УО «Белорусский государственный университет информатики и радиоэлектроники»

Кафедра ПОИТ

Отчет по лабораторной работе №1 по предмету

Теория информации

Вариант 7

Выполнила:

Лутай В.В.

Проверила:

Болтак С.В.

Группа:

351003

Минск 2025

**Задания для варианта**

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

- **метод поворачивающейся решетки (**текст на английском языке**),** использовать размер решетки 4х4 и схему шифрования как в примере на рисунке 1.3 стр.6);

- 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.

**Метод поворачивающейся решетки**

Тестовая фраза: hell234o worЛДld!!!

В конечном итоге строка будет конвертирована в: Helloworldabcdef (дополнение до 16 символов)

Отверстия решетки:

|  |  |  |  |
| --- | --- | --- | --- |
| X | X | X |  |
|  |  | X |  |
|  |  |  |  |
|  |  |  |  |

Пошаговое шифрование:

Шаг 1: Шаг 2:

|  |  |  |  |
| --- | --- | --- | --- |
| h | e | l |  |
|  |  | l |  |
|  |  |  |  |
|  |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| h | e | l | o |
|  |  | l | w |
|  |  | o | r |
|  |  |  |  |

Шаг 3: Шаг 4:

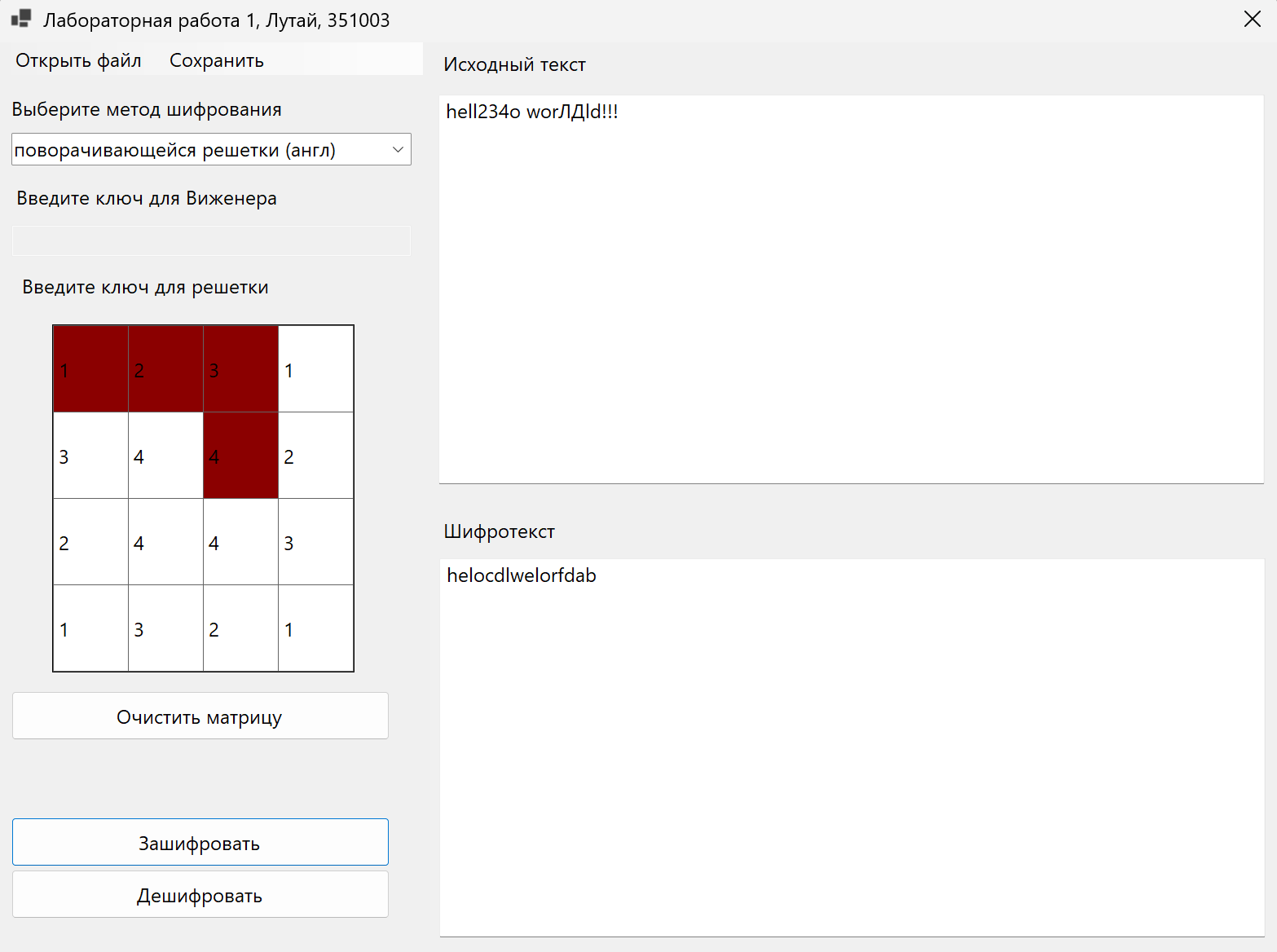
|  |  |  |  |
| --- | --- | --- | --- |
| h | e | l | o |
|  |  | l | w |
|  | l | o | r |
|  | d | a | b |

