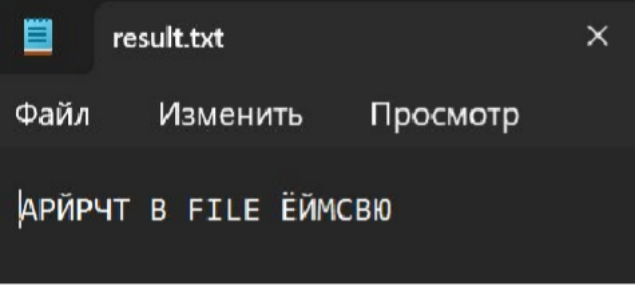
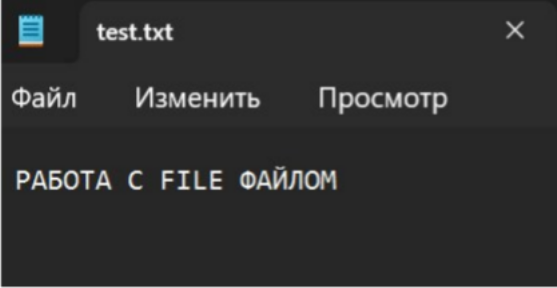
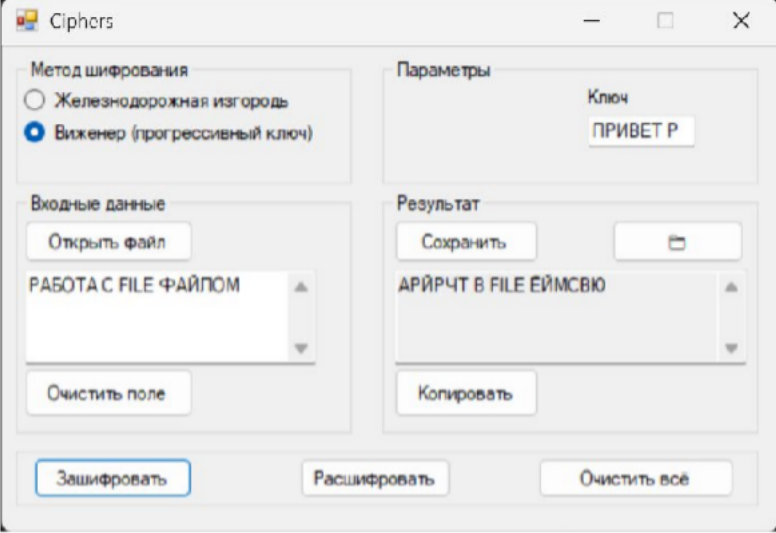
1. Шифрование методом “железнодорожной изгороди”



1. Дешифрование методом “железнодорожной изгороди”



1. Шифрование алгоритмом Виженера



1. Дешифрование алгоритмом Виженера

