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 (ТИ)

**ОТЧЕТ**
к лабораторной работе №1
Тема работы: ПРОСТЕЙШИЕ ШИФРЫ

*Вариант 6*

Выполнил Ешманский В.В.
студент: гр. 451002

Проверил: Болтак С.В.

Минск 2026

**СОДЕРЖАНИЕ**

1 Задание к лабораторной работе ..... 3
2 Тестирование программы ..... 4

## 1 ЗАДАНИЕ К ЛАБОРАТОРНОЙ РАБОТЕ

Вариант 6.

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

– Метод децимаций текст на английском языке;

– алгоритм Виженера, прямой ключ, текст на русском языке.

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.

Для всех алгоритмов ключ задается с клавиатуры пользователем.

## 2 ТЕСТИРОВАНИЕ ПРОГРАММЫ

### Тест 1

**Тестовая ситуация:** Метод децимаций. *Дымовое тестирование*

**Исходные данные:** Plaintext = “1Hello!”
Key = 3

**Ожидаемый результат:**
Проверка ключа:

Ключ должен взаимно простым с 26 (длиной алфавита), иначе разные буквы после шифрования могут превращаться в одну и ту же.

gcd(3,26)=1

Ключ допустим.

Английский алфавит:

| **A** | **B** | **C** | **D** | **E** | **F** | **G** | **H** | **I** | **J** | **K** | **L** | **M** | **N** | **O** | **P** | **Q** | **R** | **S** | **T** | **U** | **V** | **W** | **X** | **Y** | **Z** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 |

Замена букв на числа:

| **Буква** | **Число** |
|---|---|
| H | 7 |
| E | 4 |
| L | 11 |
| L | 11 |
| O | 14 |

Формула шифрования:

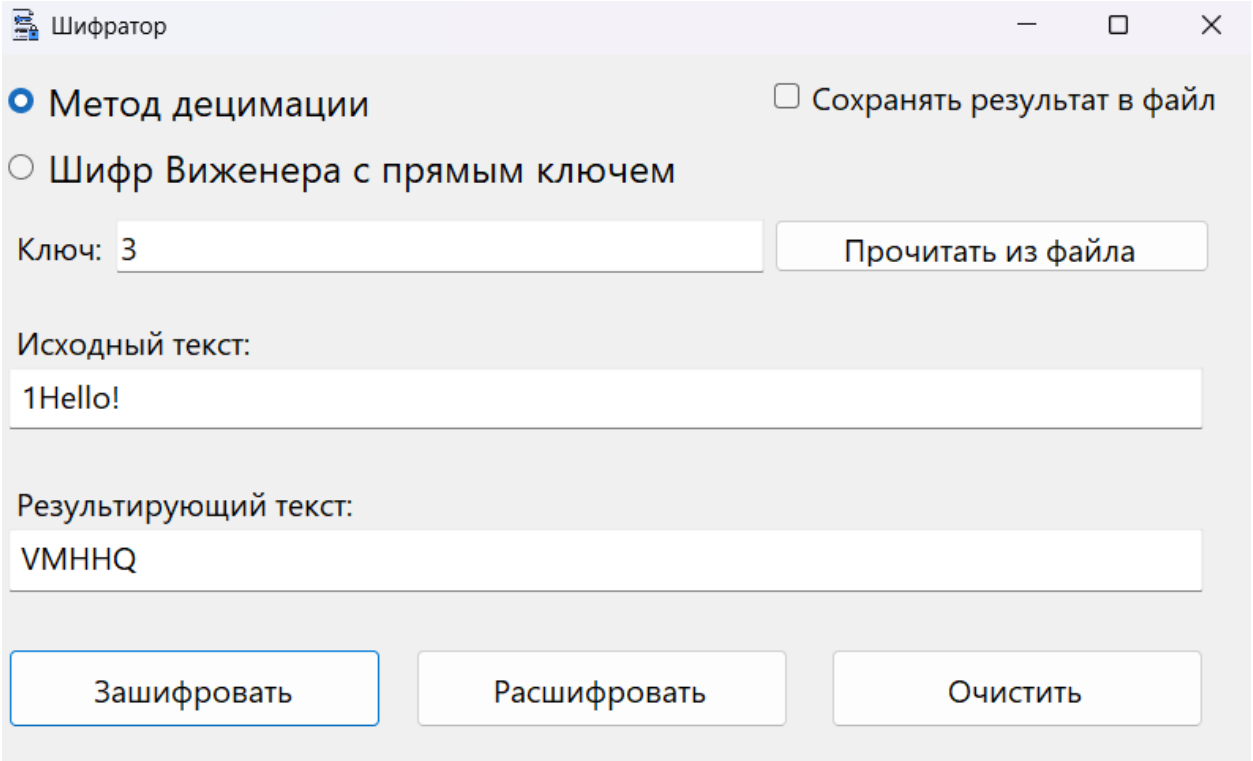
$$E(x) = (k \cdot x) mod 26$$

| **Буква** | **x** | **3 · x** | **mod 26** | **Новое число** |
|---|---|---|---|---|
| H | 7 | 21 | 21 | 21 |
| E | 4 | 12 | 12 | 12 |
| L | 11 | 33 | 7 | 7 |
| L | 11 | 33 | 7 | 7 |
| O | 14 | 42 | 16 | 16 |

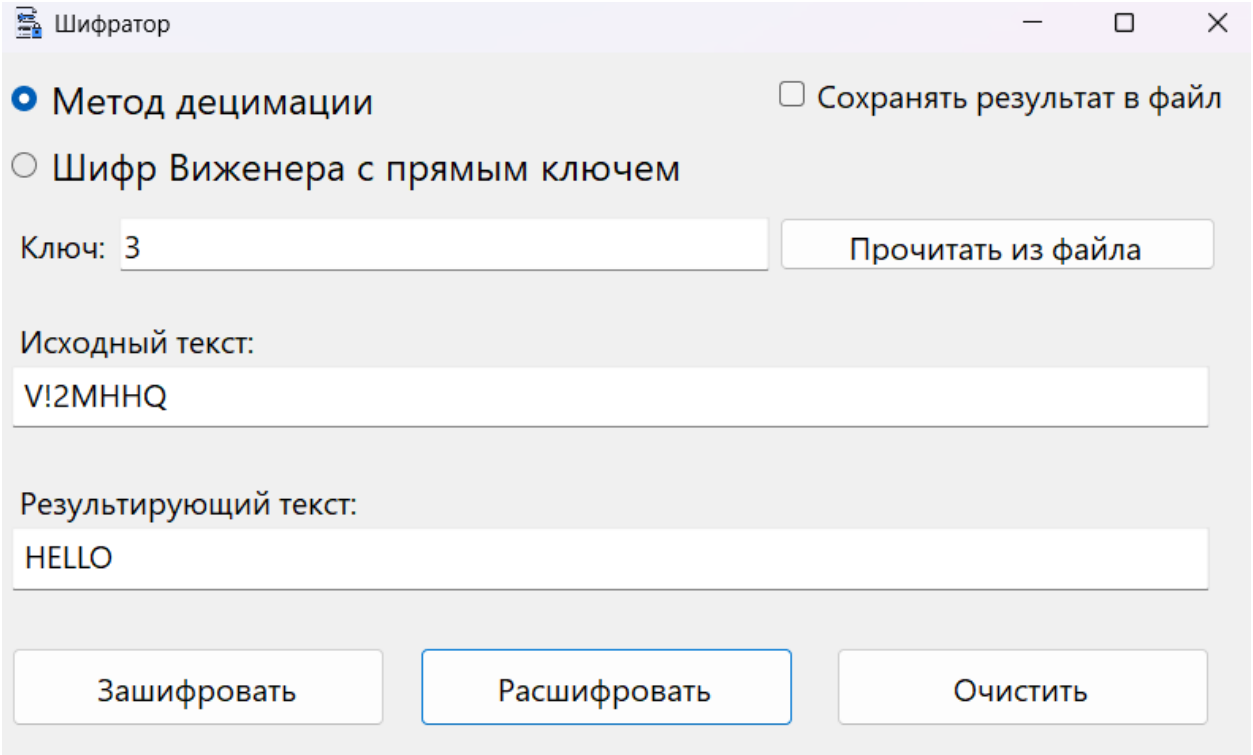
Обратная замена чисел в буквы:

| **Число** | **Буква** |
|---|---|
| 21 | V |
| 12 | M |
| 7 | H |
| 7 | H |
| 16 | Q |

**Полученный результат при шифровании:**



**Полученный результат при дешифровании:**




**Тест 2**

**Тестовая ситуация:** Метод децимаций. *Ломаем на валидных данных. Ключ* ***меньше*** *длины алфавита.*

**Исходные данные:** Plaintext = “Hello”
Key = 5

**Ожидаемый результат:**

Проверка ключа:

Ключ должен взаимно простым с 26 (длиной алфавита), иначе разные буквы после шифрования могут превращаться в одну и ту же.

$$gcd(5,26)=1$$

Ключ допустим.

