УО «Белорусский государственный университет информатики и радиоэлектроники»

Кафедра ПОИТ

Отчет по лабораторной работе №1

по предмету «Теория информации»

Выполнила:

Мазалевич П.В.

гр. 451003

Проверила:

Болтак С.В.

Минск 2026

Вариант №5.

**Условие задания:**

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

- **«столбцовый метод» улучшенный**, текст на английском языке;

- **алгоритм Виженера**, самогенерирующийся 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.

**«Столбцовый метод» улучшенный**

1. *Дымовое тестирование:*

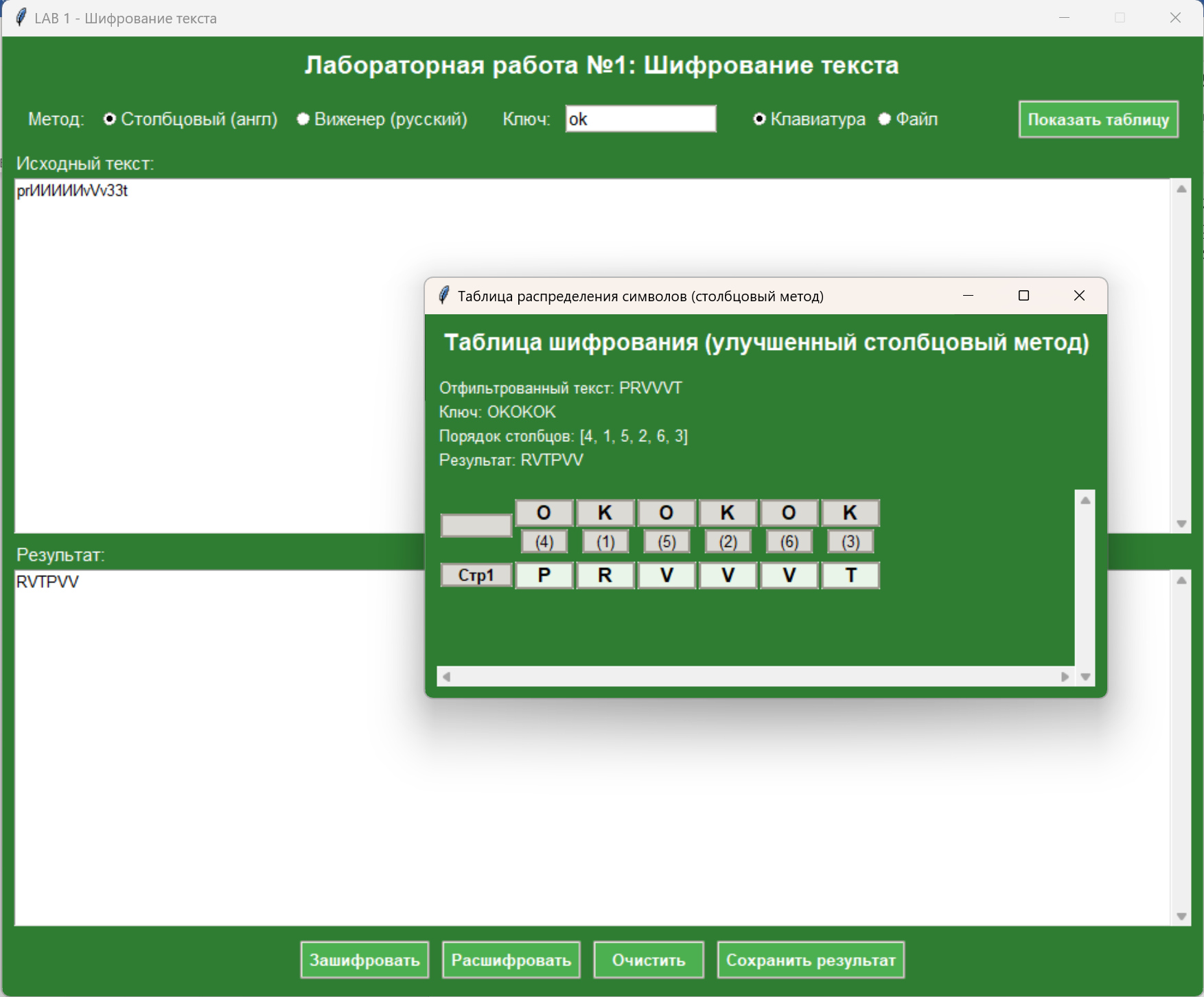
Тестовая фраза: prИИИИИvVv33t

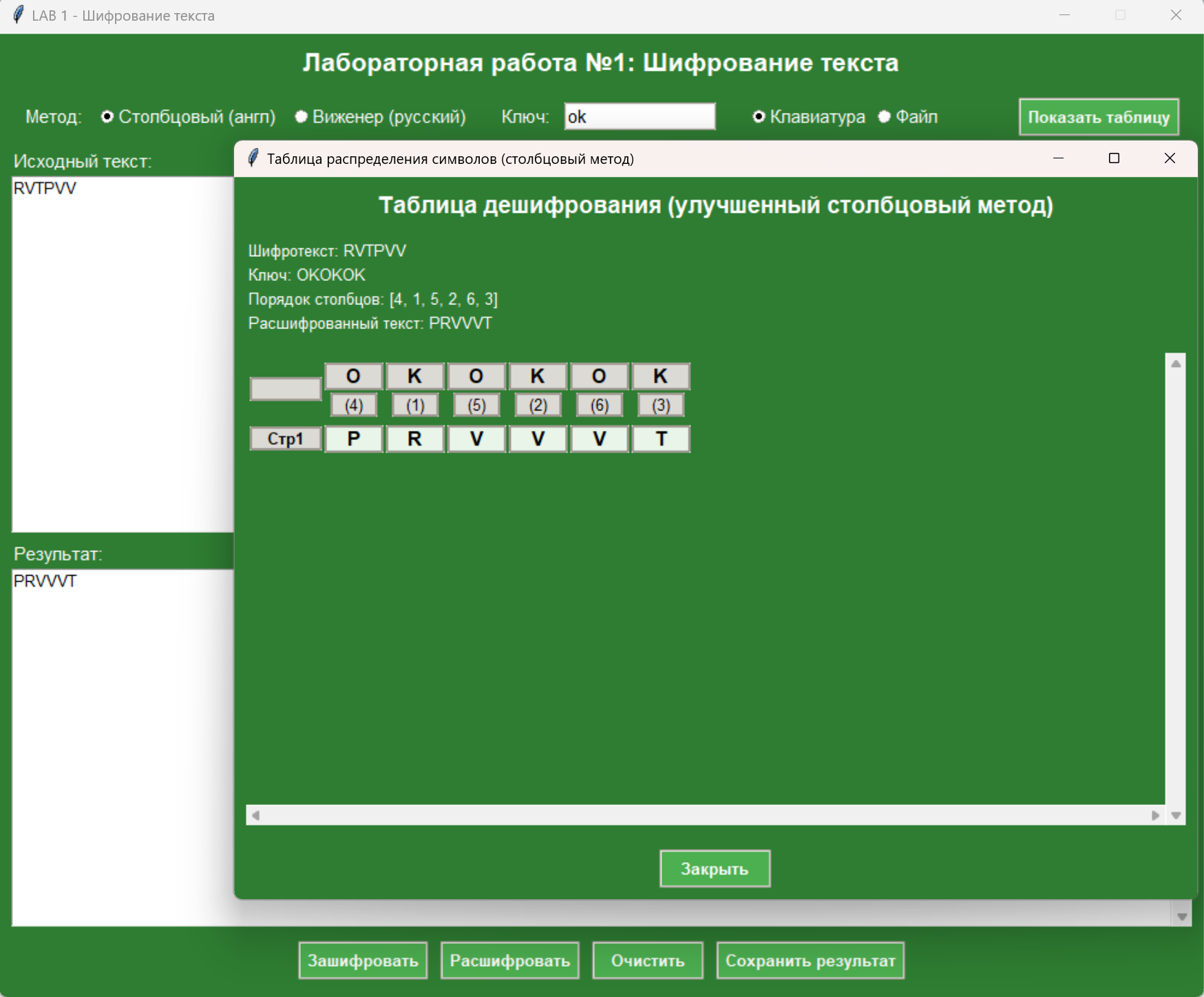
Ключ: ok

Таблица:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| O | K | O | K | O | K |
| 4 | 1 | 5 | 2 | 6 | 3 |
| P | R | V | V | V | T |