|  |  |  |  |
| --- | --- | --- | --- |
| h | e | l | o |
| c | d | l | w |
| e | l | o | r |
| f | d | a | b |

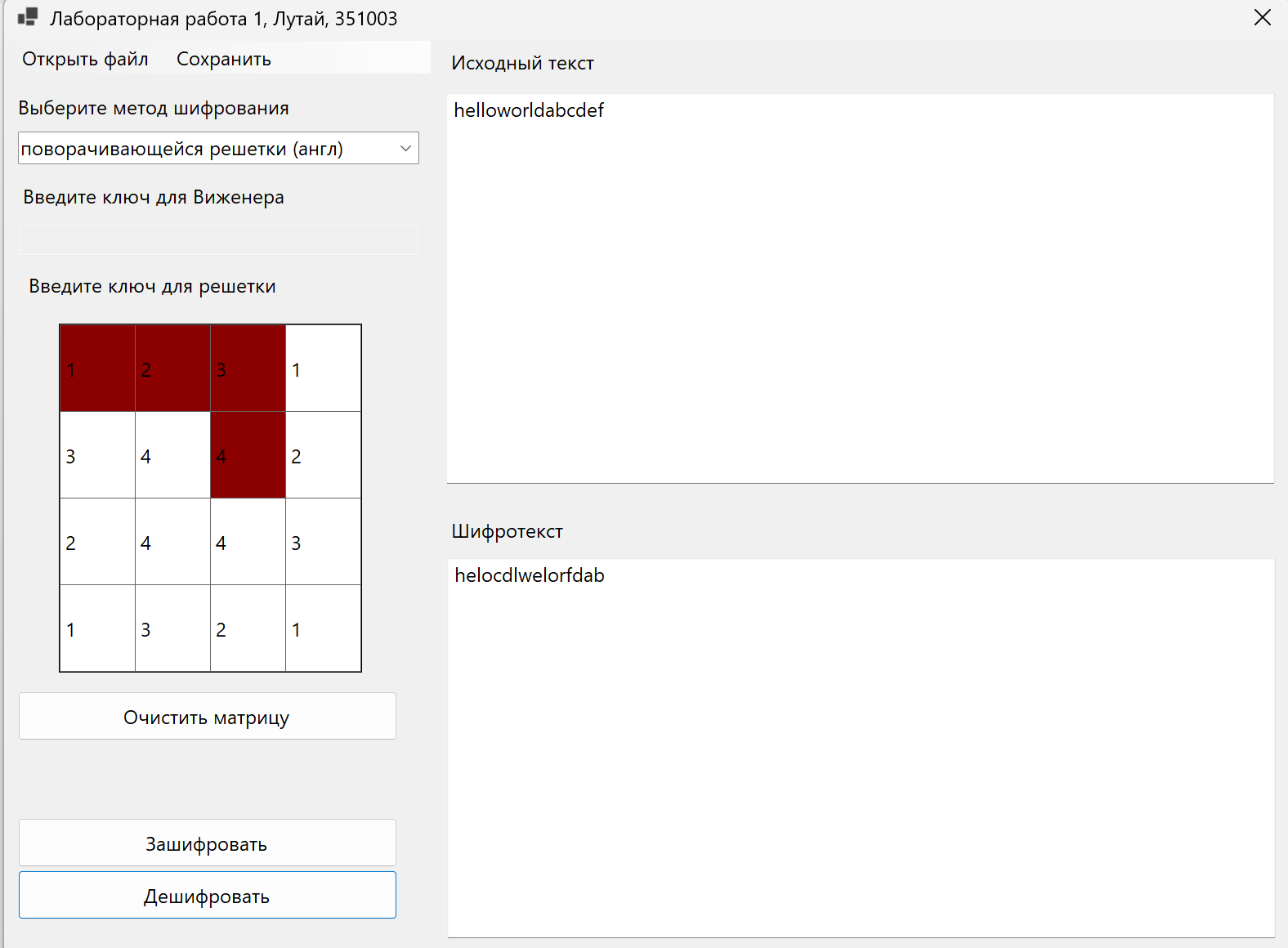