Английский алфавит:

| **A** | **B** | **C** | **D** | **E** | **F** | **G** | **H** | **I** | **J** | **K** | **L** | **M** | **N** | **O** | **P** | **Q** | **R** | **S** | **T** | **U** | **V** | **W** | **X** | **Y** | **Z** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 |

Замена букв на числа:

| **Буква** | **Число** |
|---|---|
| H | 7 |
| E | 4 |
| L | 11 |
| L | 11 |
| O | 14 |

Формула шифрования:

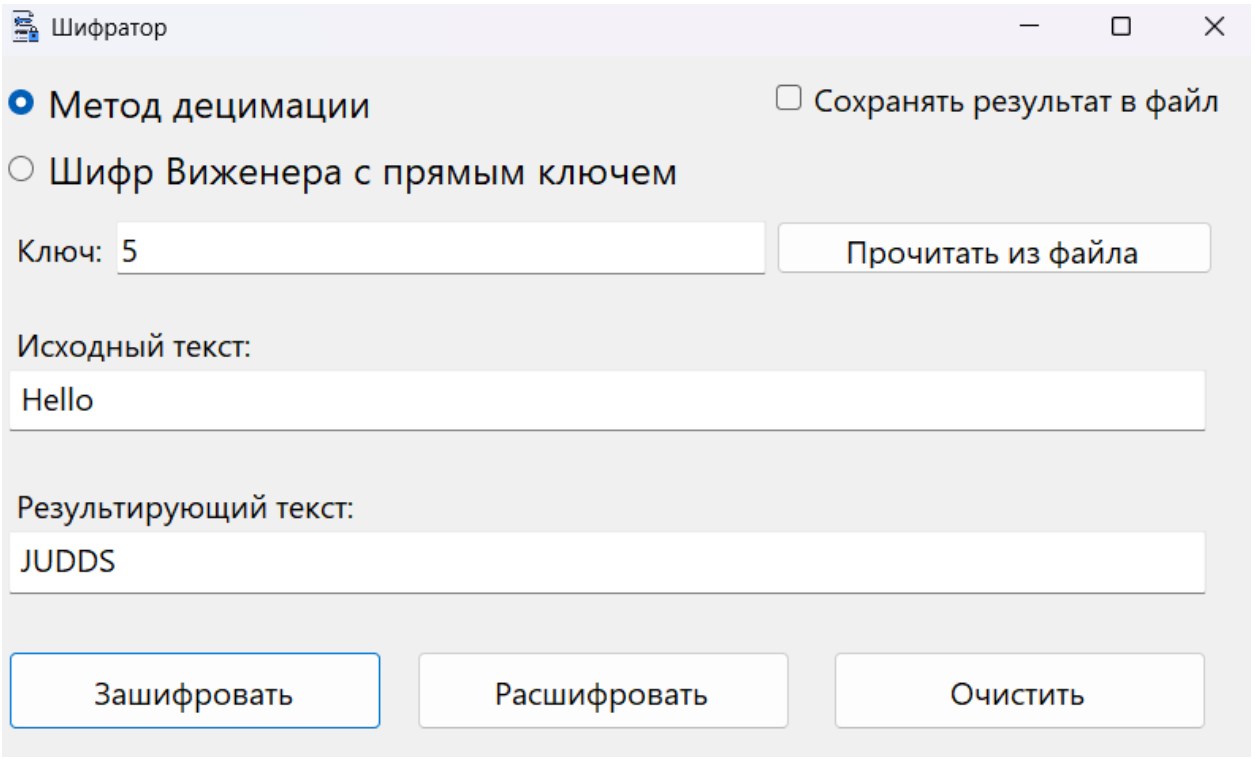
$$E(x) = (k \cdot x) mod 26$$

| **Буква** | **x** | **5 · x** | **mod 26** | **Новое число** |
|---|---|---|---|---|
| H | 7 | 35 | 9 | 9 |
| E | 4 | 20 | 20 | 20 |
| L | 11 | 55 | 3 | 3 |
| L | 11 | 55 | 3 | 3 |
| O | 14 | 70 | 18 | 18 |

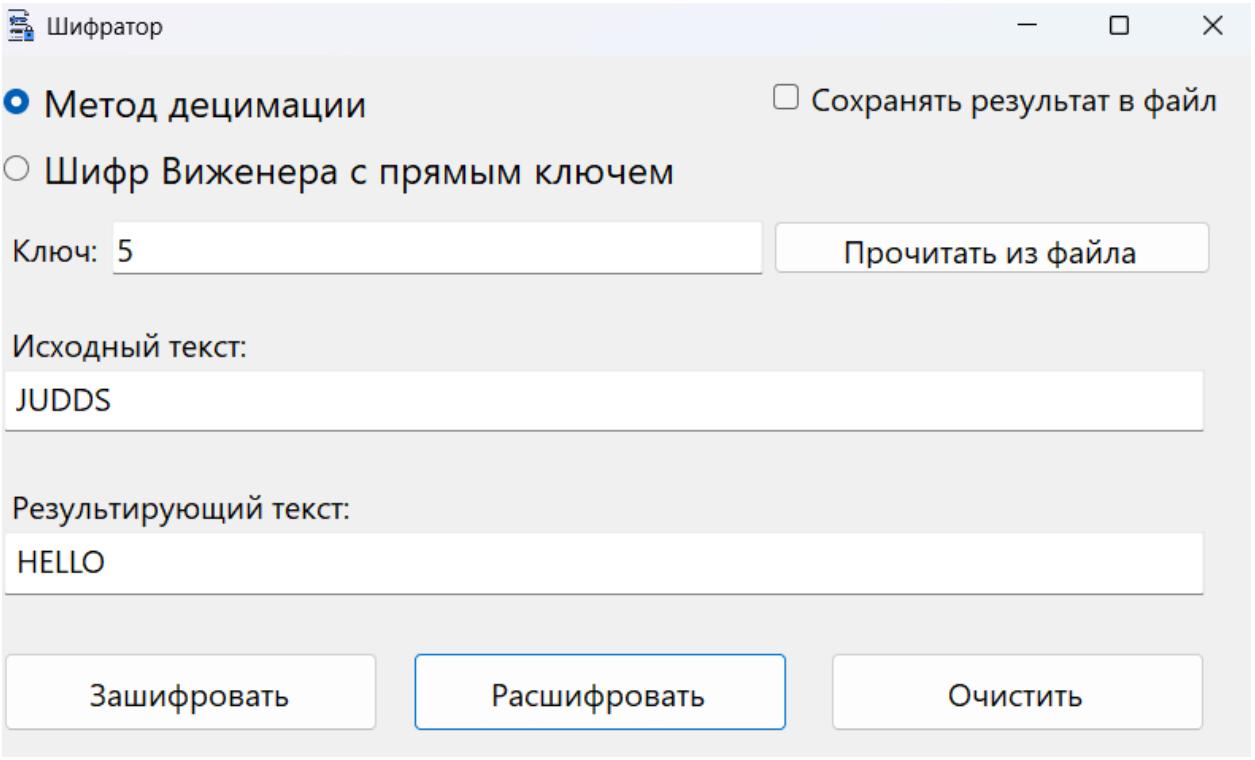
Обратная замена чисел в буквы:

| **Число** | **Буква** |
|---|---|
| 9 | J |
| 20 | U |
| 3 | D |
| 3 | D |
| 18 | S |

**Полученный результат при шифровании:**




**Полученный результат при дешифровании:**



## Тест 3

**Тестовая ситуация:** Метод децимаций. *Ломаем на валидных данных. Ключ* ***больше*** *длины алфавита.*

**Исходные данные:** Plaintext = “Hello”
Key = 35

**Ожидаемый результат:**

Проверка ключа:

Ключ должен взаимно простым с 26 (длиной алфавита), иначе разные буквы после шифрования могут превращаться в одну и ту же.

$$gcd(35,26)=1$$

Ключ допустим.

Английский алфавит:

| **A** | **B** | **C** | **D** | **E** | **F** | **G** | **H** | **I** | **J** | **K** | **L** | **M** | **N** | **O** | **P** | **Q** | **R** | **S** | **T** | **U** | **V** | **W** | **X** | **Y** | **Z** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 |

Замена букв на числа:

| **Буква** | **Число** |
|---|---|
| H | 7 |
| E | 4 |
| L | 11 |
| L | 11 |
| O | 14 |

Формула шифрования:

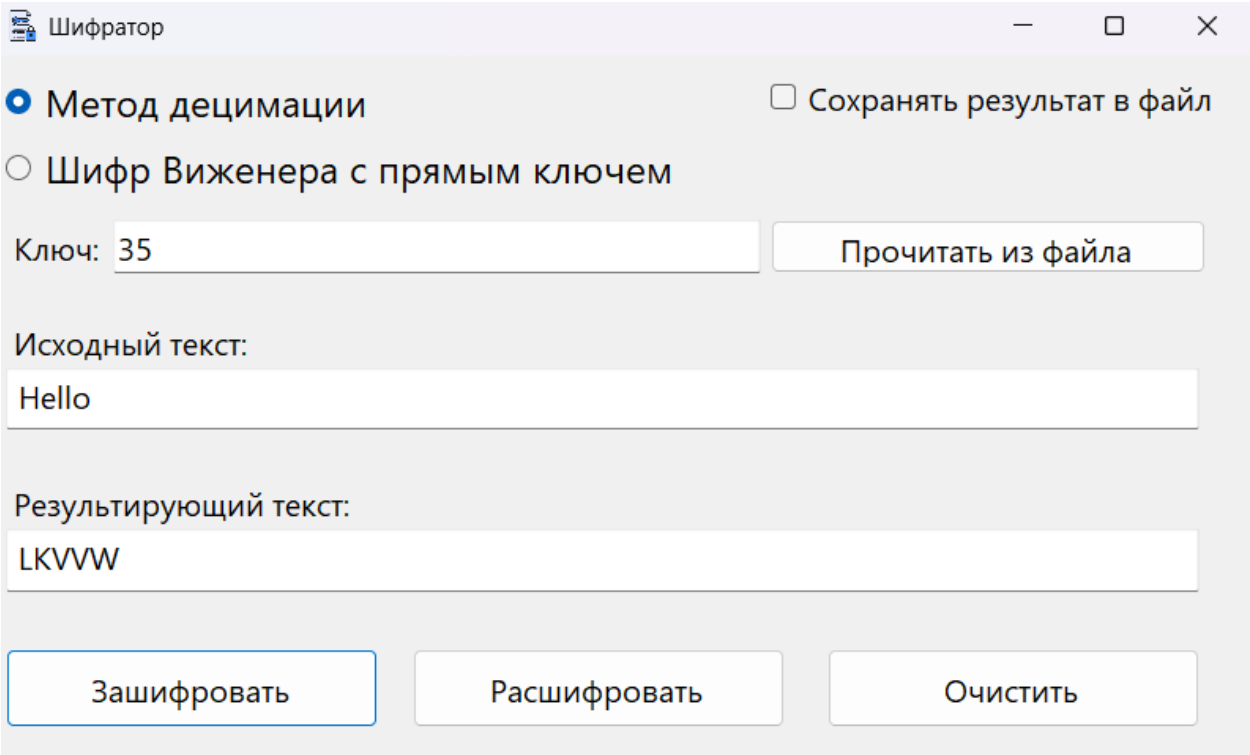
$$E(x) = (k \cdot x) mod 26$$

| **Буква** | **x** | **35·x** | **mod 26** | **Новое число** |
|---|---|---|---|---|
| H | 7 | 245 | 11 | 11 |
| E | 4 | 140 | 10 | 10 |
| L | 11 | 385 | 21 | 21 |
| L | 11 | 385 | 21 | 21 |
| O | 14 | 490 | 22 | 22 |