Шифротекст: RVTPVV





**ТЕСТ ПРОЙДЕН**

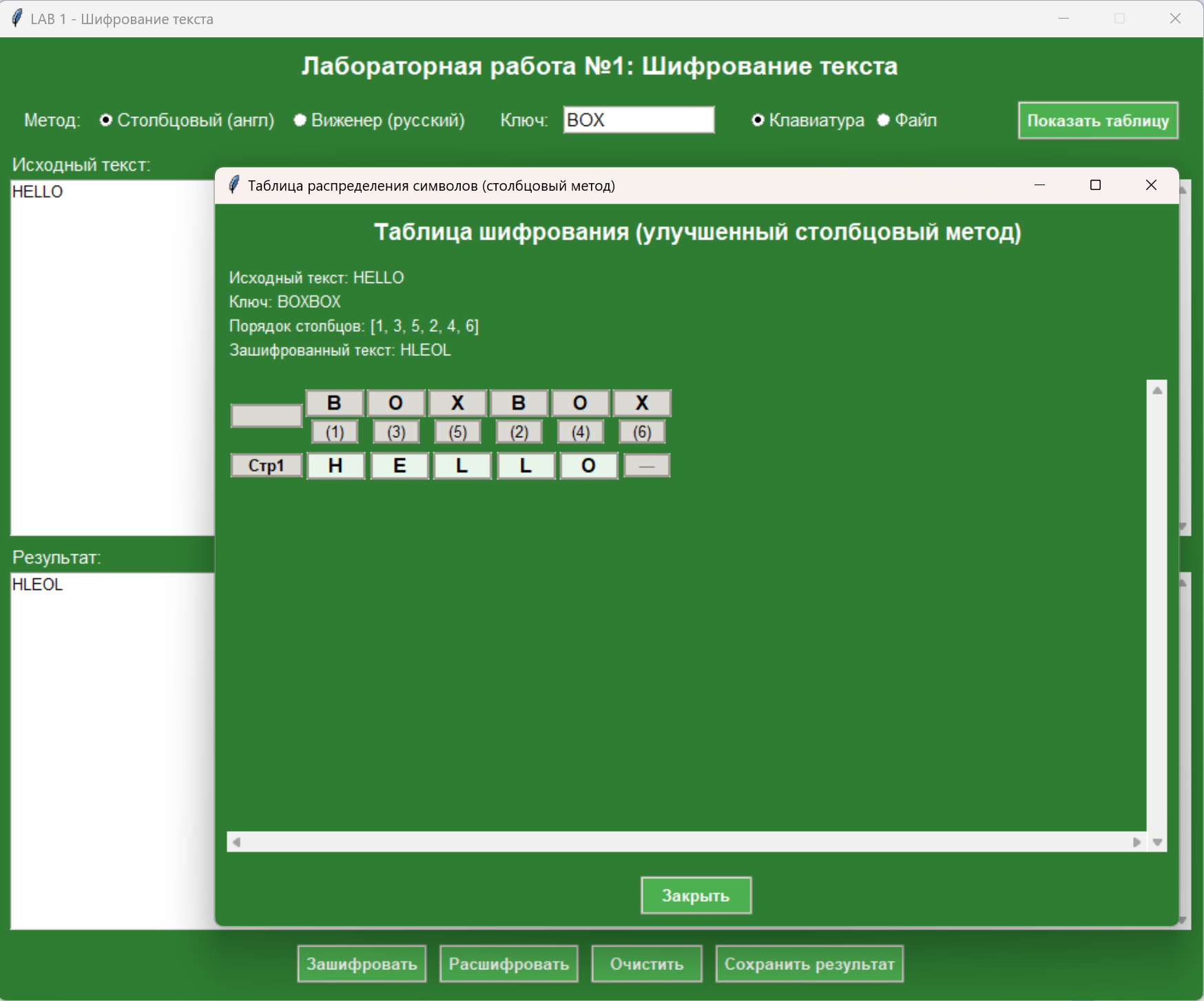
Тестовая фраза: HELLO

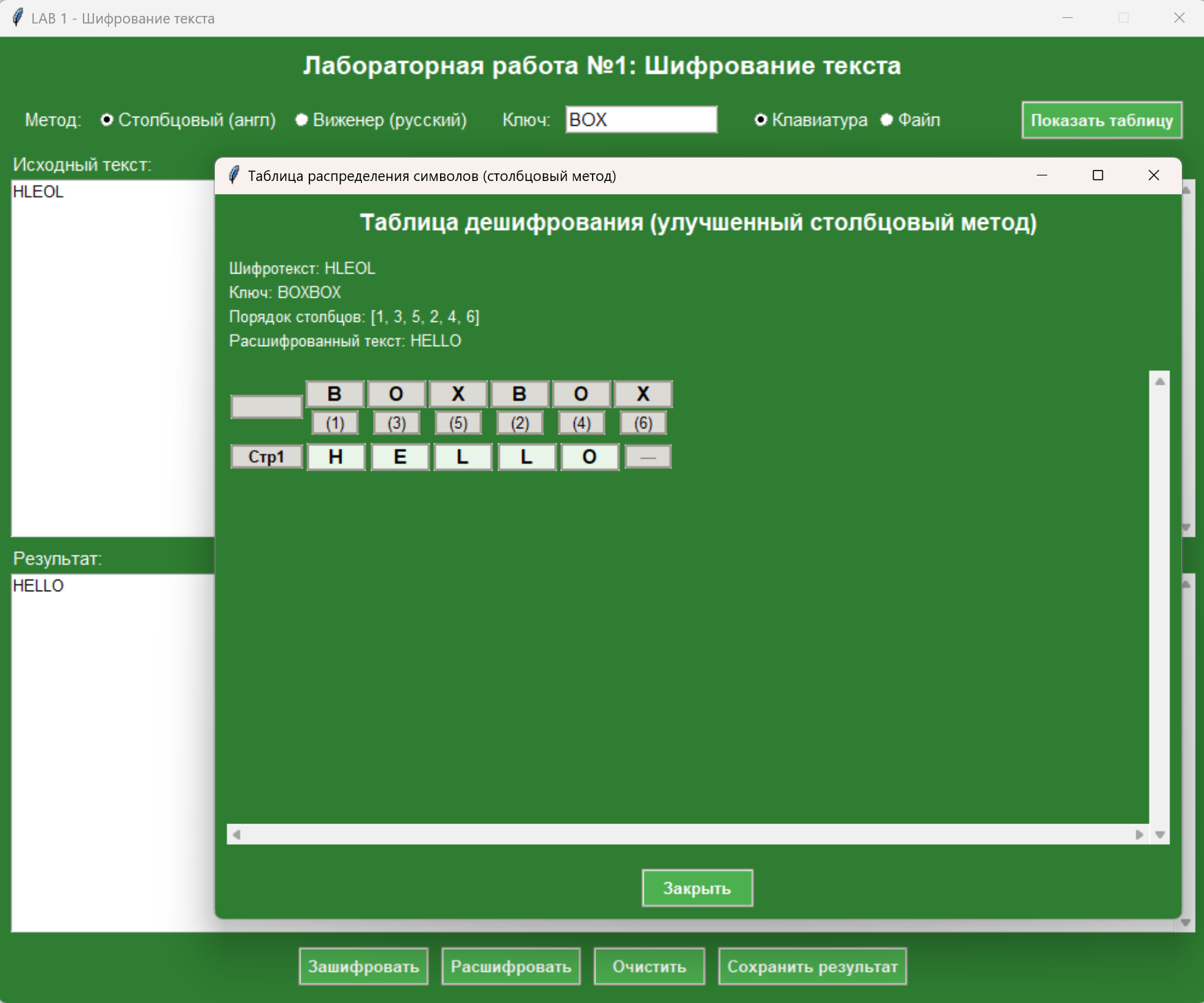
Ключ: BOX

Таблица:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| B | O | X | B | O | X |
| 1 | 3 | 5 | 2 | 4 | 6 |
| H | E | L | L | O |  |