Шифротекст: hellocdlwelorfdab

Результат работы программы:

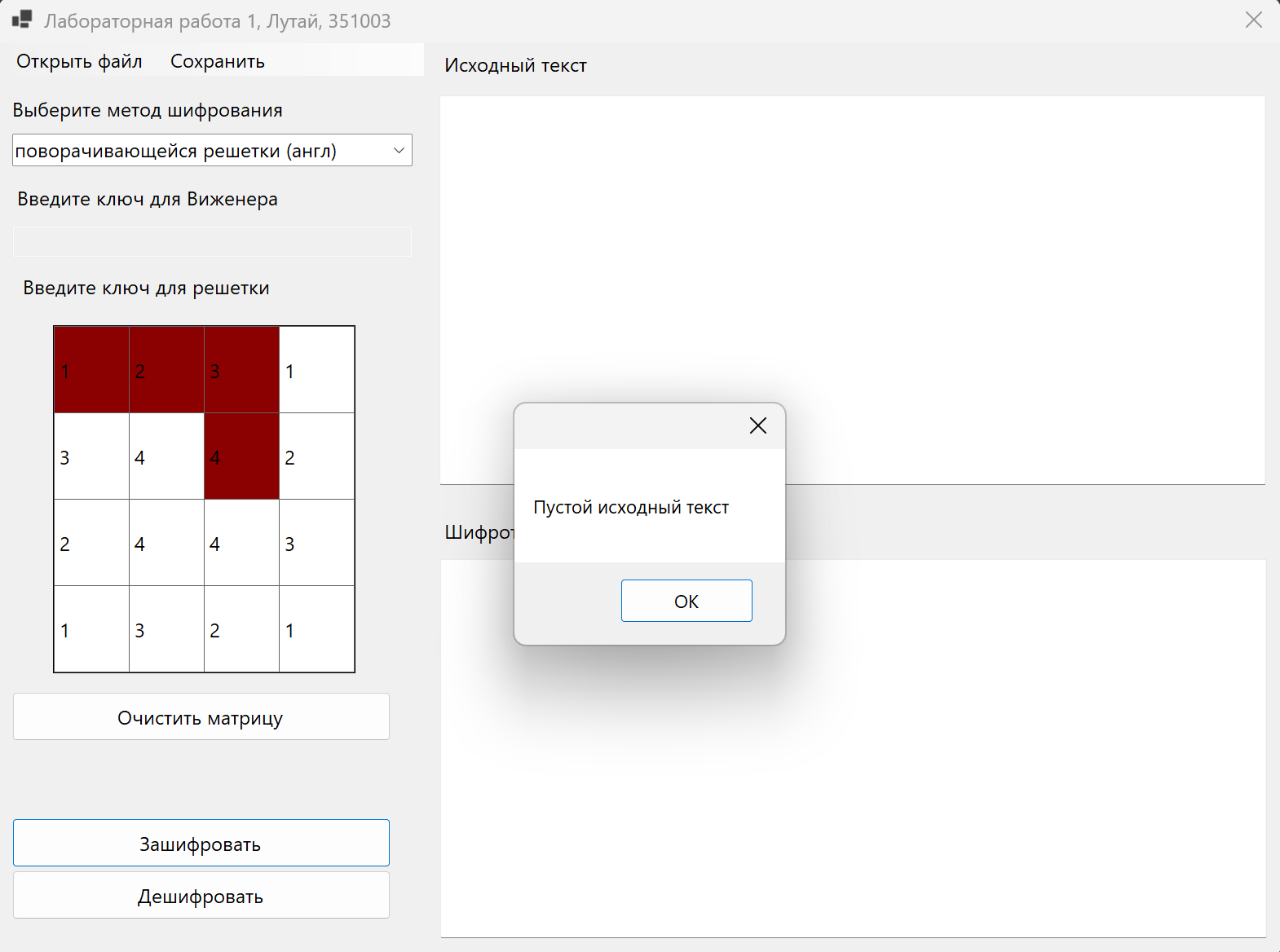
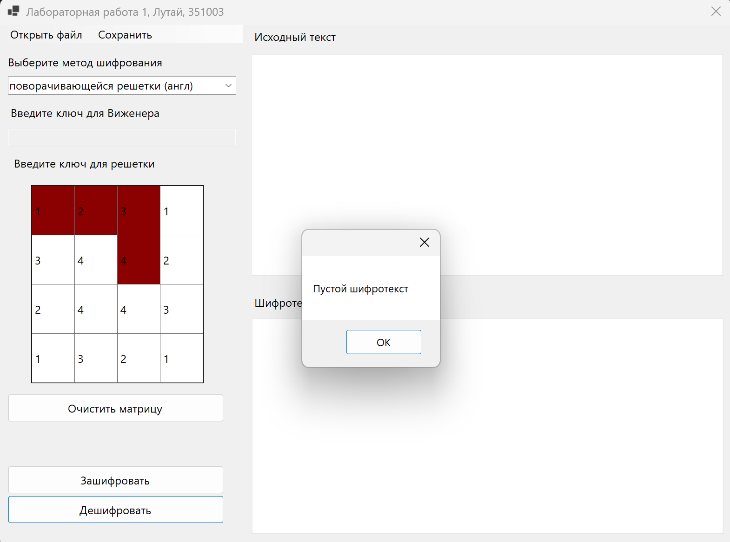
Шифрирование