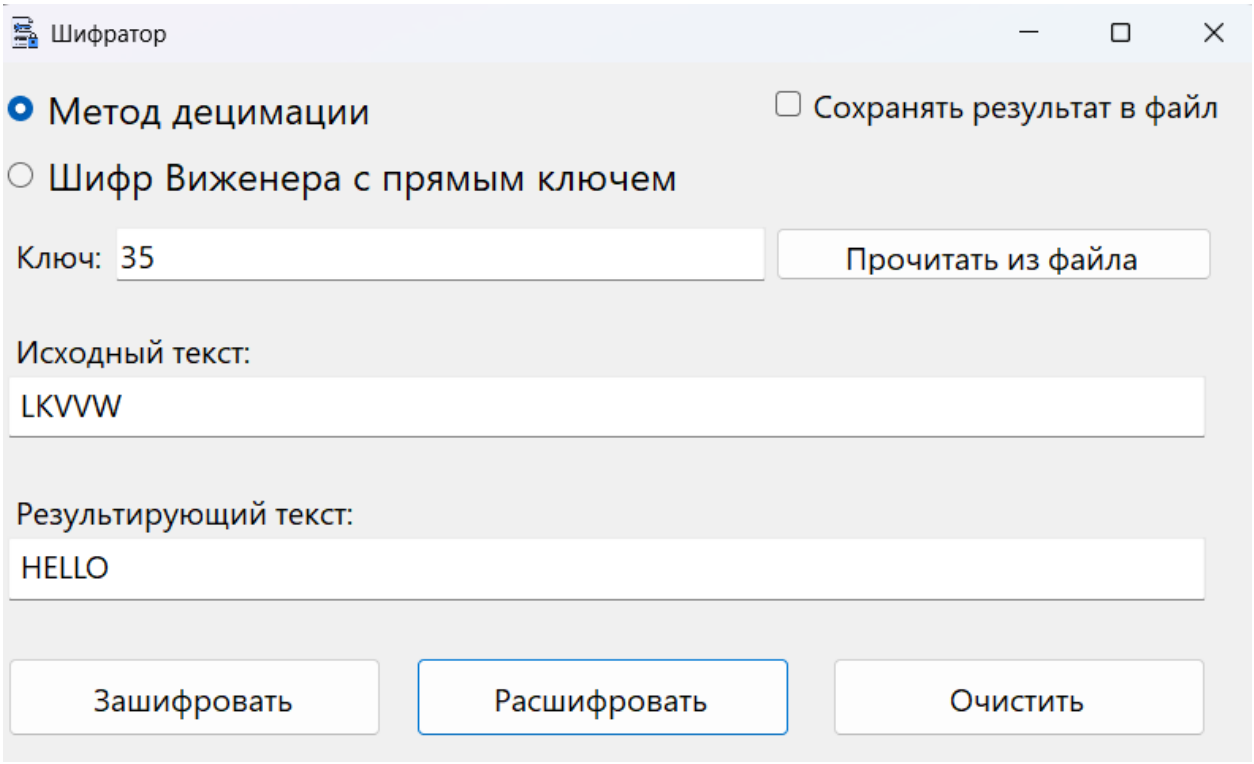
Обратная замена чисел в буквы:

| **Число** | **Буква** |
|---|---|
| 11 | L |
| 10 | K |
| 21 | V |
| 21 | V |
| 22 | W |

**Полученный результат при шифровании:**



**Полученный результат при дешифровании:**




**Тест 4**

**Тестовая ситуация:** Метод децимаций. *Ломаем на не валидных данных. Ключ* ***содержит недопустимые значения***.

**Исходные данные:** Plaintext = “Hello”
Key = “Se3!c»re:t5K”л|ю’ч”

**Ожидаемый результат:**

Проверка ключа:

Ключ должен взаимно простым с 26 (длиной алфавита), иначе разные буквы после шифрования могут превращаться в одну и ту же.

$$gcd(35,26)=1$$

Ключ допустим.

Английский алфавит:

| **A** | **B** | **C** | **D** | **E** | **F** | **G** | **H** | **I** | **J** | **K** | **L** | **M** | **N** | **O** | **P** | **Q** | **R** | **S** | **T** | **U** | **V** | **W** | **X** | **Y** | **Z** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 |

Замена букв на числа:

| **Буква** | **Число** |
|---|---|
| H | 7 |
| E | 4 |
| L | 11 |
| L | 11 |
| O | 14 |

Формула шифрования:

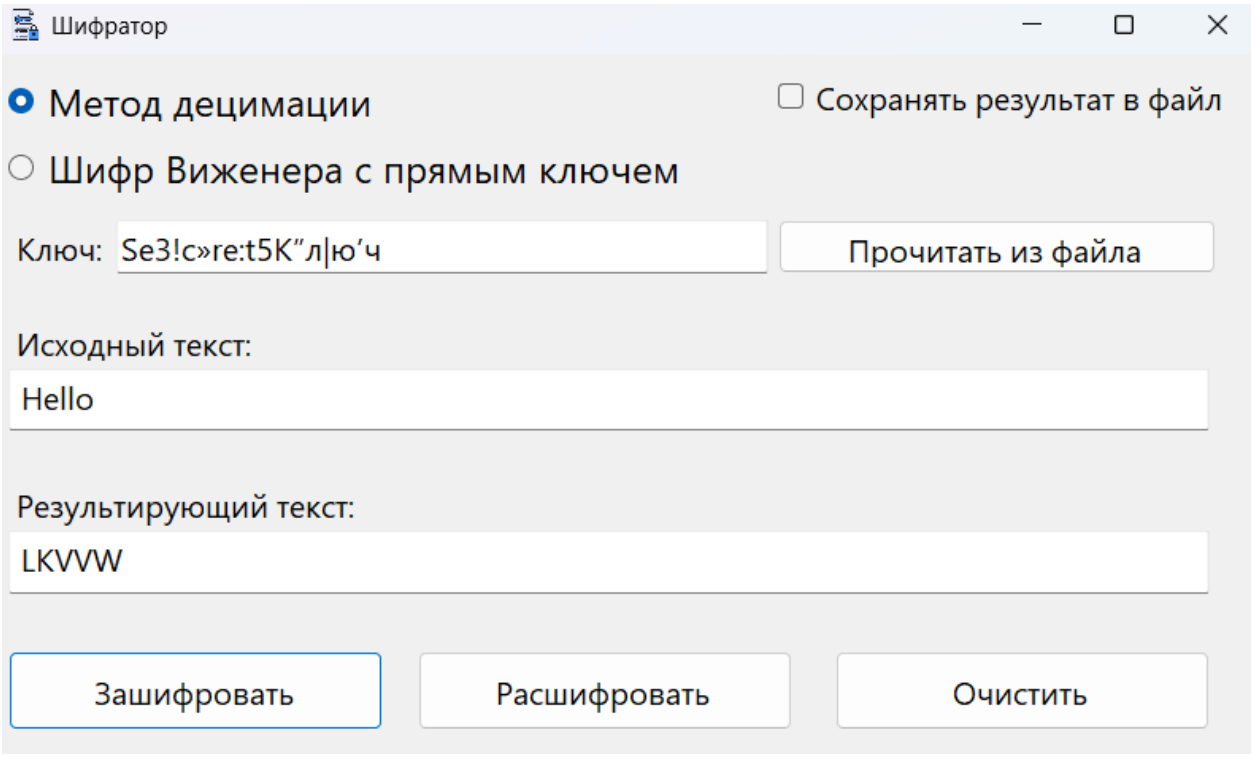
$$E(x) = (k \cdot x) mod 26$$

| **Буква** | **x** | **35·x** | **mod 26** | **Новое число** |
|---|---|---|---|---|
| H | 7 | 245 | 11 | 11 |
| E | 4 | 140 | 10 | 10 |
| L | 11 | 385 | 21 | 21 |
| L | 11 | 385 | 21 | 21 |
| O | 14 | 490 | 22 | 22 |

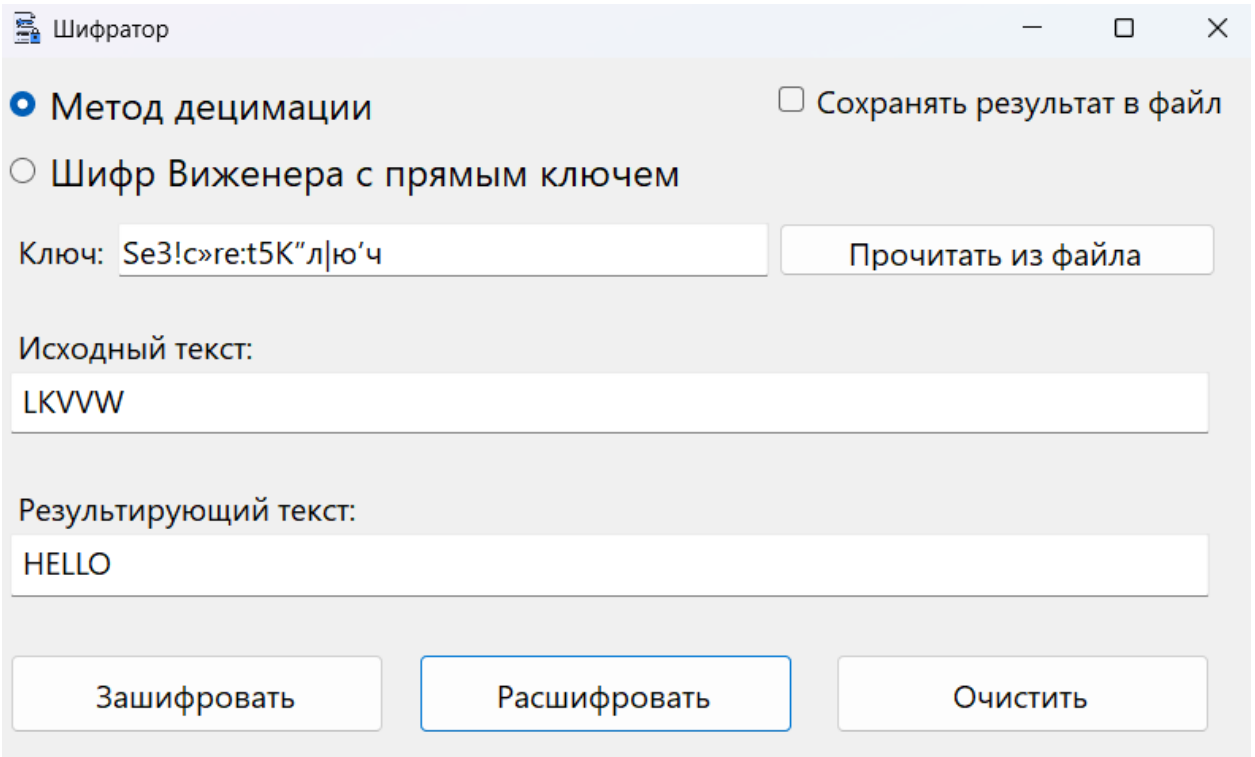
Обратная замена чисел в буквы:

| **Число** | **Буква** |
|---|---|
| 11 | L |
| 10 | K |
| 21 | V |
| 21 | V |
| 22 | W |

**Полученный результат при шифровании:**




**Полученный результат при дешифровании:**



## Тест 5

**Тестовая ситуация:** Шифр Виженера. *Дымовое тестирование.*

**Исходные данные:** Plaintext = “CE!K 1PET3”
Key = “ёлки”

**Ожидаемый результат:**
Формула шифрования:

$$C_i = (P_i + K_j) \bmod N$$

$C_i$ – Позиция зашифрованного символа в алфавите
$P_i$ – Позиция шифруемого символа в алфавите
$K_j$ – Позиция символа ключа в алфавите
N – Длина алфавита (в русском составляет 33)

Каждая буква шифруется с помощью «сдвига», который задаёт соответствующая буква ключа, а остаток по модулю нужен, чтобы оставаться в пределах алфавита.