Шифротекст: HLEOL





**ТЕСТ ПРОЙДЕН**

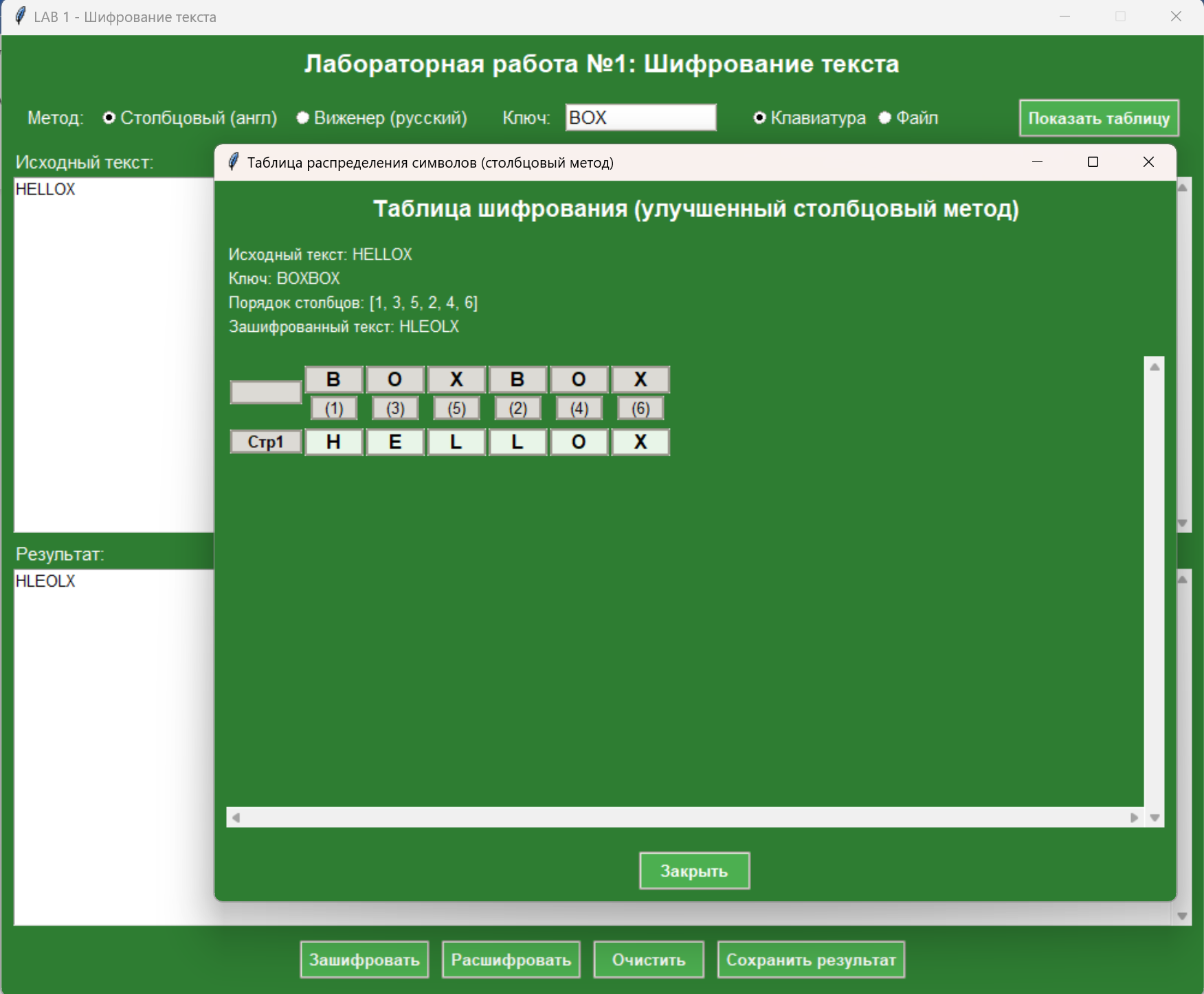
Тестовая фраза: HELLOX

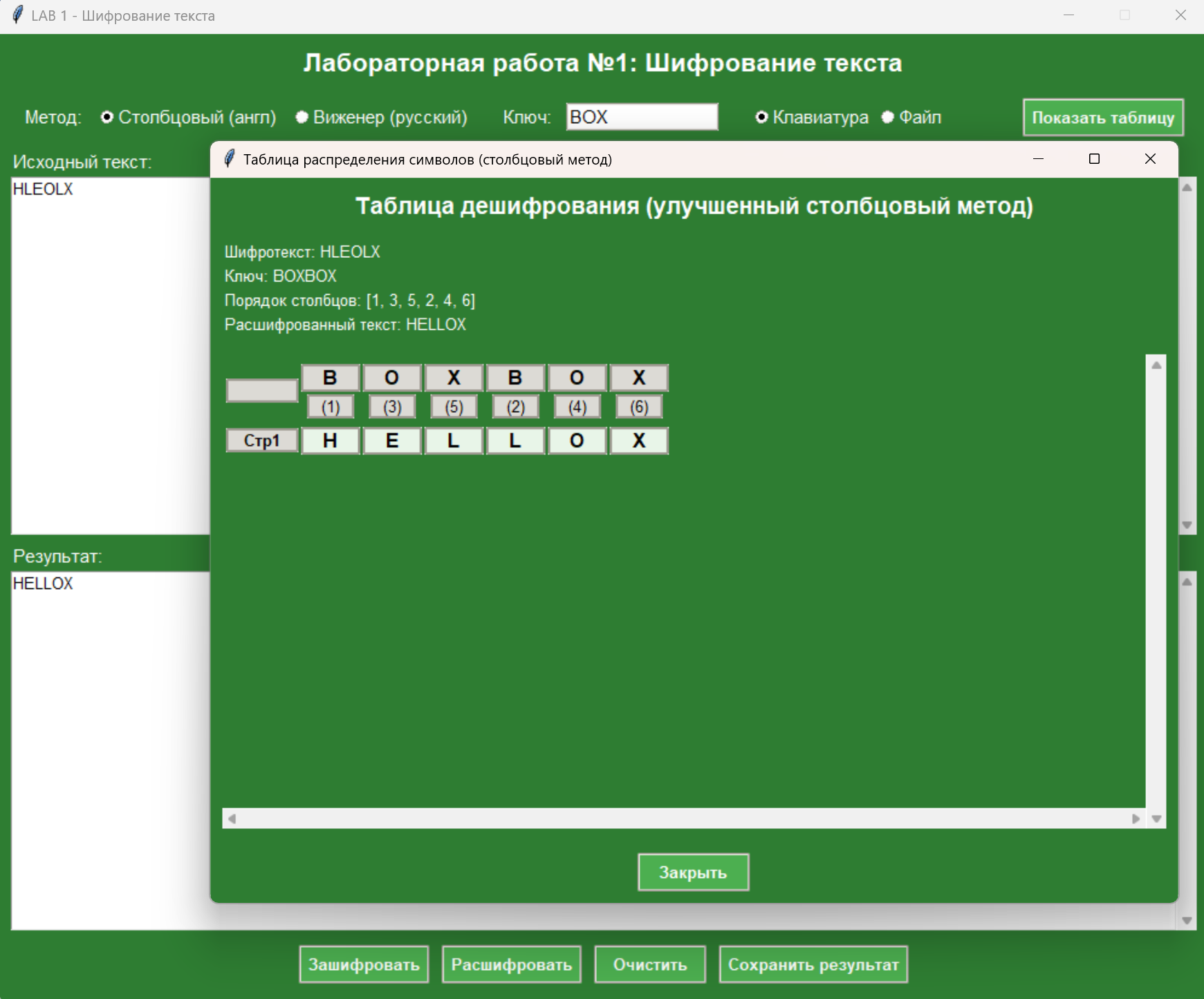
Ключ: BOX

Таблица:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| B | O | X | B | O | X |
| 1 | 3 | 5 | 2 | 4 | 6 |
| H | E | L | L | O | X |

Шифротекст: HLEOLX

****

****

**ТЕСТ ПРОЙДЕН**

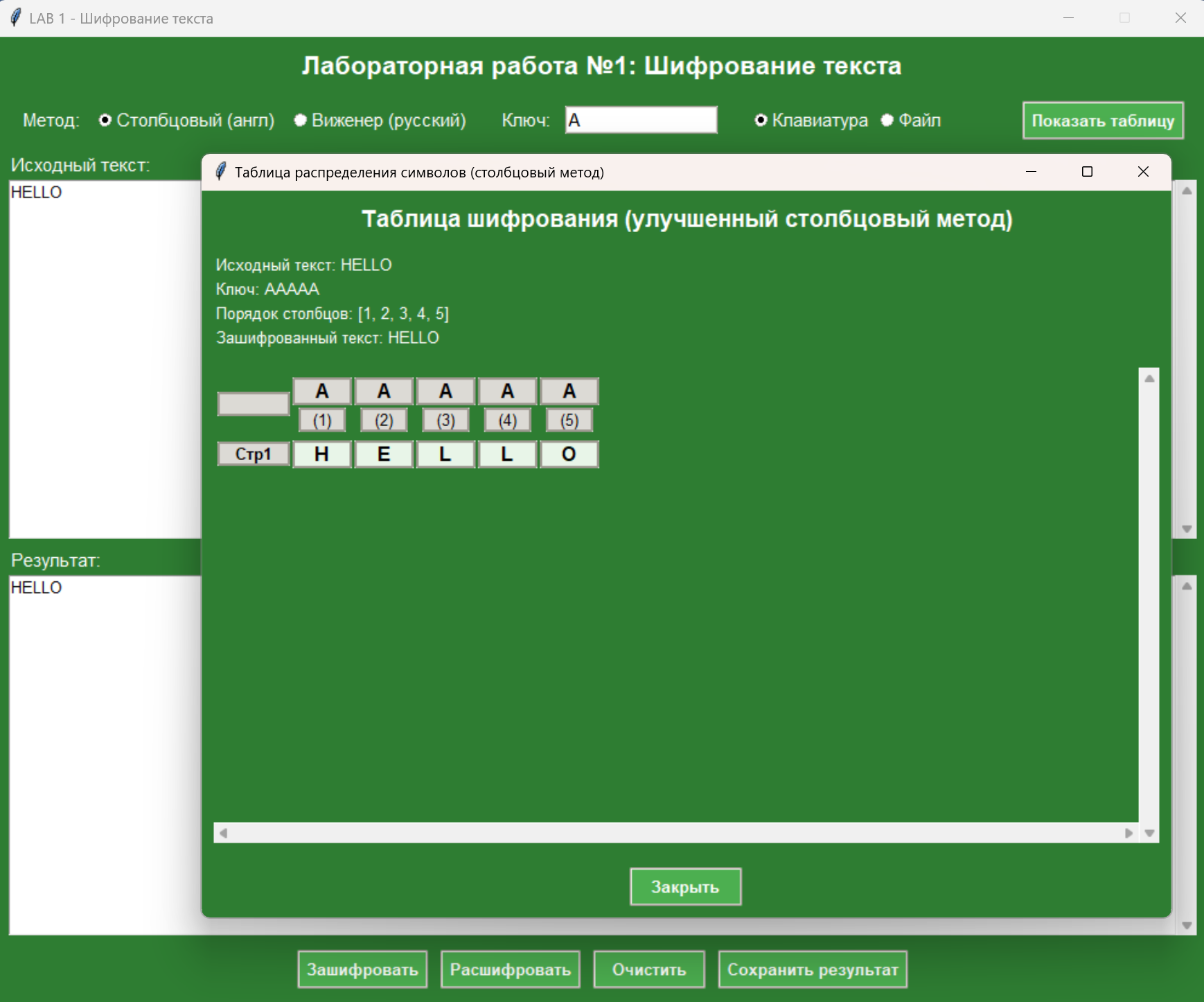
3. Крайние значения ключа:

Тестовая фраза: HELLO

Ключ: A

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| A | A | A | A | A |
| 1 | 2 | 3 | 4 | 5 |
| H | E | L | L | O |

Шифротекст: HELLO



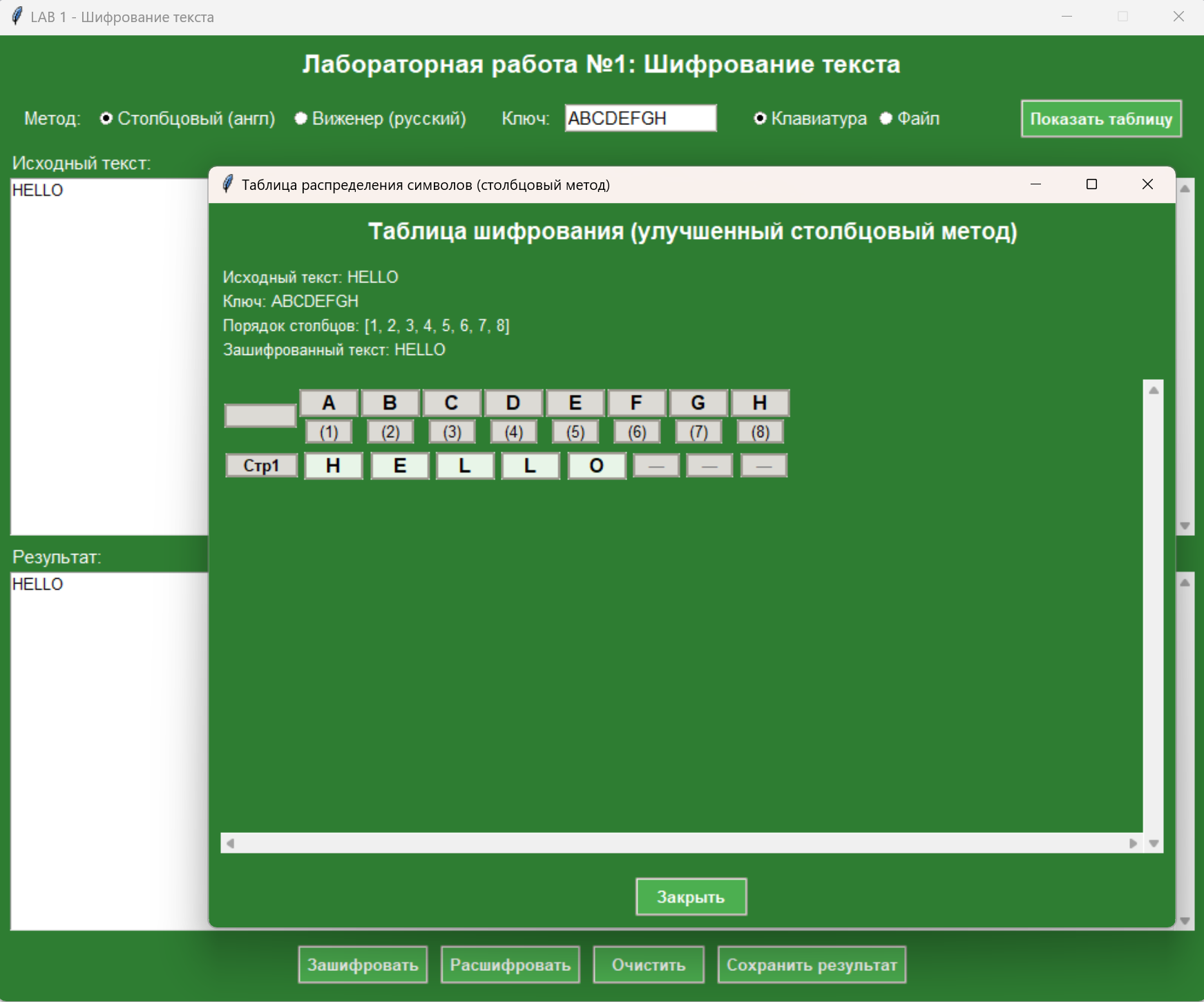
**ТЕСТ ПРОЙДЕН**

Тестовая фраза: HELLO

Ключ: ABCDEFGH

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| A | B | C | D | E | F | G | H |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| H | E | L | L | O |  |  |  |