****

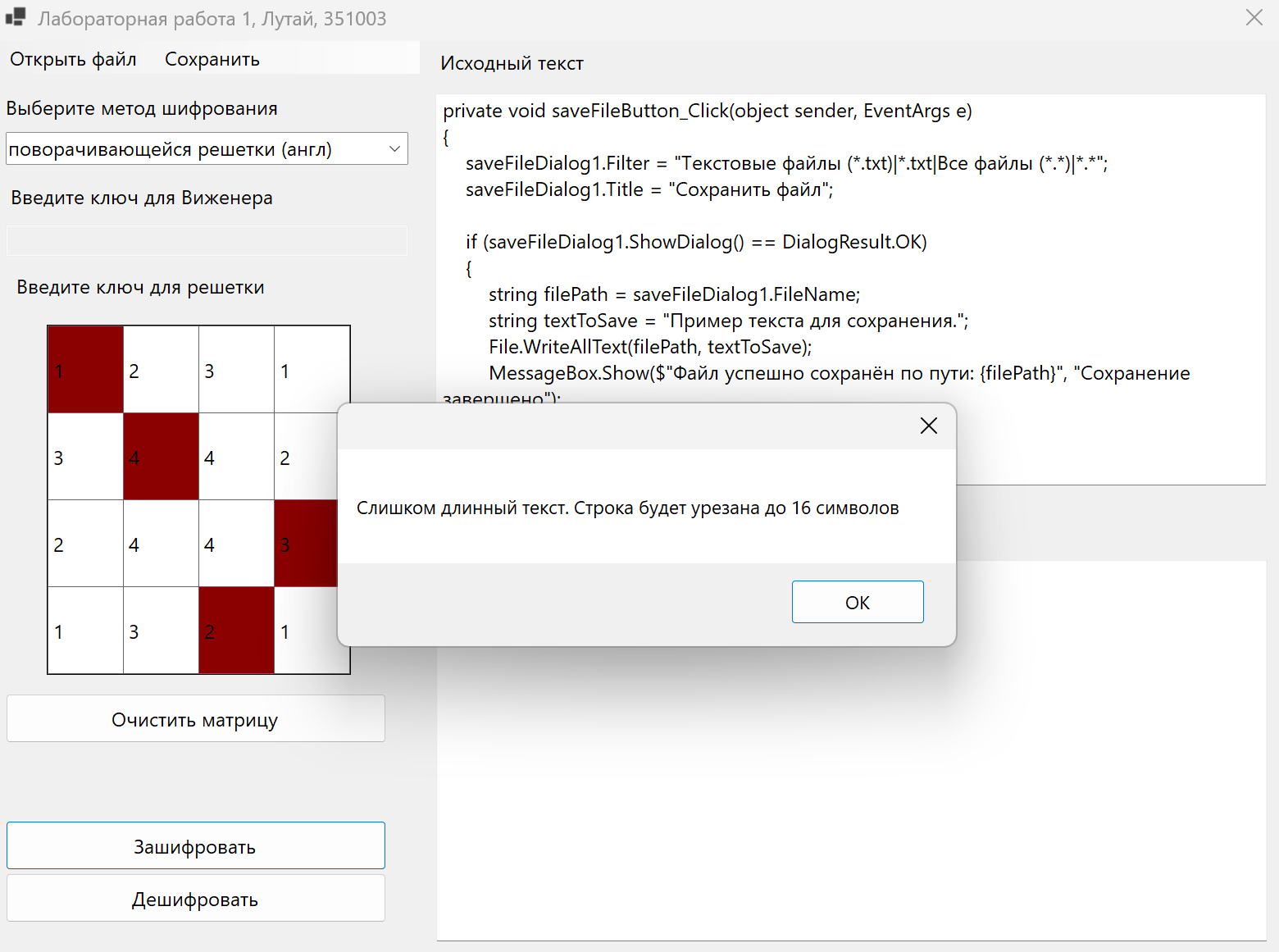
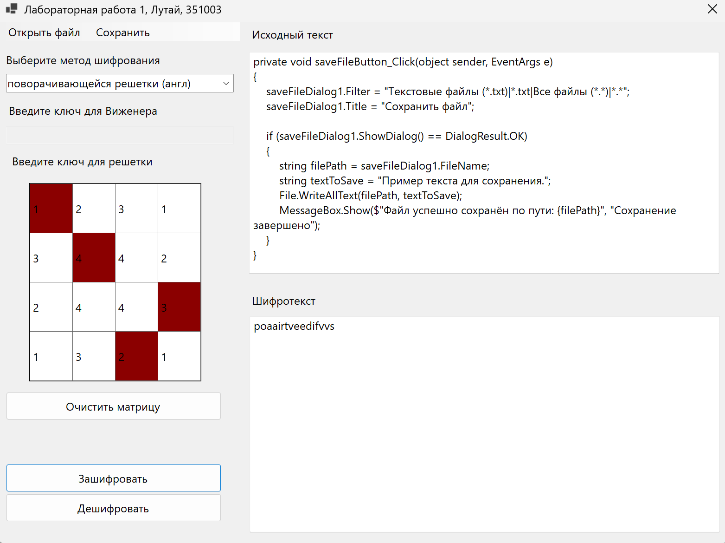
Дешифрирование