Операция **mod 33** всегда возвращает результат **0…32**, так что алфавит нумеруем с нуля.

Русский алфавит

| А | Б | В | Г | Д | Е | Ё | Ж | З | И | Й | К | Л | М | Н | О | П | Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ь | Ы | Ъ | Э | Ю | Я |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 |

Шифруемый текст:

| С | Е | К | Р | Е | Т |
|---|---|---|---|---|---|
| 18 | 5 | 11 | 17 | 5 | 19 |

Ключ:

| Ё | Л | К | И | Ё | Л |
|---|---|---|---|---|---|
| 6 | 12 | 11 | 9 | 6 | 12 |

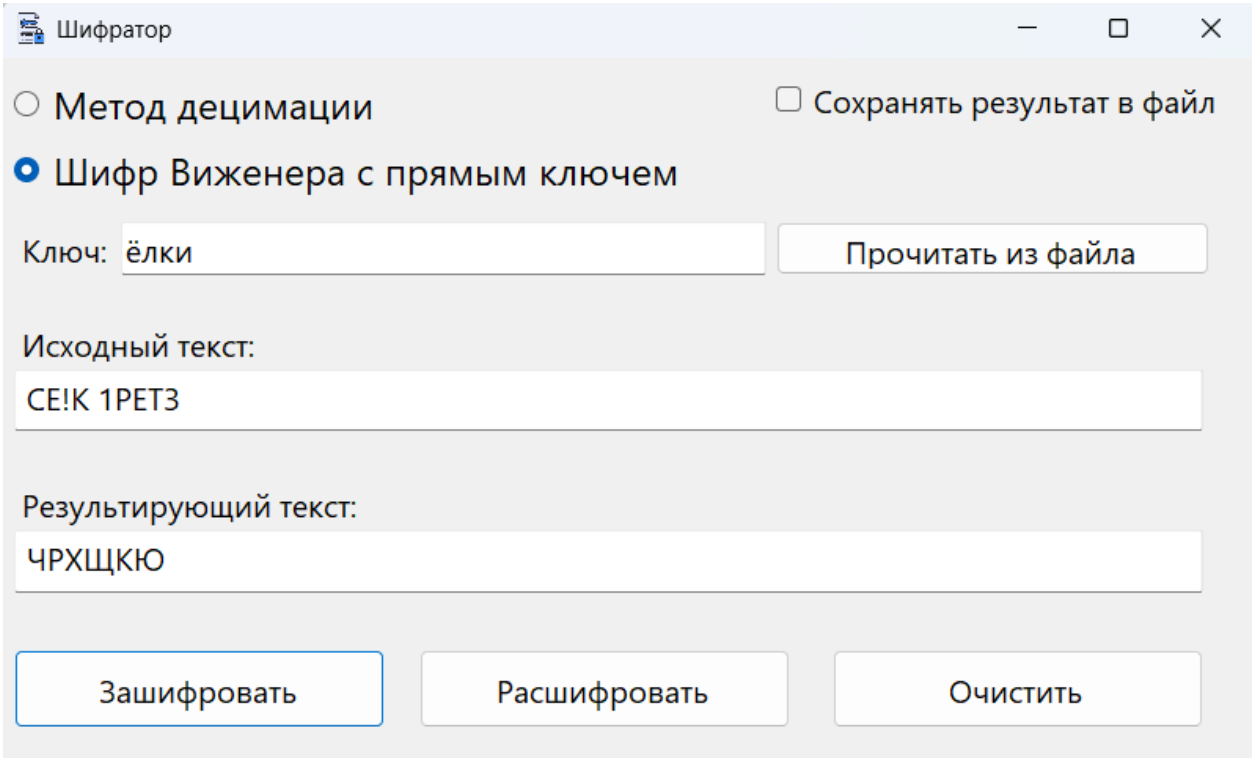
Применение формулы:

| **P_i** | **K_j** | **P_i + K_j** | **(mod 33)** | **C_i** |
|---|---|---|---|---|
| 18 | 6 | 24 | 24 | 24 |
| 5 | 12 | 17 | 17 | 17 |
| 11 | 11 | 22 | 22 | 22 |
| 17 | 9 | 26 | 26 | 26 |
| 5 | 6 | 11 | 11 | 11 |
| 19 | 12 | 31 | 31 | 31 |

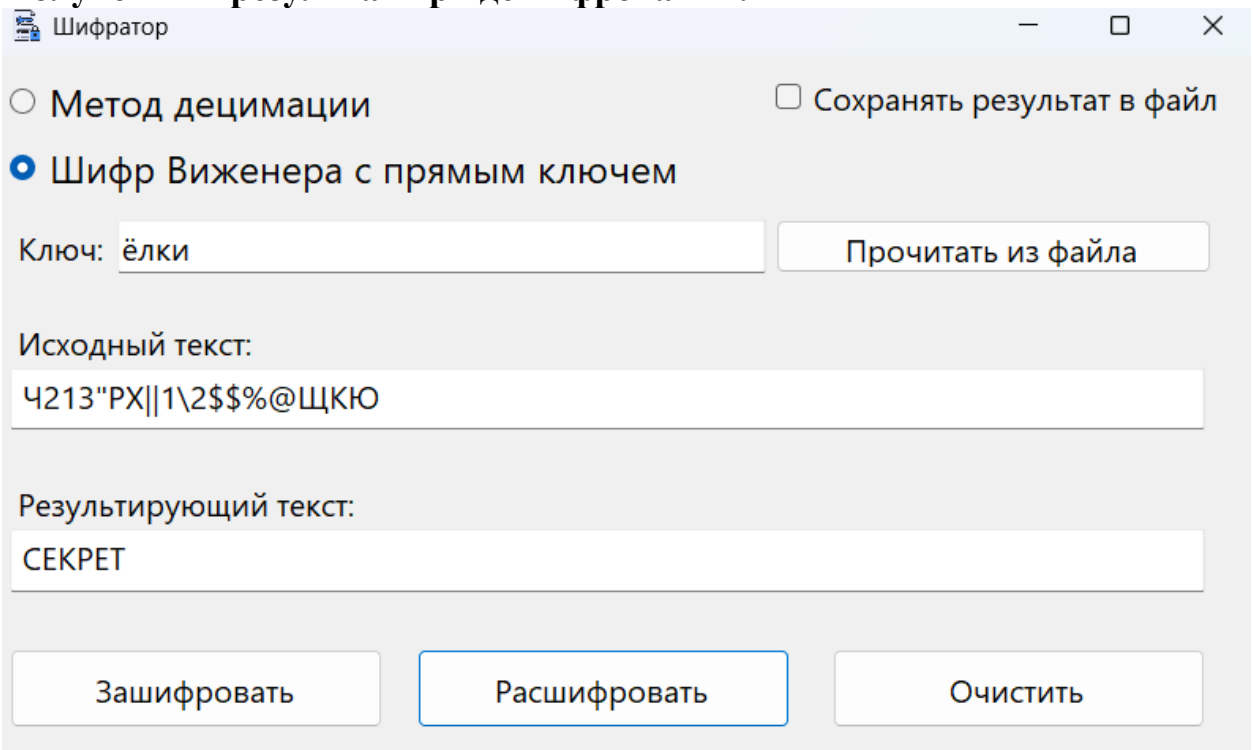
Обратная замена чисел в буквы:

| **C_i** | **24** | **17** | **22** | **26** | **11** | **31** |
|---|---|---|---|---|---|---|
| Буква | Ч | Р | Х | Щ | К | Ю |

**Полученный результат при шифровании:**




**Полученный результат при дешифровании:**



## Тест 6

**Тестовая ситуация:** Шифр Виженера. *Ломаем на валидных данных. Тестовая фраза содержит “ё”.*

**Исходные данные:** Plaintext = “ЁЖИК32 222В ЛЕ"№СУ!”
Key = “поп”

**Ожидаемый результат:**
Формула шифрования:

$$C_i = (P_i + K_j) \bmod N$$

$C_i$ – Позиция зашифрованного символа в алфавите
$P_i$ – Позиция шифруемого символа в алфавите
$K_j$ – Позиция символа ключа в алфавите
N – Длина алфавита (в русском составляет 33)

Каждая буква шифруется с помощью «сдвига», который задаёт соответствующая буква ключа, а остаток по модулю нужен, чтобы оставаться в пределах алфавита.

Операция **mod 33** всегда возвращает результат **0…32**, так что алфавит нумеруем с нуля.