Шифротекст: HELLO

****

**ТЕСТ ПРОЙДЕН**

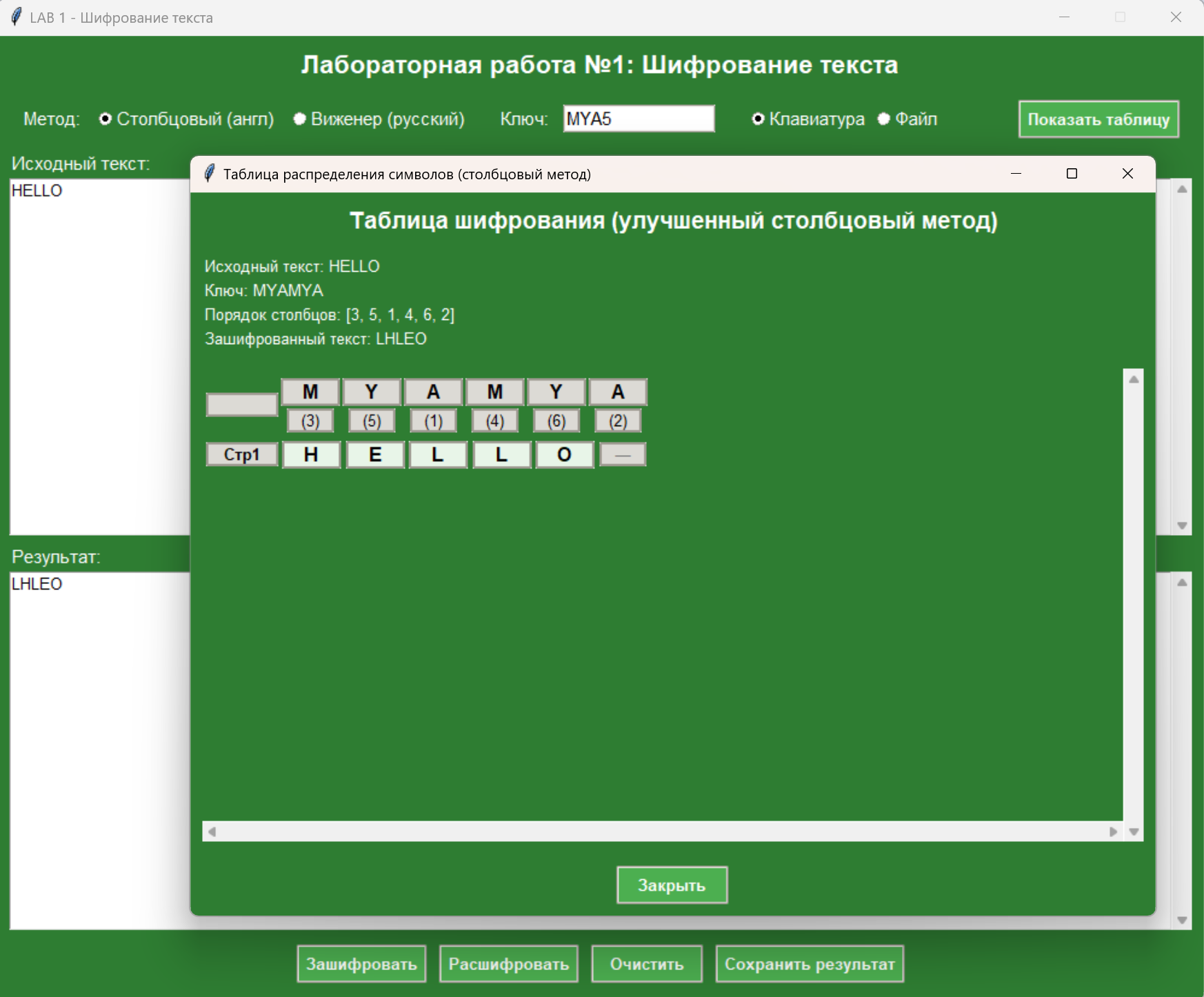
4. Ключ, содержащий недопустимые символы (после нажатия ключ преобразуется в правильный вид):

Тестовая фраза: HELLO

Ключ: MYA5

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| M | Y | A | M | Y | A |
| 3 | 5 | 1 | 4 | 6 | 2 |
| H | E | L | L | O |  |

Шифротекст: LHLEO



**ТЕСТ ПРОЙДЕН**

**ШИФР ВИЖЕНЕРА**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **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** | **Ъ** | **Ы** | **Ь** | **Э** | **Ю** | **Я** |
| **А** | 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 | Ъ | Ы | Ь | Э | Ю | Я |
| **Б** | 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 | Ъ | Ы | Ь | Э | Ю | Я | А |
| **В** | 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 | Ъ | Ы | Ь | Э | Ю | Я | А | Б |
| **Г** | Г | Д | Е | Ё | Ж | З | И | Й | К | Л | М | Н | О | П | Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ъ | Ы | Ь | Э | Ю | Я | А | Б | В |
| **Д** | Д | Е | Ё | Ж | З | И | Й | К | Л | М | Н | О | П | Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ъ | Ы | Ь | Э | Ю | Я | А | Б | В | Г |
| **Е** | Е | Ё | Ж | З | И | Й | К | Л | М | Н | О | П | Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ъ | Ы | Ь | Э | Ю | Я | А | Б | В | Г | Д |
| **Ё** | Ё | Ж | З | И | Й | К | Л | М | Н | О | П | Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ъ | Ы | Ь | Э | Ю | Я | А | Б | В | Г | Д | Е |
| **Ж** | Ж | З | И | Й | К | Л | М | Н | О | П | Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ъ | Ы | Ь | Э | Ю | Я | А | Б | В | Г | Д | Е | Ё |
| **З** | З | И | Й | К | Л | М | Н | О | П | Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ъ | Ы | Ь | Э | Ю | Я | А | Б | В | Г | Д | Е | Ё | Ж |
| **И** | И | Й | К | Л | М | Н | О | П | Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ъ | Ы | Ь | Э | Ю | Я | А | Б | В | Г | Д | Е | Ё | Ж | З |
| **Й** | Й | К | Л | М | Н | О | П | Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ъ | Ы | Ь | Э | Ю | Я | А | Б | В | Г | Д | Е | Ё | Ж | З | И |
| **К** | К | Л | М | Н | О | П | Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ъ | Ы | Ь | Э | Ю | Я | А | Б | В | Г | Д | Е | Ё | Ж | З | И | Й |
| **Л** | Л | М | Н | О | П | Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ъ | Ы | Ь | Э | Ю | Я | А | Б | В | Г | Д | Е | Ё | Ж | З | И | Й | К |
| **М** | М | Н | О | П | Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ъ | Ы | Ь | Э | Ю | Я | А | Б | В | Г | Д | Е | Ё | Ж | З | И | Й | К | Л |
| **Н** | Н | О | П | Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ъ | Ы | Ь | Э | Ю | Я | А | Б | В | Г | Д | Е | Ё | Ж | З | И | Й | К | Л | М |
| **О** | О | П | Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ъ | Ы | Ь | Э | Ю | Я | А | Б | В | Г | Д | Е | Ё | Ж | З | И | Й | К | Л | М | Н |
| **П** | П | Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ъ | Ы | Ь | Э | Ю | Я | А | Б | В | Г | Д | Е | Ё | Ж | З | И | Й | К | Л | М | Н | О |
| **Р** | Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ъ | Ы | Ь | Э | Ю | Я | А | Б | В | Г | Д | Е | Ё | Ж | З | И | Й | К | Л | М | Н | О | П |
| **С** | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ъ | Ы | Ь | Э | Ю | Я | А | Б | В | Г | Д | Е | Ё | Ж | З | И | Й | К | Л | М | Н | О | П | Р |
| **Т** | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ъ | Ы | Ь | Э | Ю | Я | А | Б | В | Г | Д | Е | Ё | Ж | З | И | Й | К | Л | М | Н | О | П | Р | С |
| **У** | У | Ф | Х | Ц | Ч | Ш | Щ | Ъ | Ы | Ь | Э | Ю | Я | А | Б | В | Г | Д | Е | Ё | Ж | З | И | Й | К | Л | М | Н | О | П | Р | С | Т |
| **Ф** | Ф | Х | Ц | Ч | Ш | Щ | Ъ | Ы | Ь | Э | Ю | Я | А | Б | В | Г | Д | Е | Ё | Ж | З | И | Й | К | Л | М | Н | О | П | Р | С | Т | У |
| **Х** | Х | Ц | Ч | Ш | Щ | Ъ | Ы | Ь | Э | Ю | Я | А | Б | В | Г | Д | Е | Ё | Ж | З | И | Й | К | Л | М | Н | О | П | Р | С | Т | У | Ф |
| **Ц** | Ц | Ч | Ш | Щ | Ъ | Ы | Ь | Э | Ю | Я | А | Б | В | Г | Д | Е | Ё | Ж | З | И | Й | К | Л | М | Н | О | П | Р | С | Т | У | Ф | Х |
| **Ч** | Ч | Ш | Щ | Ъ | Ы | Ь | Э | Ю | Я | А | Б | В | Г | Д | Е | Ё | Ж | З | И | Й | К | Л | М | Н | О | П | Р | С | Т | У | Ф | Х | Ц |
| **Ш** | Ш | Щ | Ъ | Ы | Ь | Э | Ю | Я | 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 |
| **Щ** | Щ | Ъ | Ы | Ь | Э | Ю | Я | 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 |
| **Ъ** | Ъ | Ы | Ь | Э | Ю | Я | 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 |
| **Ы** | Ы | Ь | Э | Ю | Я | 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 | Ъ |
| **Ь** | Ь | Э | Ю | Я | 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 | Ъ | Ы |
| **Э** | Э | Ю | Я | 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 | Ъ | Ы | Ь |
| **Ю** | Ю | Я | 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 | Ъ | Ы | Ь | Э |
| **Я** | Я | 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 | Ъ | Ы | Ь | Э | Ю |