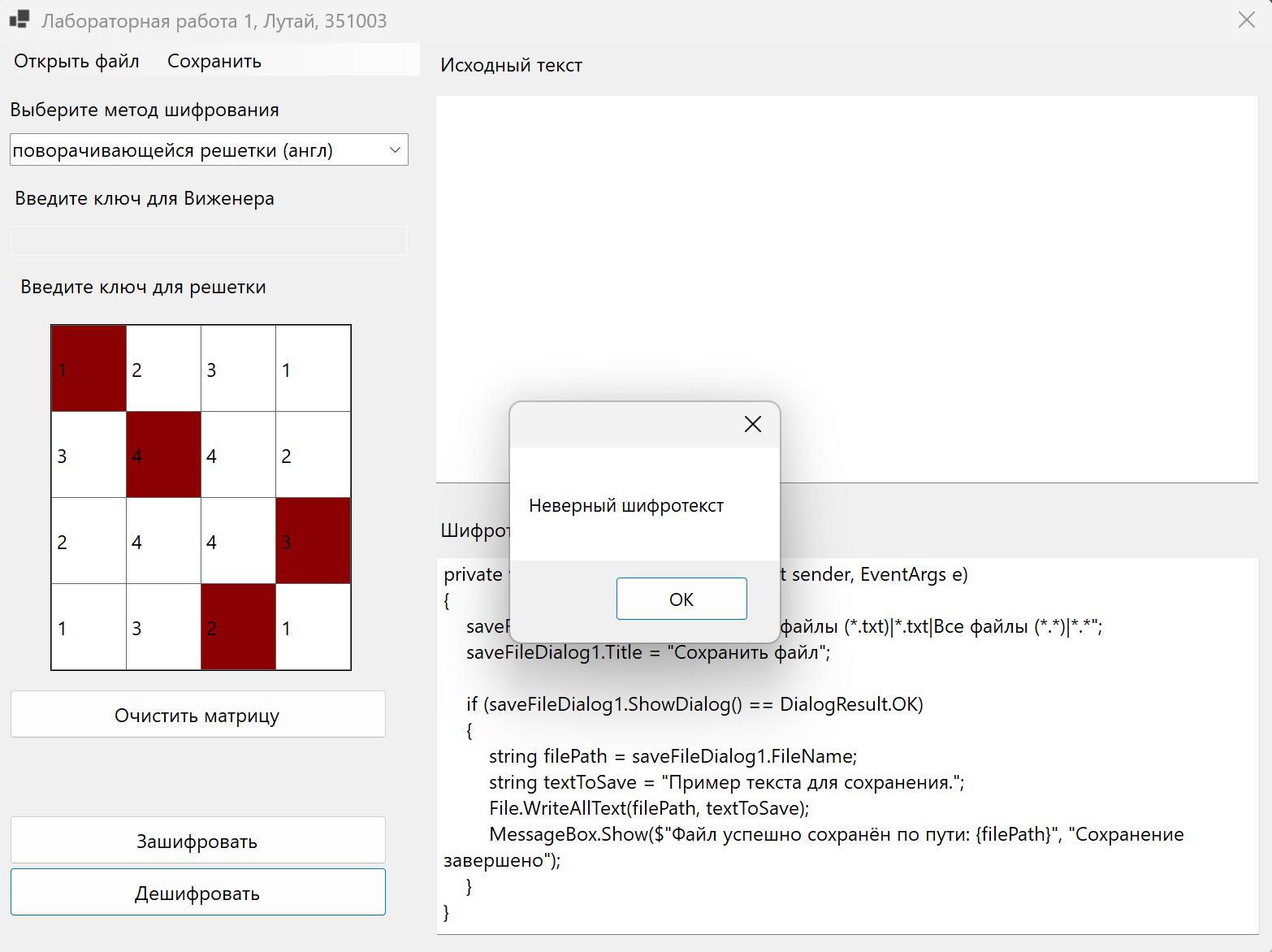
Шифрование/дешифрирование пустого файла:



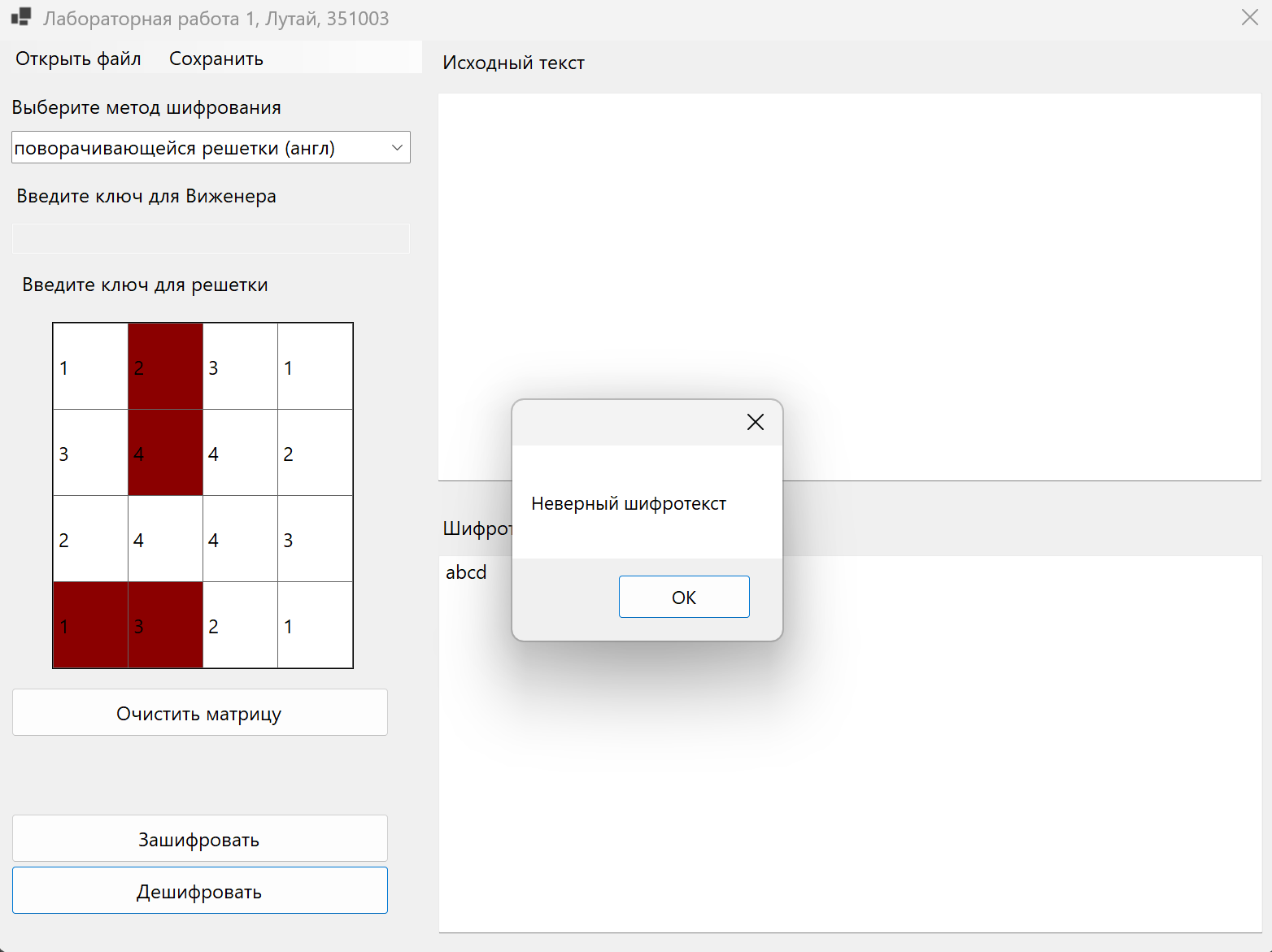
Шифрование/дешифрирование файлов с числом символов более 16: Шифрование



Дешифрирование



Дешифрирование при шифротексте, меньшем 16 символов:



**Шифр Виженера (прогрессивный ключ)**

Тестовая