Русский алфавит

| А | Б | В | Г | Д | Е | Ё | Ж | З | И | Й | К | Л | М | Н | О | П | Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ь | Ы | Ъ | Э | Ю | Я |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 |

Шифруемый текст:

| Ё | Ж | И | К | В | Л | Е | С | У |
|---|---|---|---|---|---|---|---|---|
| 6 | 7 | 9 | 11 | 2 | 12 | 5 | 18 | 20 |

Ключ:

| П | О | П | П | О | П | П | О | П |
|---|---|---|---|---|---|---|---|---|
| 16 | 15 | 16 | 16 | 16 | 16 | 16 | 16 | 16 |

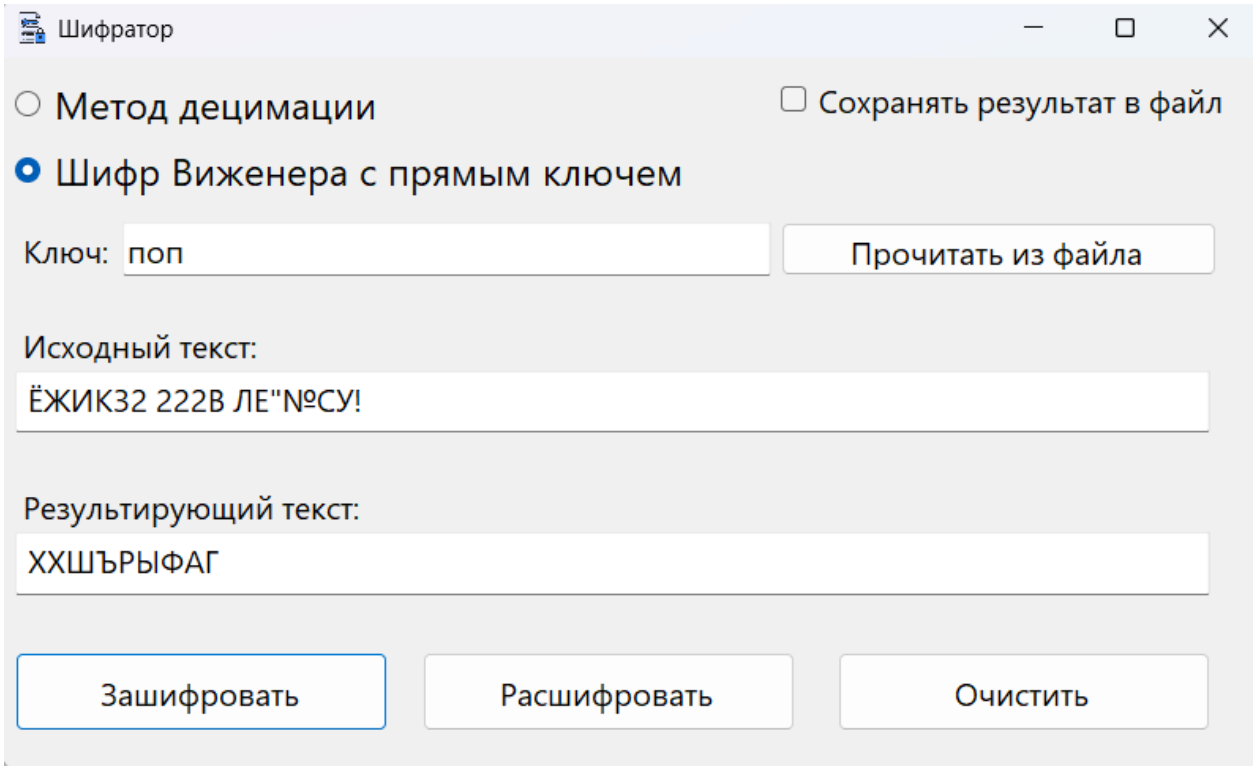
Применение формулы:

| **P_i** | **K_j** | **P_i + K_j** | **(mod 33)** | **C_i** |
|---|---|---|---|---|
| 6 | 16 | 22 | 22 | 22 |
| 7 | 15 | 22 | 22 | 22 |
| 9 | 16 | 25 | 25 | 25 |
| 11 | 16 | 27 | 27 | 27 |
| 2 | 15 | 17 | 17 | 17 |
| 12 | 16 | 28 | 28 | 28 |
| 5 | 16 | 21 | 21 | 21 |
| 18 | 15 | 33 | 0 | 0 |
| 20 | 16 | 36 | 3 | 3 |

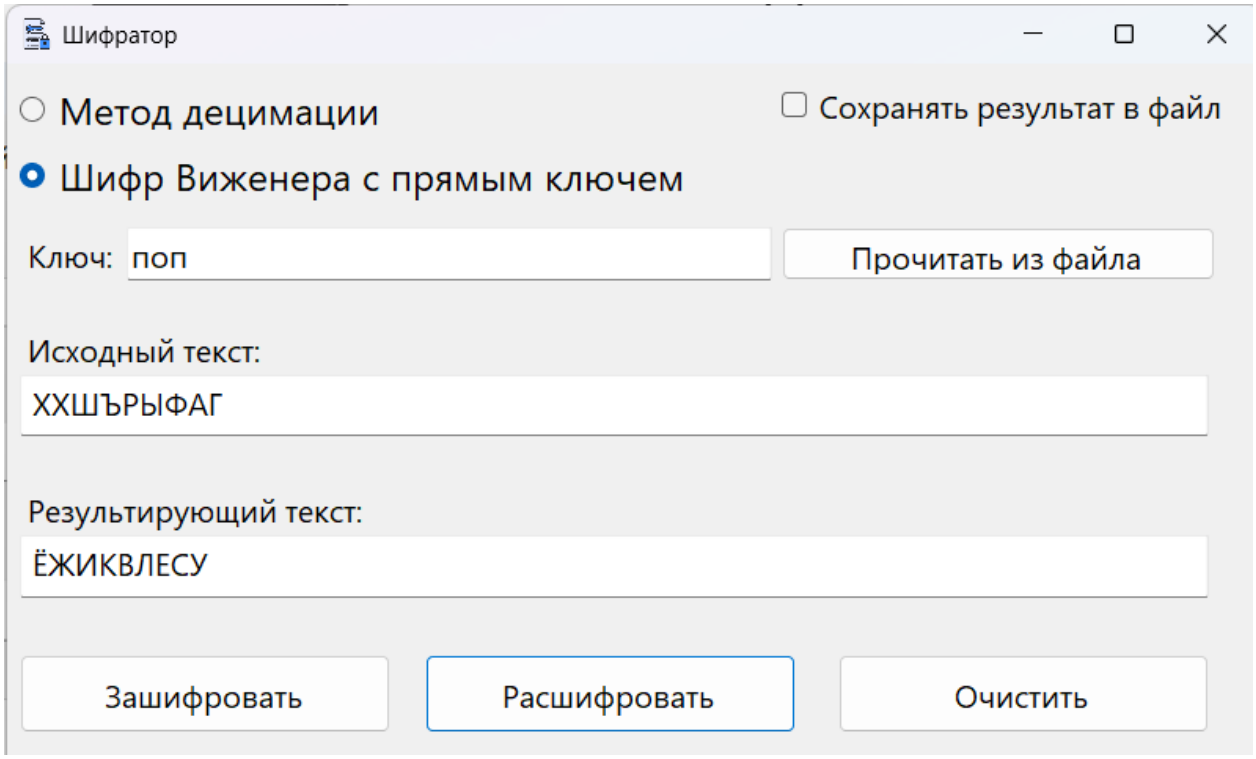
Обратная замена чисел в буквы:

| **C_i** | **22** | **22** | **25** | **27** | **17** | **28** | **21** | **0** | **3** |
|---|---|---|---|---|---|---|---|---|---|
| Буква | Х | Х | Ш | Ъ | Р | Ы | Ф | А | Г |

**Полученный результат при шифровании:**



**Полученный результат при дешифровании:**




**Тест 7**

**Тестовая ситуация:** Шифр Виженера. *Ломаем на не валидных данных. Ключ содержит недопустимые значения.*

**Исходные данные:** Plaintext = “Суббота”
Key = “Q’ROбл.@#a23ка”

**Ожидаемый результат:**
Формула шифрования:

$$C_i = (P_i + K_j) \bmod N$$

$C_i$ – Позиция зашифрованного символа в алфавите
$P_i$ – Позиция шифруемого символа в алфавите
$K_j$ – Позиция символа ключа в алфавите
N – Длина алфавита (в русском составляет 33)

Каждая буква шифруется с помощью «сдвига», который задаёт соответствующая буква ключа, а остаток по модулю нужен, чтобы оставаться в пределах алфавита.

Операция **mod 33** всегда возвращает результат **0…32**, так что алфавит нумеруем с нуля.

Русский алфавит

| А | Б | В | Г | Д | Е | Ё | Ж | З | И | Й | К | Л | М | Н | О | П | Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ь | Ы | Ъ | Э | Ю | Я |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 |

Шифруемый текст:

| С | У | Б | Б | О | Т | А |
|---|---|---|---|---|---|---|
| 18 | 20 | 1 | 1 | 15 | 19 | 0 |

Ключ:

| О | Б | Л | А | К | А | О |
|---|---|---|---|---|---|---|
| 15 | 1 | 12 | 0 | 10 | 0 | 15 |

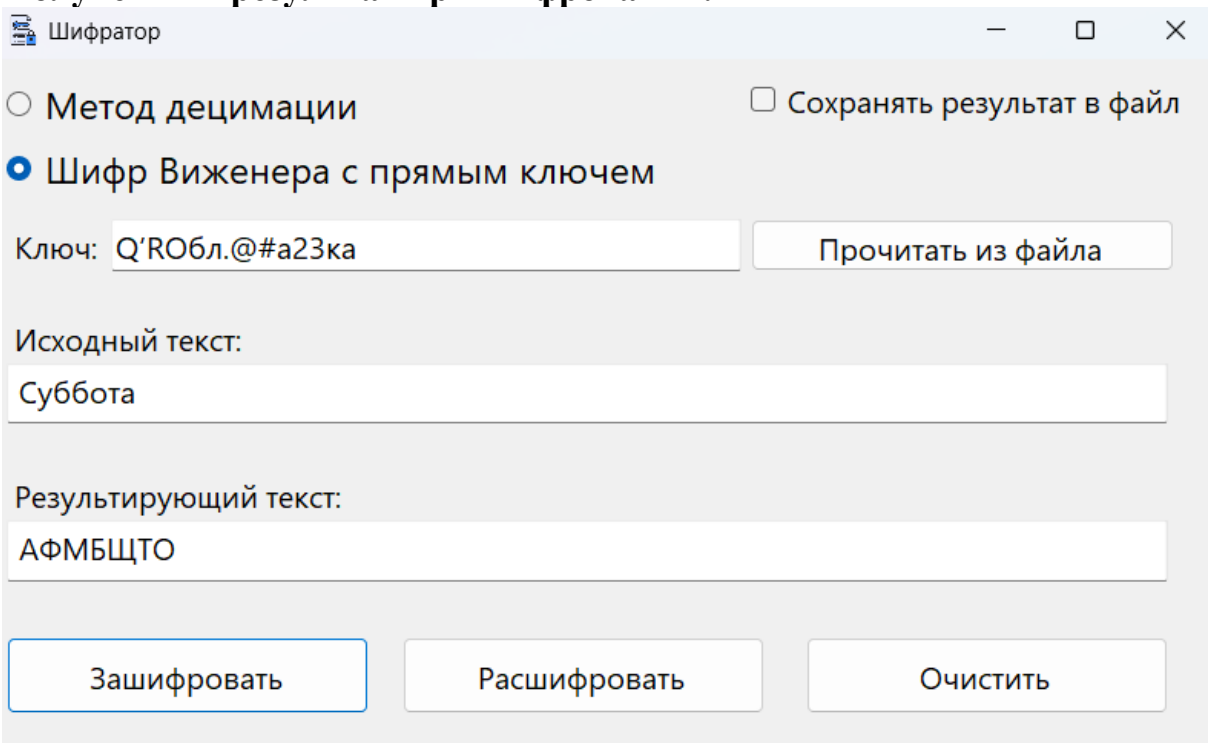
Применение формулы:

| **P_i** | **K_j** | **P_i + K_j** | **mod 33** | **C_i** |
|---|---|---|---|---|
| 18 | 15 | 33 | 0 | 0 |
| 20 | 1 | 21 | 21 | 21 |
| 1 | 12 | 13 | 13 | 13 |
| 1 | 0 | 1 | 1 | 1 |
| 15 | 10 | 25 | 25 | 25 |
| 19 | 0 | 19 | 19 | 19 |
| 0 | 15 | 15 | 15 | 15 |

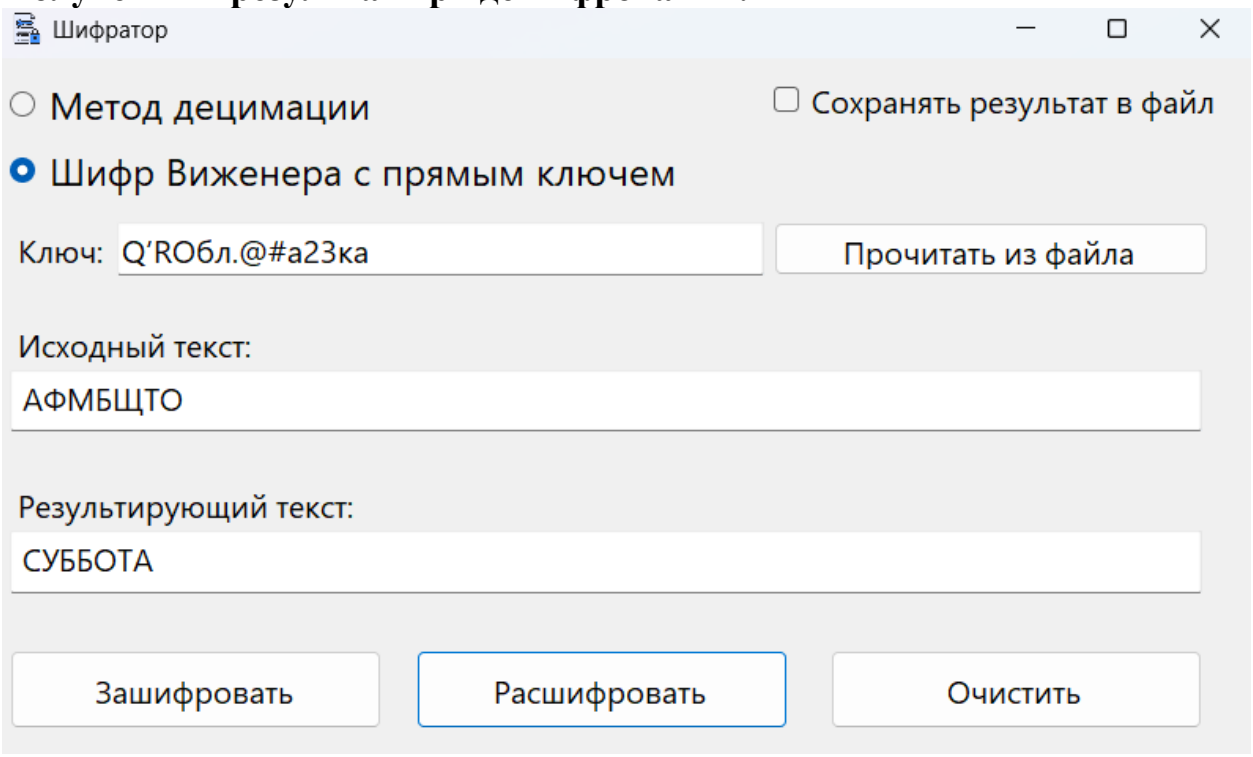
Обратная замена чисел в буквы:

| **C_i** | **0** | **21** | **13** | **1** | **25** | **19** | **15** |
|---|---|---|---|---|---|---|---|
| Буква | А | Ф | М | Б | Щ | Т | О |

**Полученный результат при шифровании:**



**Полученный результат при дешифровании:**



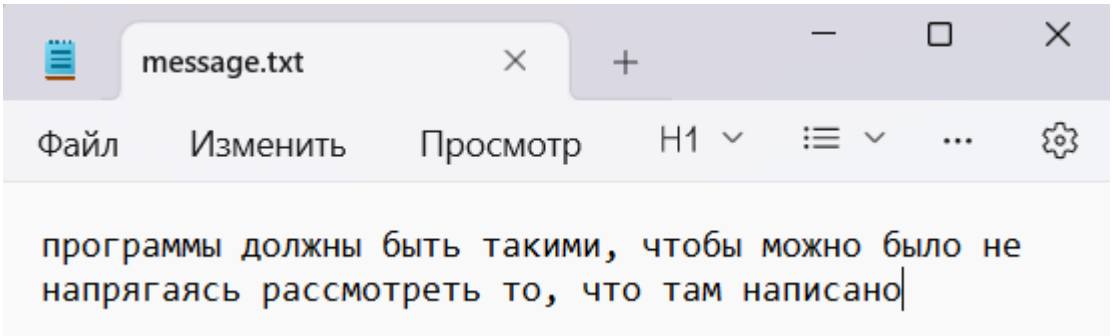

**Тест 8**

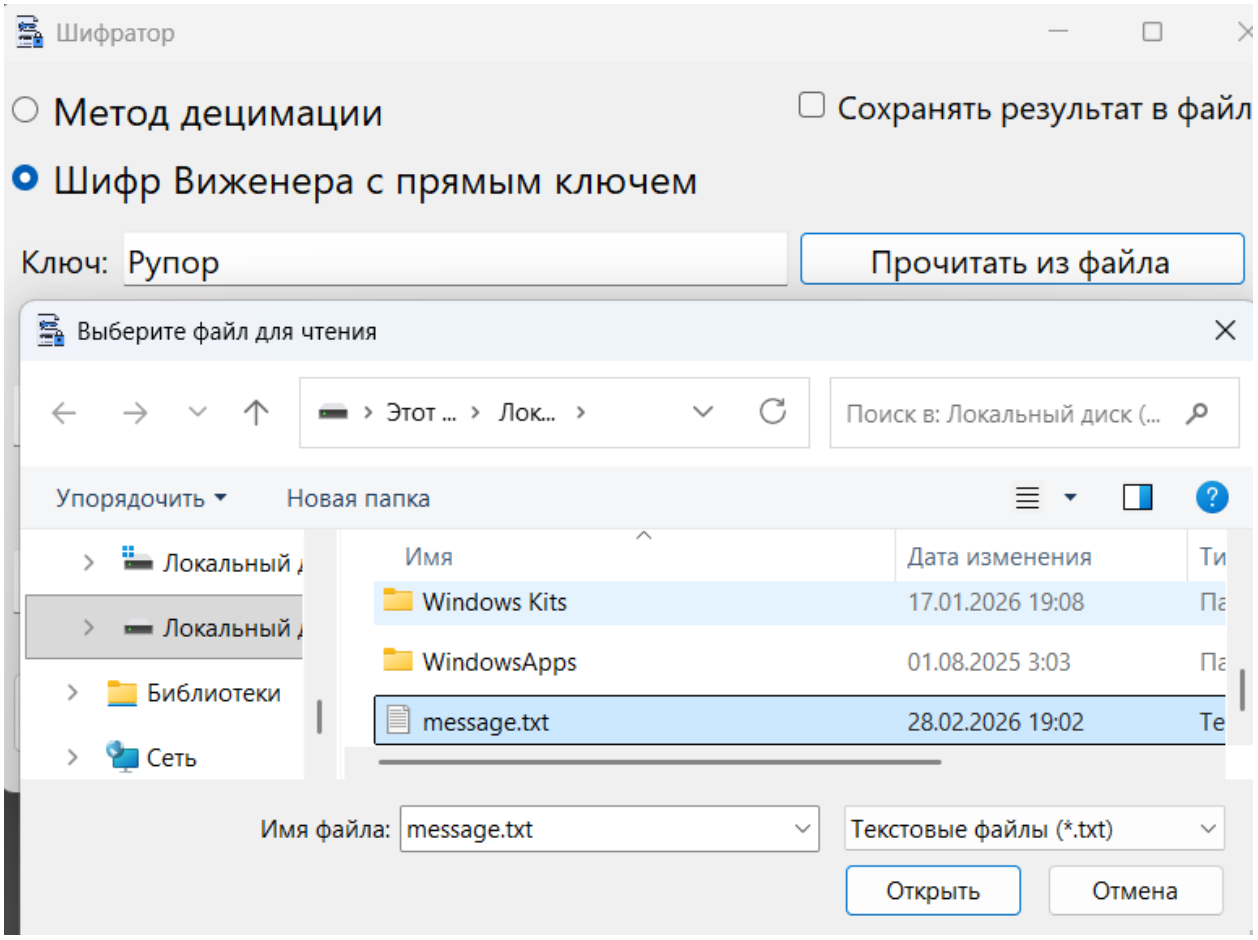
**Тестовая ситуация:** Загрузка исходных данных из файла и сохранение результата в файл.