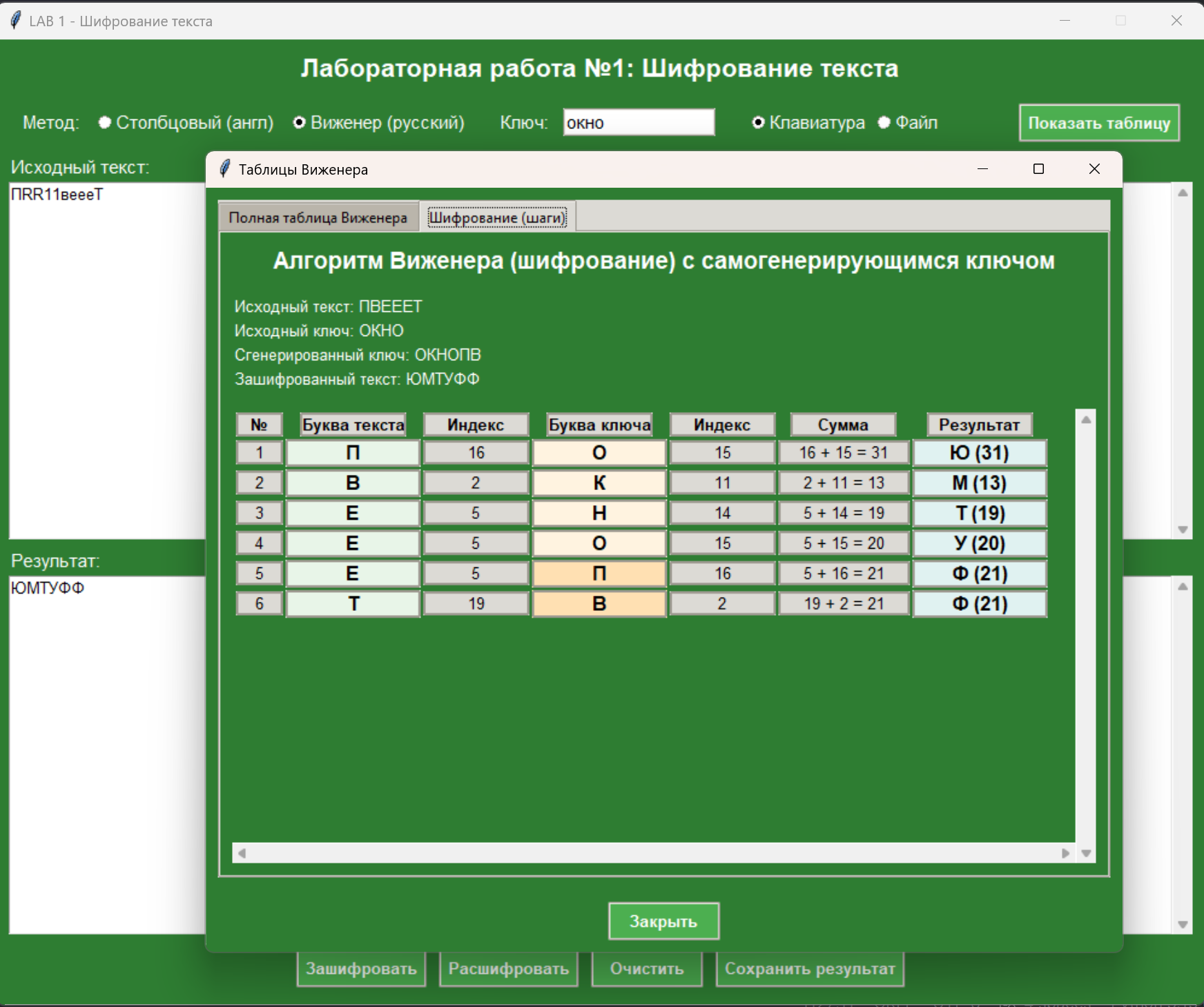
1. *Дымовое тестирование:*

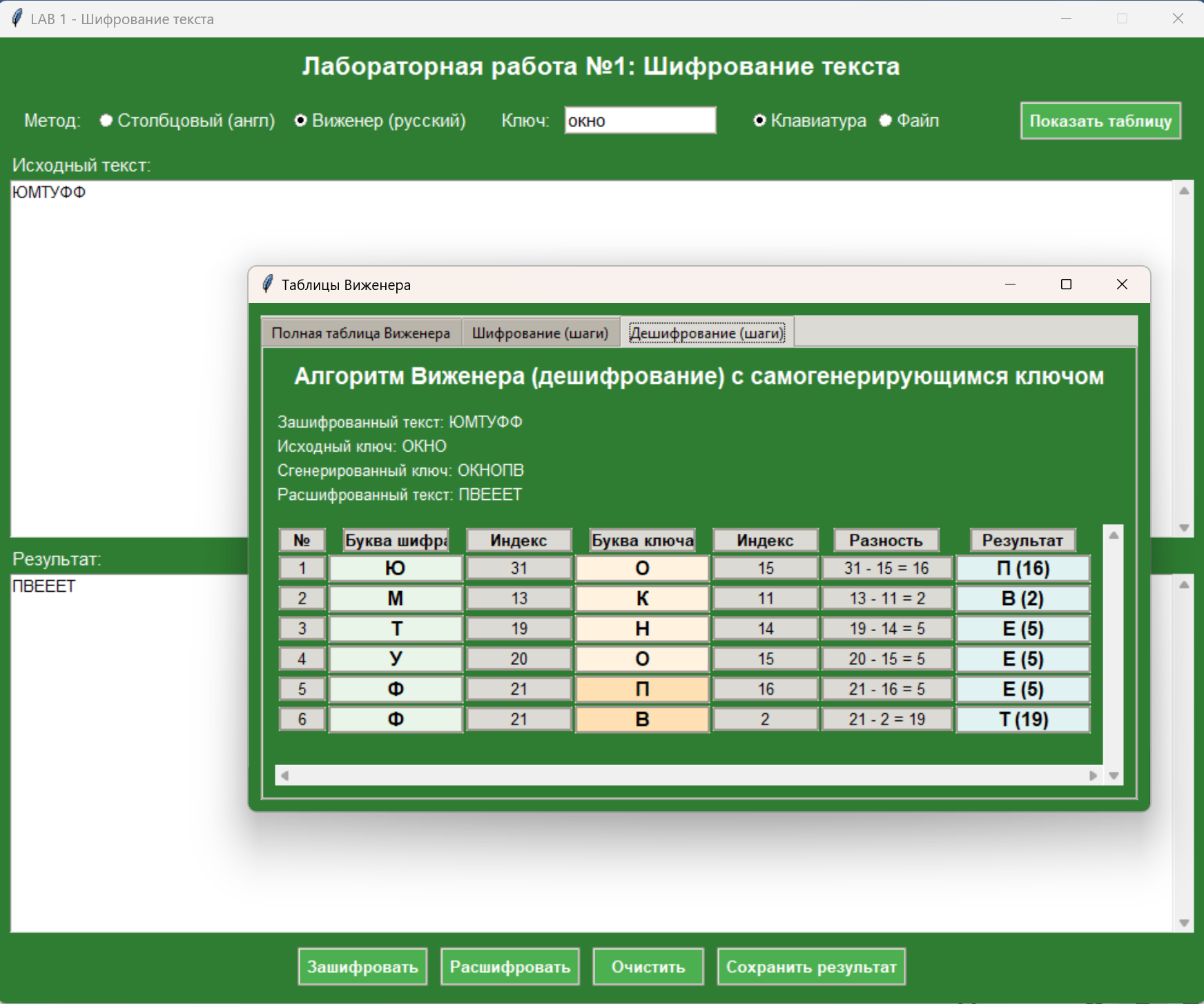
Тестовая фраза: ПRR11веееТ

Ключ: окно

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| П | В | Е | Е | Е | Т |
| О | К | Н | О | П | В |
| Ю | М | Т | У | Ф | Ф |