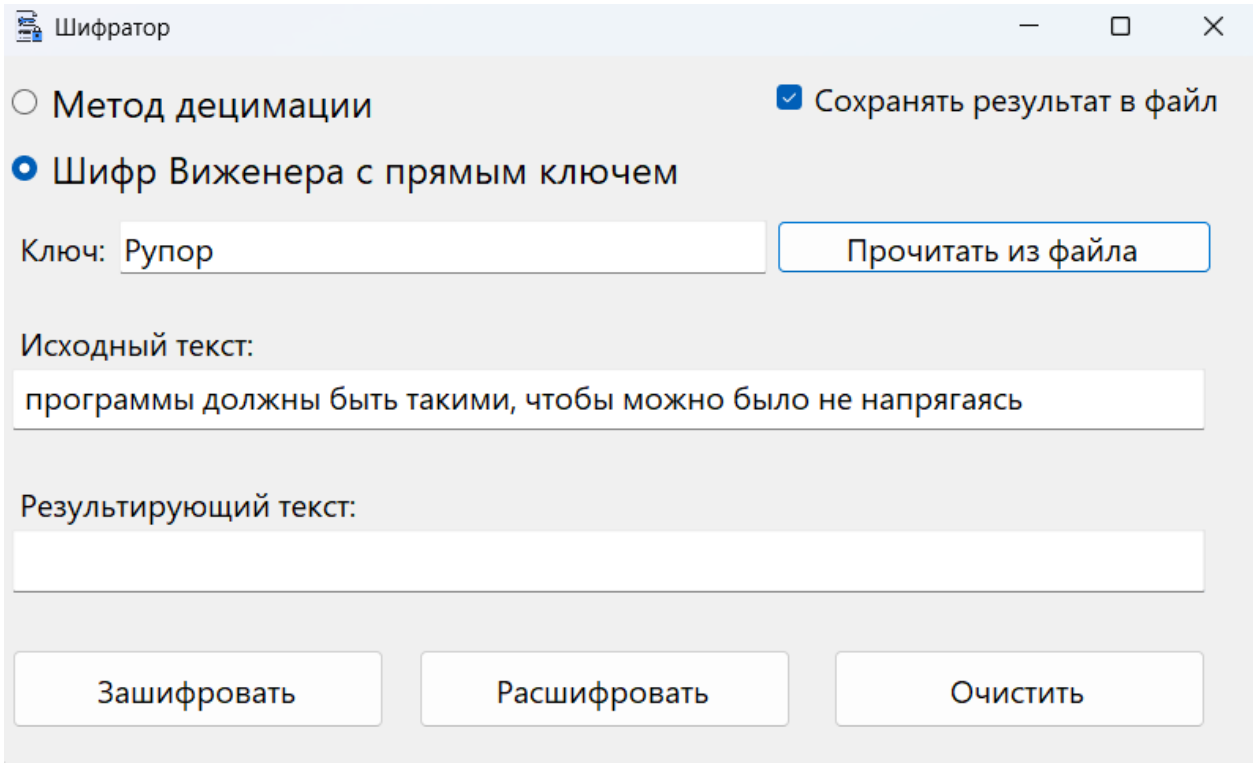
**Исходные данные:** Plaintext из message.txt
Key = “Рупор”

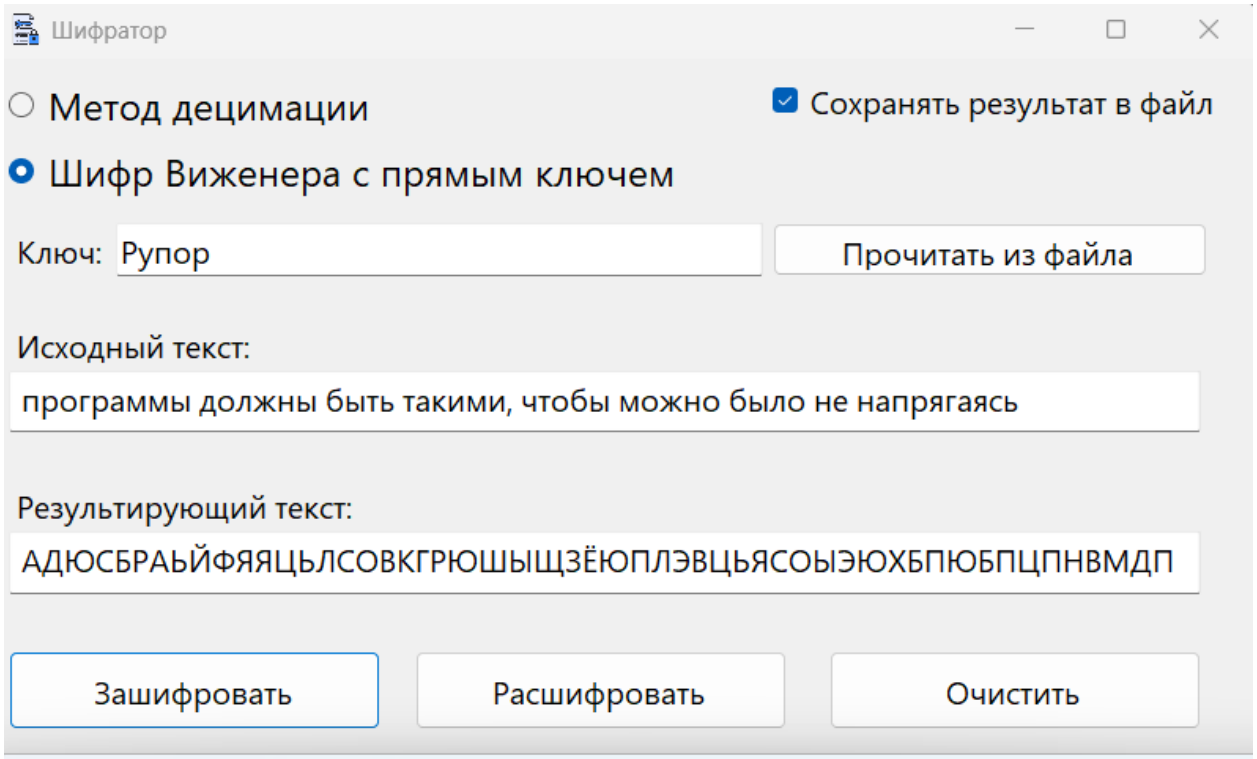
**Ожидаемый результат:**
Заполнение поля “Plaintext” данными из файла, сохранение результата в файл.

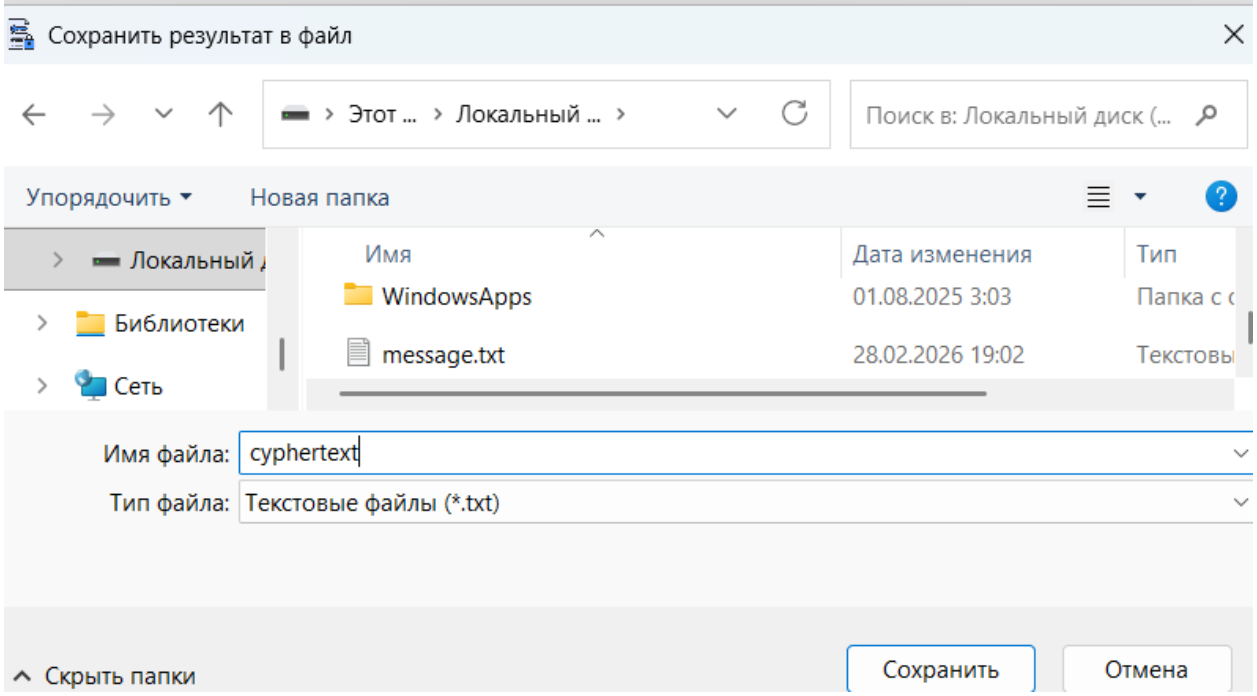
**Полученный результат:**

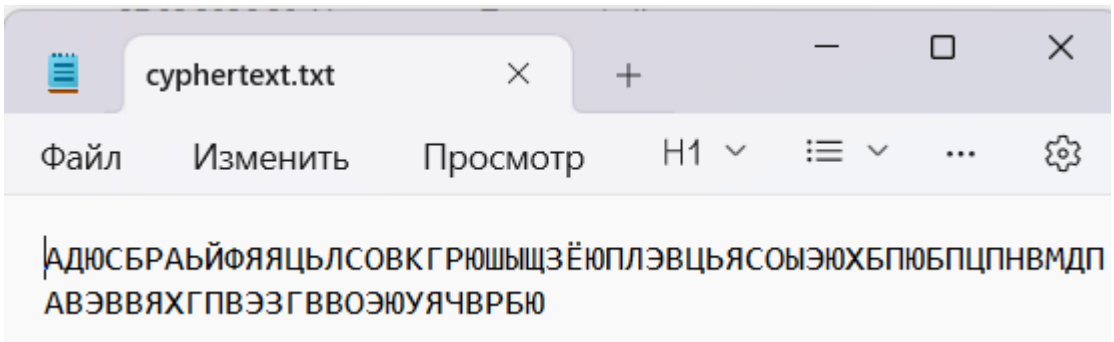


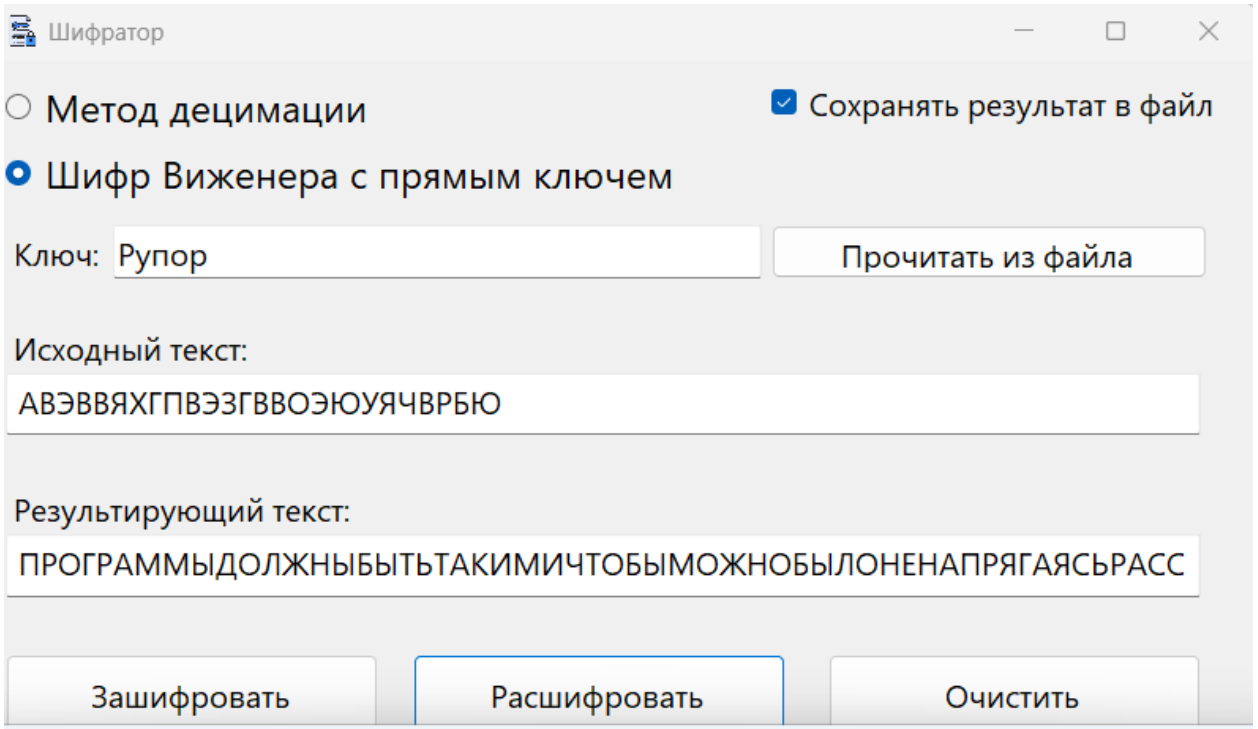

Шифратор
Метод децимации
Сохранять результат в файл
Шифр Виженера с прямым ключем
Ключ: Рупор
Прочитать из файла
Выберите файл для чтения
Этот ... › Лок... ›
Поиск в: Локальный диск (...
Упорядочить
Новая папка
Имя
Дата изменения
Windows Kits
17.01.2026 19:08
WindowsApps
01.08.2025 3:03
message.txt
28.02.2026 19:02
Библиотеки
Сеть
Имя файла: message.txt
Текстовые файлы (*.txt)
Открыть
Отмена

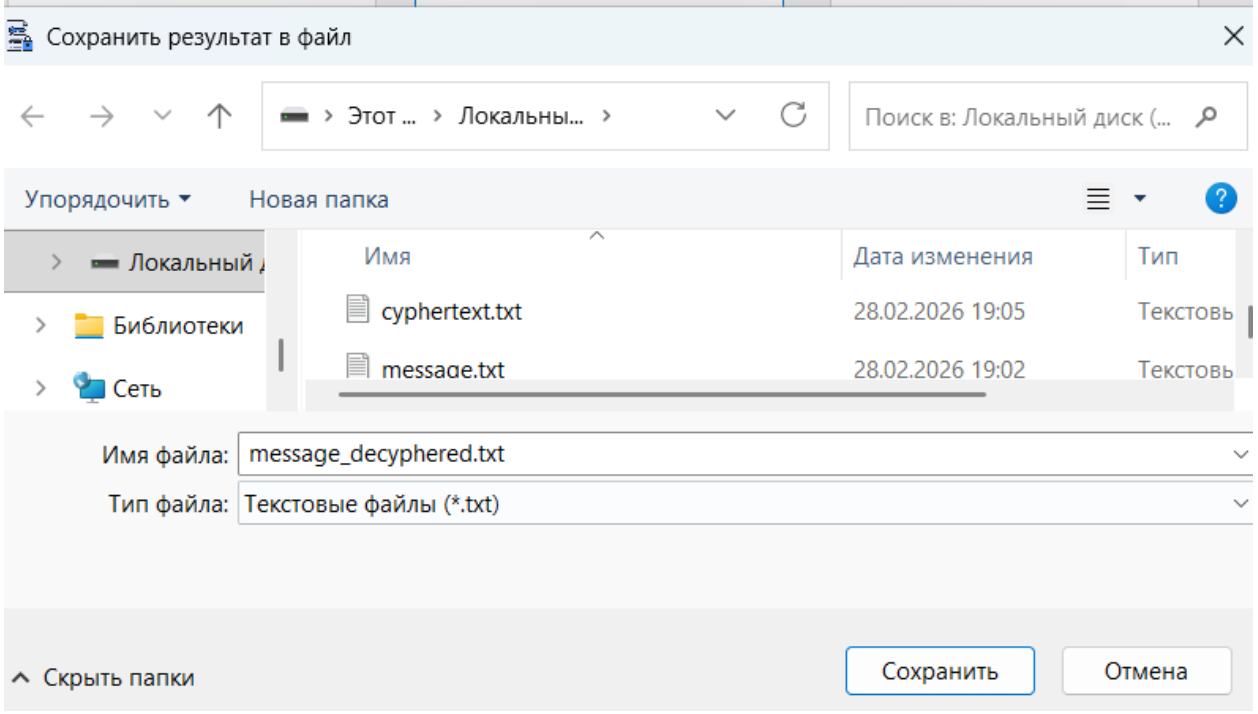

Шифратор
Метод децимации
Сохранять результат в файл
Шифр Виженера с прямым ключем
Ключ: Рупор
Прочитать из файла
Исходный текст:
программы должны быть такими, чтобы можно было не напрягаясь
Результирующий текст:
Зашифровать
Расшифровать
Очистить

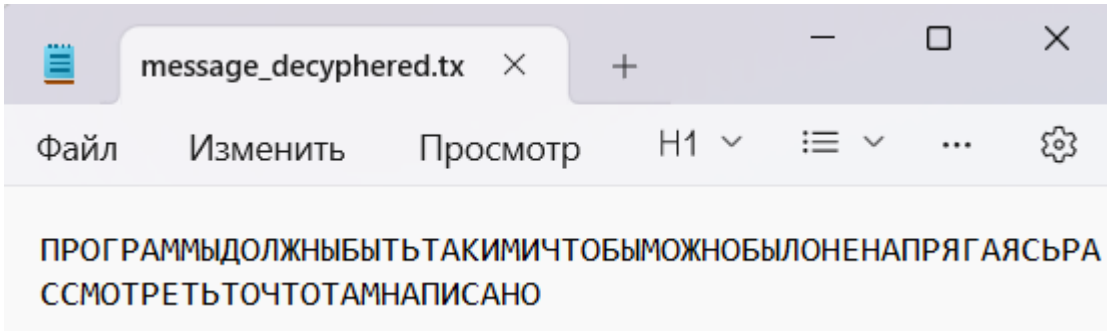

Шифратор
Метод децимации
Сохранять результат в файл
Шифр Виженера с прямым ключем
Ключ: Рупор
Прочитать из файла
Исходный текст:
программы должны быть такими, чтобы можно было не напрягаясь
Результирующий текст:
АДЮСБРАЬЙФЯЯЦЬЛСОВКГРЮШЫЩЗЁЮПЛЭВЦЬЯСОЫЭЮХБПЮБПЦПНВМДП
Зашифровать
Расшифровать
Очистить


Сохранить результат в файл
Этот ...
Локальный ...
Поиск в: Локальный диск (...
Упорядочить
Новая папка
Локальный
Библиотеки
Сеть
Имя
Дата изменения
Тип
WindowsApps
01.08.2025 3:03
message.txt
28.02.2026 19:02
Имя файла: cyphertext
Тип файла: Текстовые файлы (*.txt)
Скрыть папки
Сохранить
Отмена


cyphertext.txt
Файл
Изменить
Просмотр
H1
АДЮСБРАЬЙФЯЯЦЬЛСОВКГРЮШЫЩЗЁЮПЛЭВЦЬЯСОЫЭЮХБПЮБПЦПНВМДП
АВЭВВЯХГПВЭЗГВВОЭЮУЯЧВРБЮ


Шифратор
Метод децимации
Сохранять результат в файл
Шифр Виженера с прямым ключем
Ключ: Рупор
Прочитать из файла
Исходный текст:
АВЭВВЯХГПВЭЗГВВОЭЮУЯЧВРБЮ
Результирующий текст:
ПРОГРАММЫДОЛЖНЫБЫТЬТАКИМИЧТОБЫМОЖНОБЫЛОНЕНАПРЯГАЯСЬРАСС
Зашифровать
Расшифровать
Очистить


Сохранить результат в файл
Этот ...
Локальны...
Поиск в: Локальный диск (...
Упорядочить
Новая папка
Локальный
Библиотеки
Сеть
Имя
Дата изменения
Тип
cyphertext.txt
28.02.2026 19:05
Текстовь
message.txt
28.02.2026 19:02
Текстовь
Имя файла: message_decyphered.txt
Тип файла: Текстовые файлы (*.txt)
Скрыть папки
Сохранить
Отмена


message_decyphered.tx
Файл
Изменить
Просмотр
H1
ПРОГРАММЫДОЛЖНЫБЫТЬТАКИМИЧТОБЫМОЖНОБЫЛОНЕНАПРЯГАЯСЬРА
ССМОТРЕТЬТОЧТОТАМНАПИСАНО