Шифротекст: ЮМТУФФ





**ТЕСТ ПРОЙДЕН**

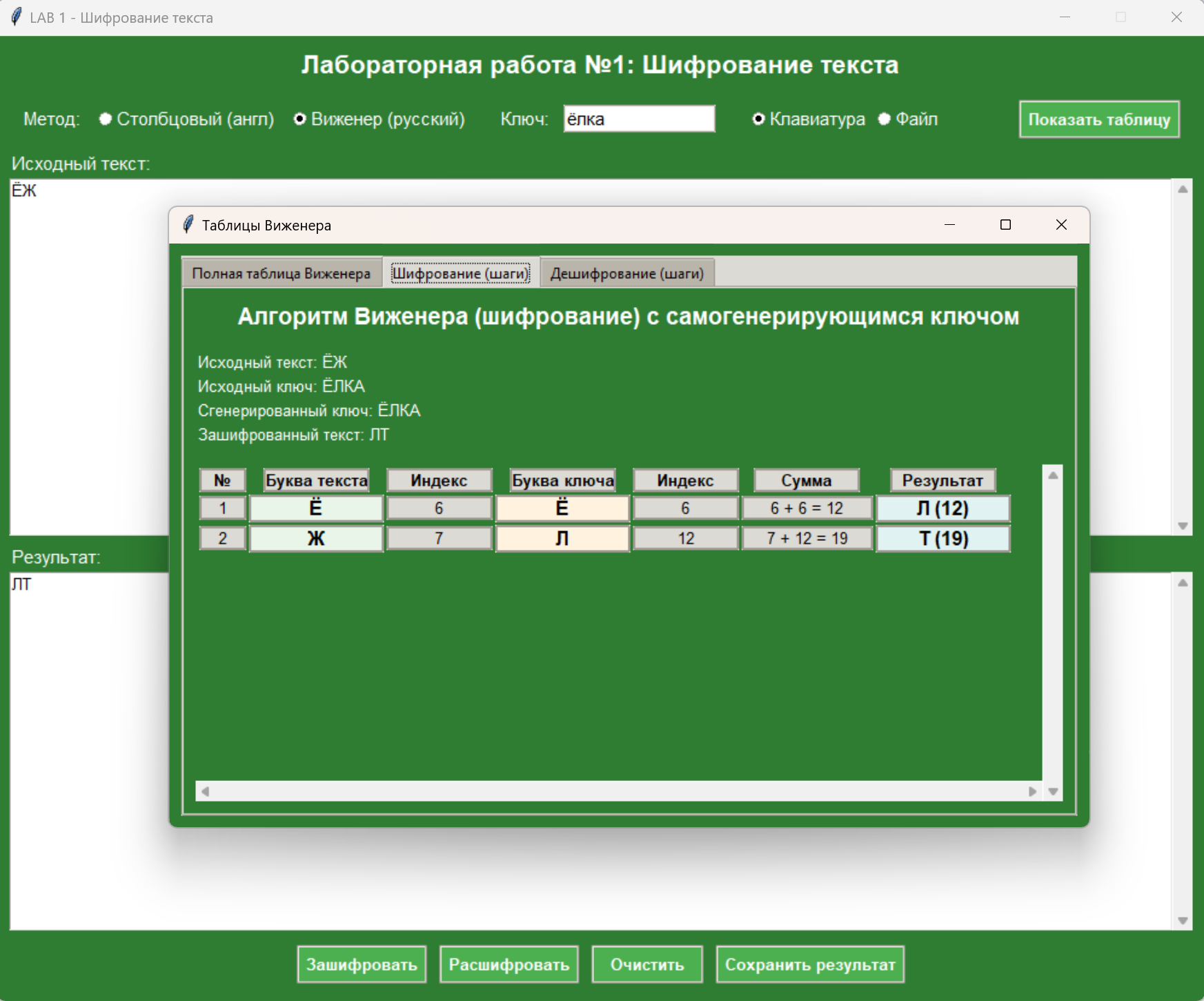
1. Тестовая фраза, содержащая букву Ё:

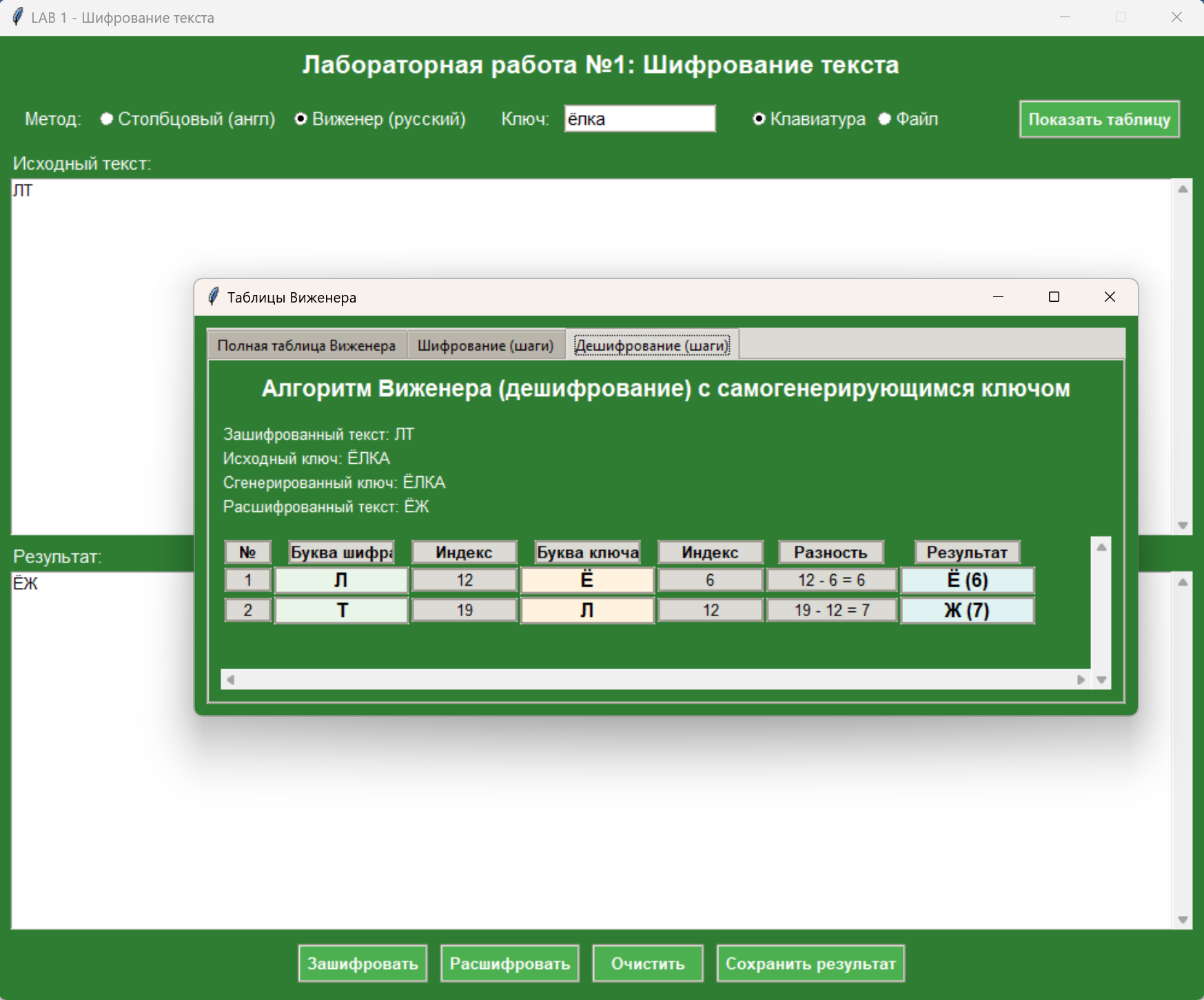
Тестовая фраза: ЁЖ

Ключ: ёлка

|  |  |
| --- | --- |
| Ё | Ж |
| Ё | Л |
| Л | Т |

Шифротекст: ЛТ





**ТЕСТ ПРОЙДЕН**

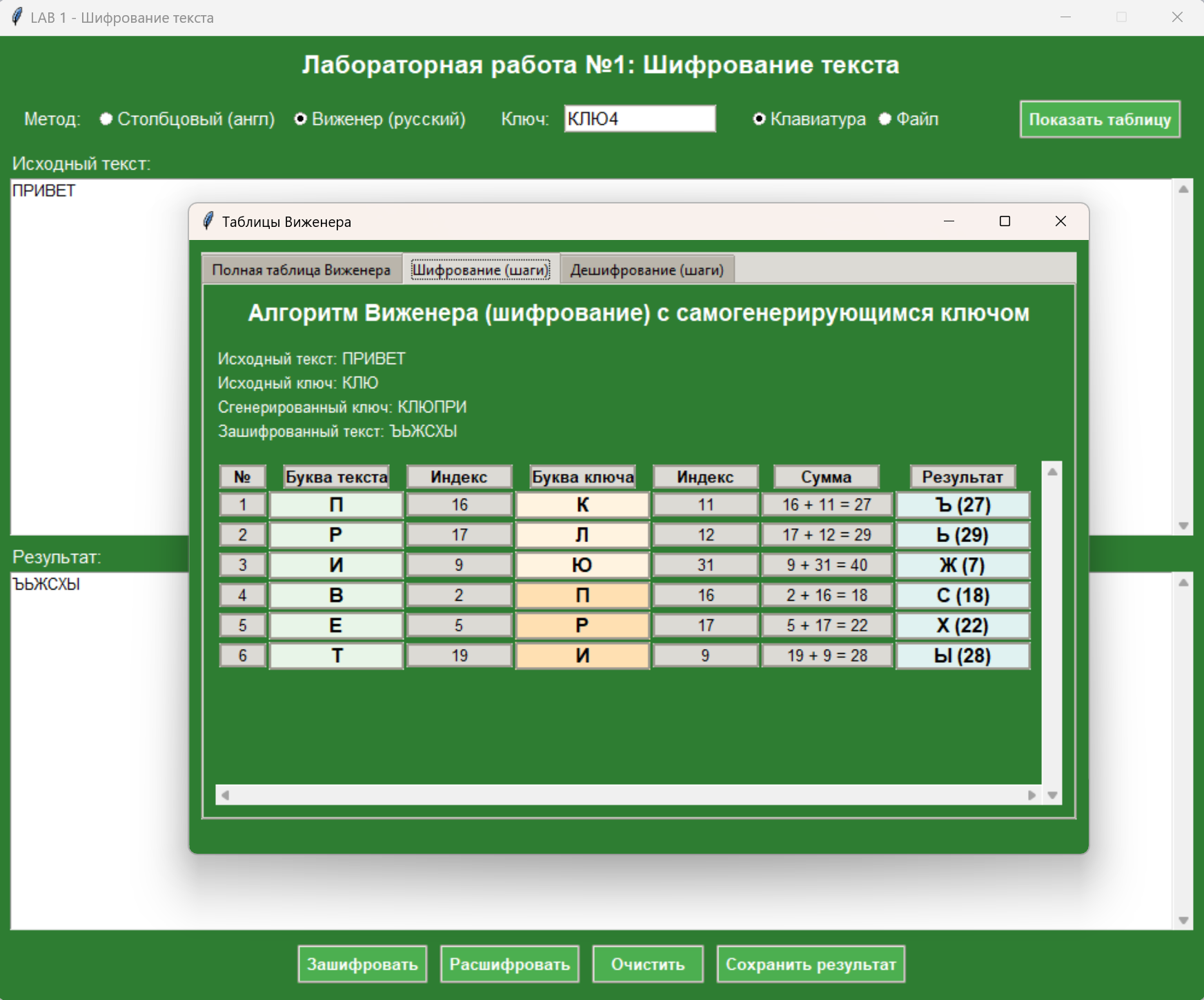
1. Ввод ключа с недопустимыми символами(после нажатия на кнопку расшифровать или зашифровать ключ преобразуется в правильный вид)

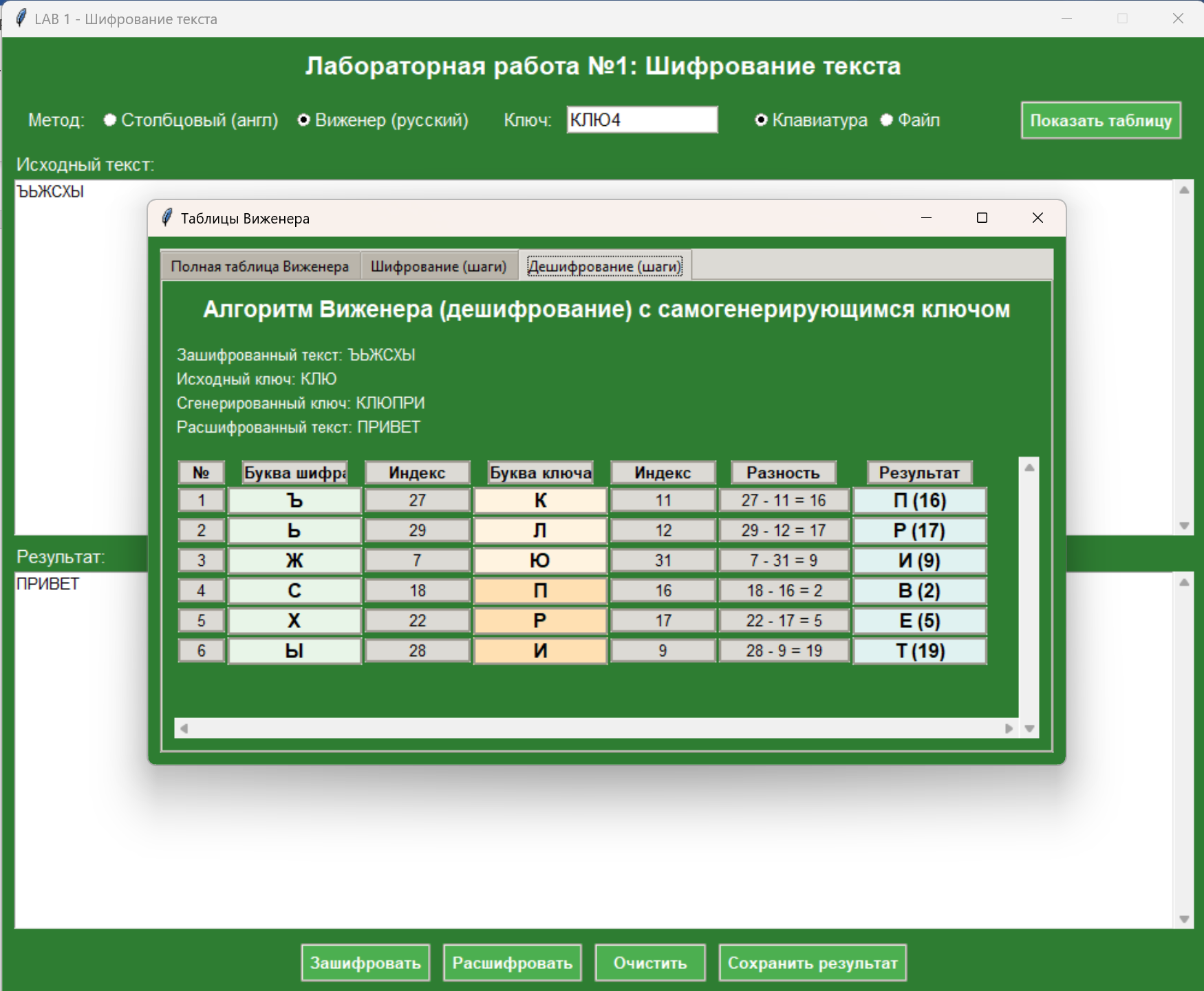
Тестовая фраза: ПРИВЕТ

Ключ: КЛЮ4

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| П | Р | И | В | Е | Т |
| К | Л | Ю | П | Р | И |
| Ъ | Ь | Ж | С | Х | Ы |

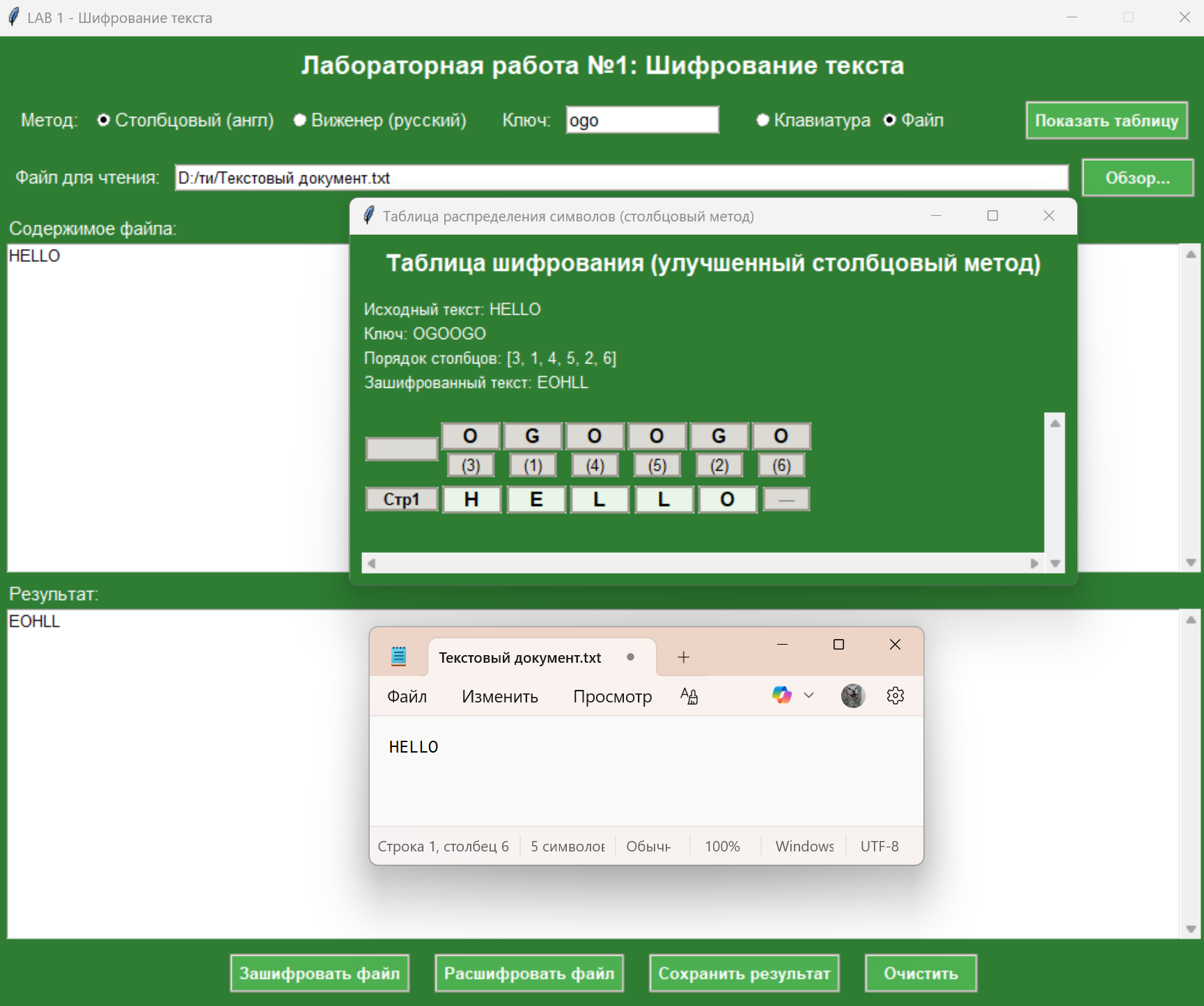
Шифротекст: ЪЬЖСХЫ

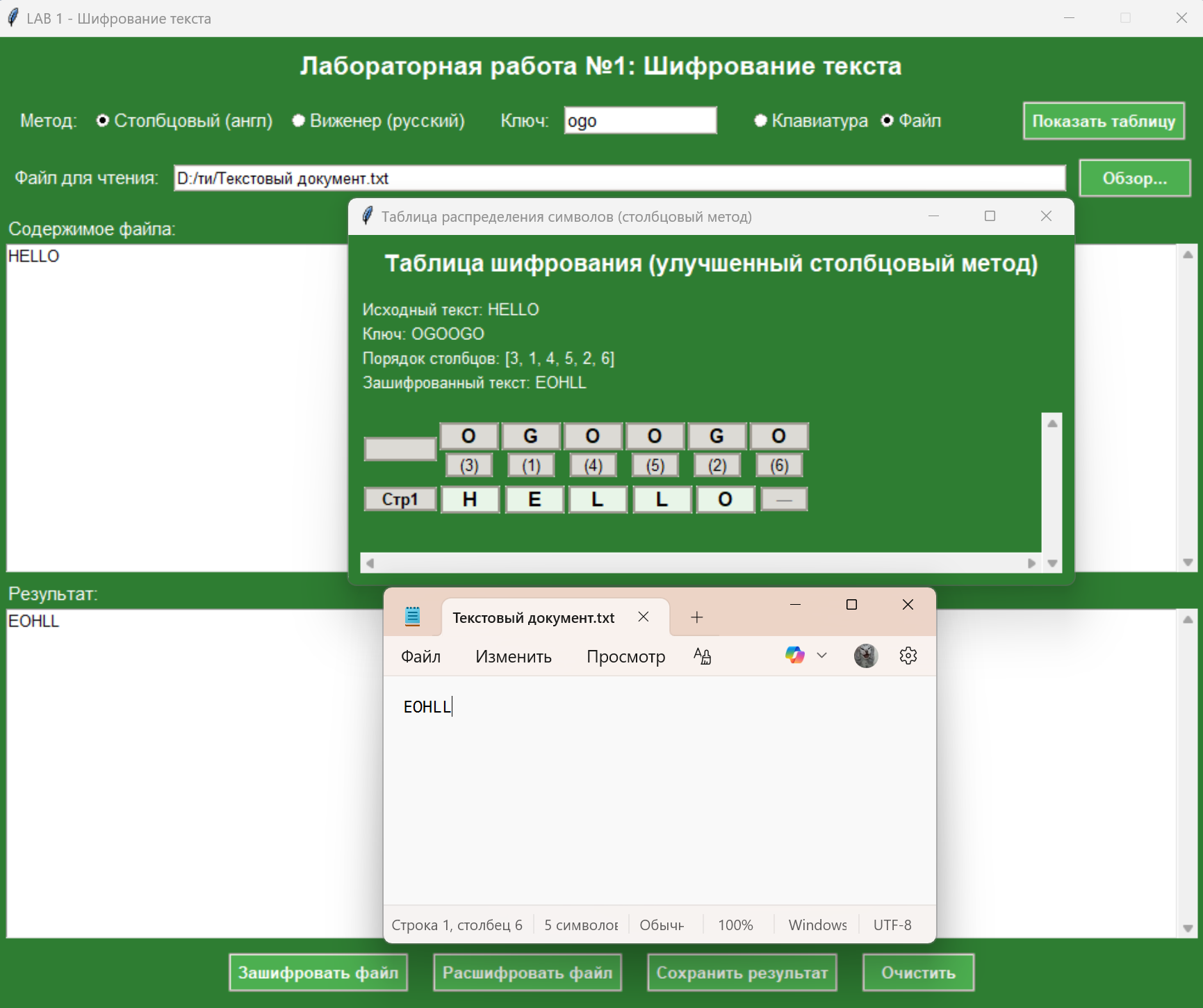


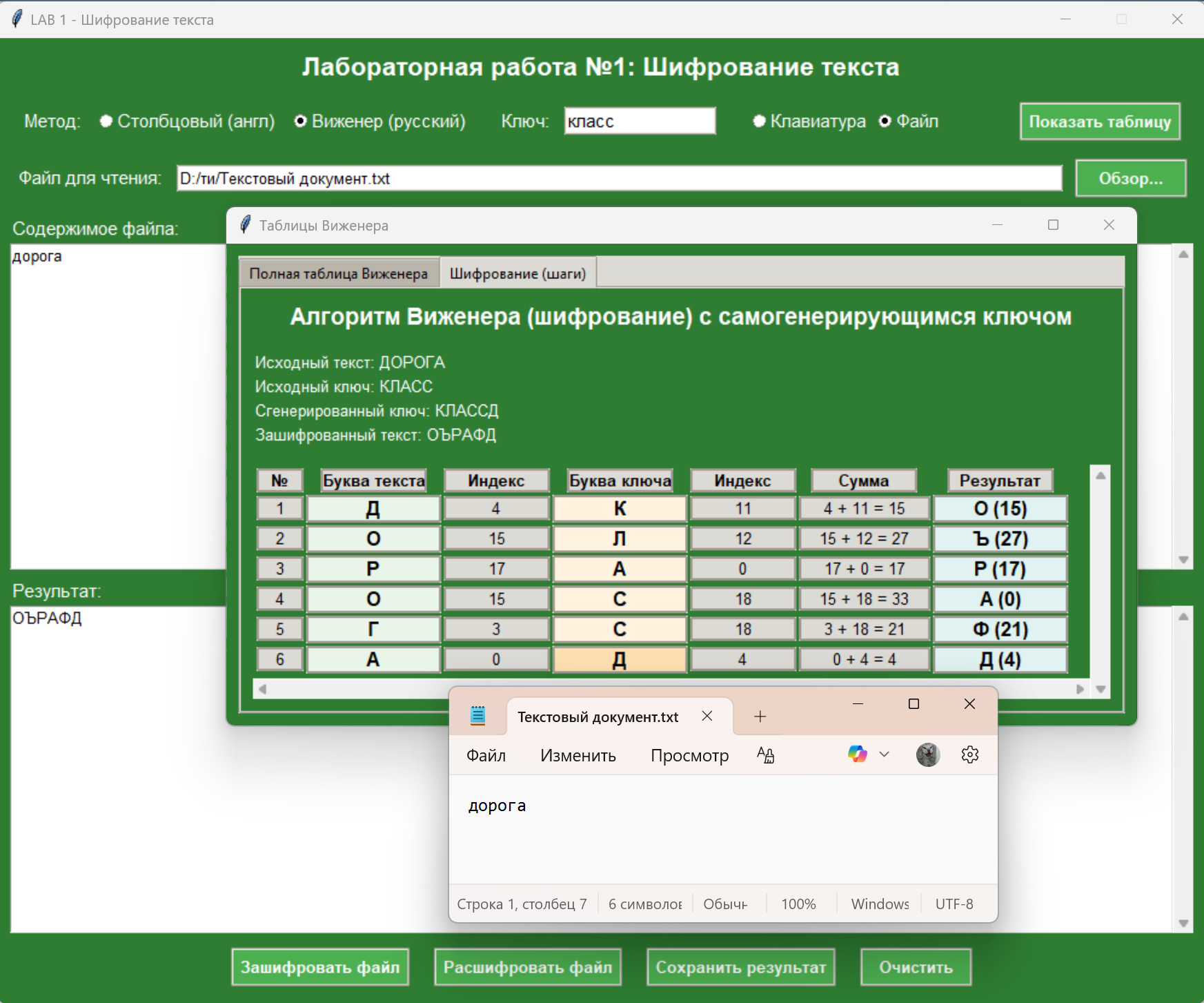


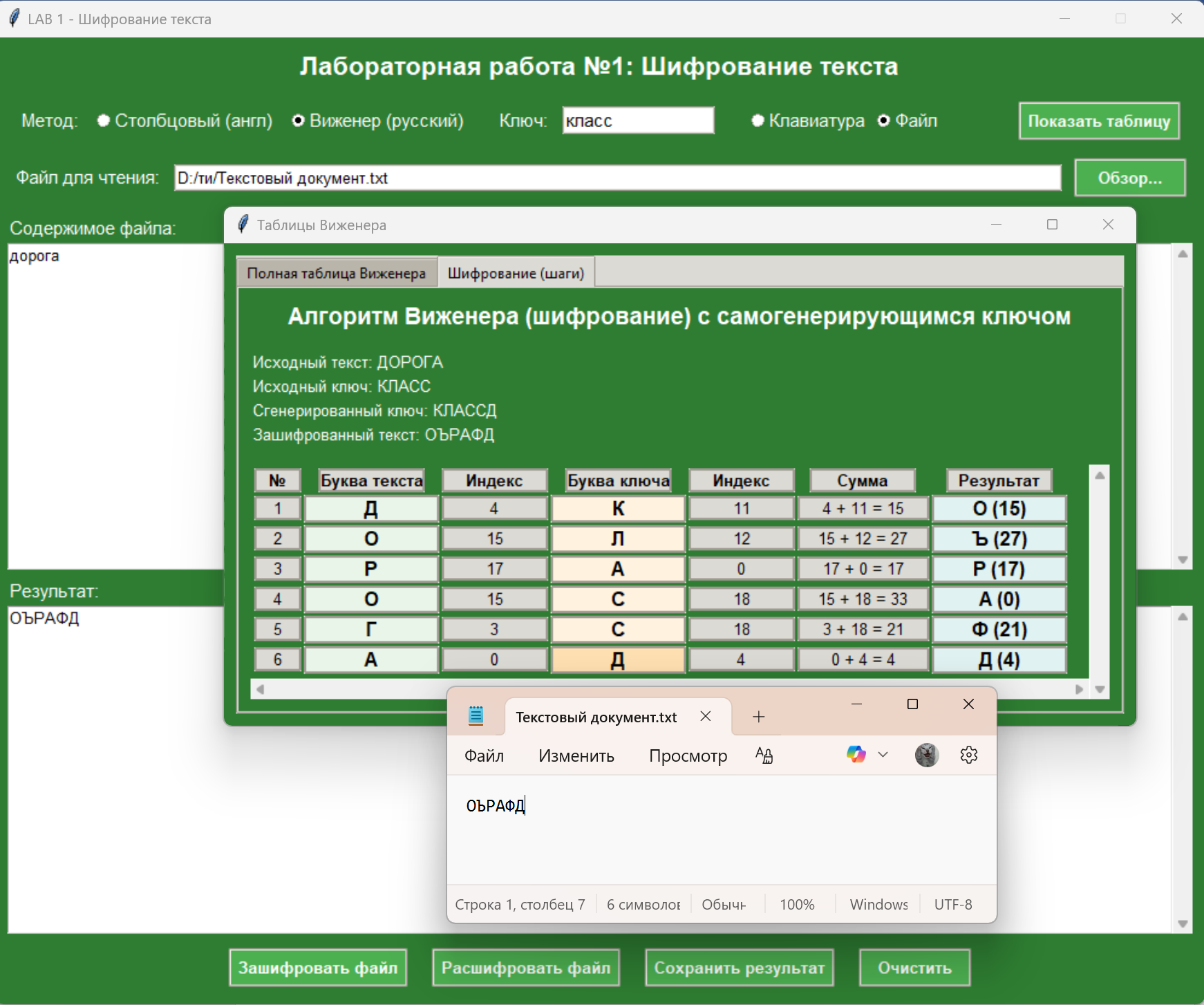
**ТЕСТ ПРОЙДЕН**

**Работа с файлами**

****

****

****

****

**Вывод**

В ходе выполнения работы были реализованы и проанализированы два различных подхода к шифрованию текста: столбцовый метод перестановки и алгоритм Виженера с самогенерирующимся ключом.

Первый метод относится к классу перестановочных шифров и отличается простотой реализации и высокой скоростью работы. Он не изменяет сами символы, а только перемешивает их, что делает его уязвимым для криптоаналитических атак, особенно при использовании коротких ключей. Стойкость шифра напрямую зависит от длины ключа и отсутствия повторяющихся букв, однако чрезмерное увеличение длины ключа приводит к появлению пустых ячеек в таблице шифрования, что снижает общую безопасность.

Второй метод, представляющий собой модификацию шифра Виженера, демонстрирует значительно более высокую криптостойкость благодаря использованию самогенерирующейся ключевой последовательности. Отсутствие периодичности в ключе позволяет эффективно шифровать текст любой длины даже при коротком начальном ключе. Существенным недостатком является высокая чувствительность к ошибкам — искажение одного символа при расшифровке делает нечитаемым весь последующий текст.

Таким образом, выбор метода шифрования должен определяться конкретными требованиями: столбцовый метод целесообразно применять в ситуациях, где приоритетны простота и скорость обработки, тогда как алгоритм Виженера с самогенерирующимся ключом является предпочтительным для задач, требующих повышенной надежности при работе с длинными текстами.