фраза: всеRgRvsy%2м 2прив 333\*/етик;)

В конечном итоге строка будет конвертирована в: всем прив етик

Ключевое слово: кл<3юCHICчик

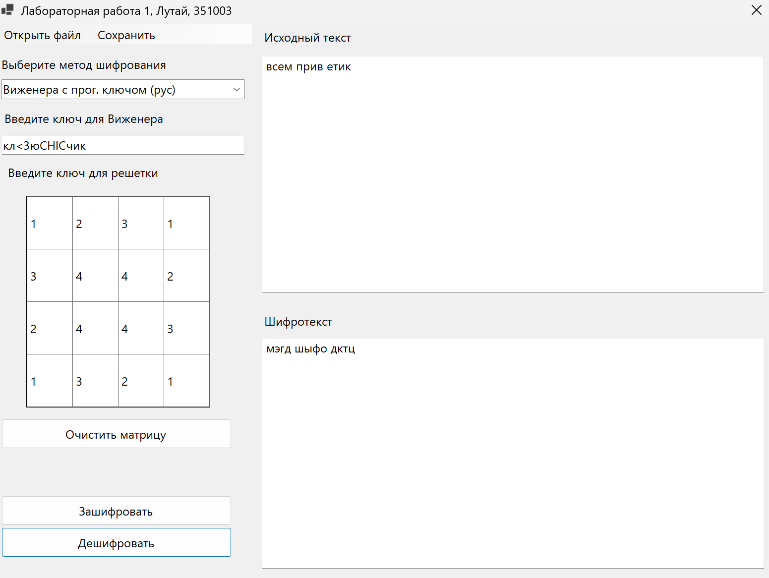
В конечном итоге строка будет конвертирована в: ключик

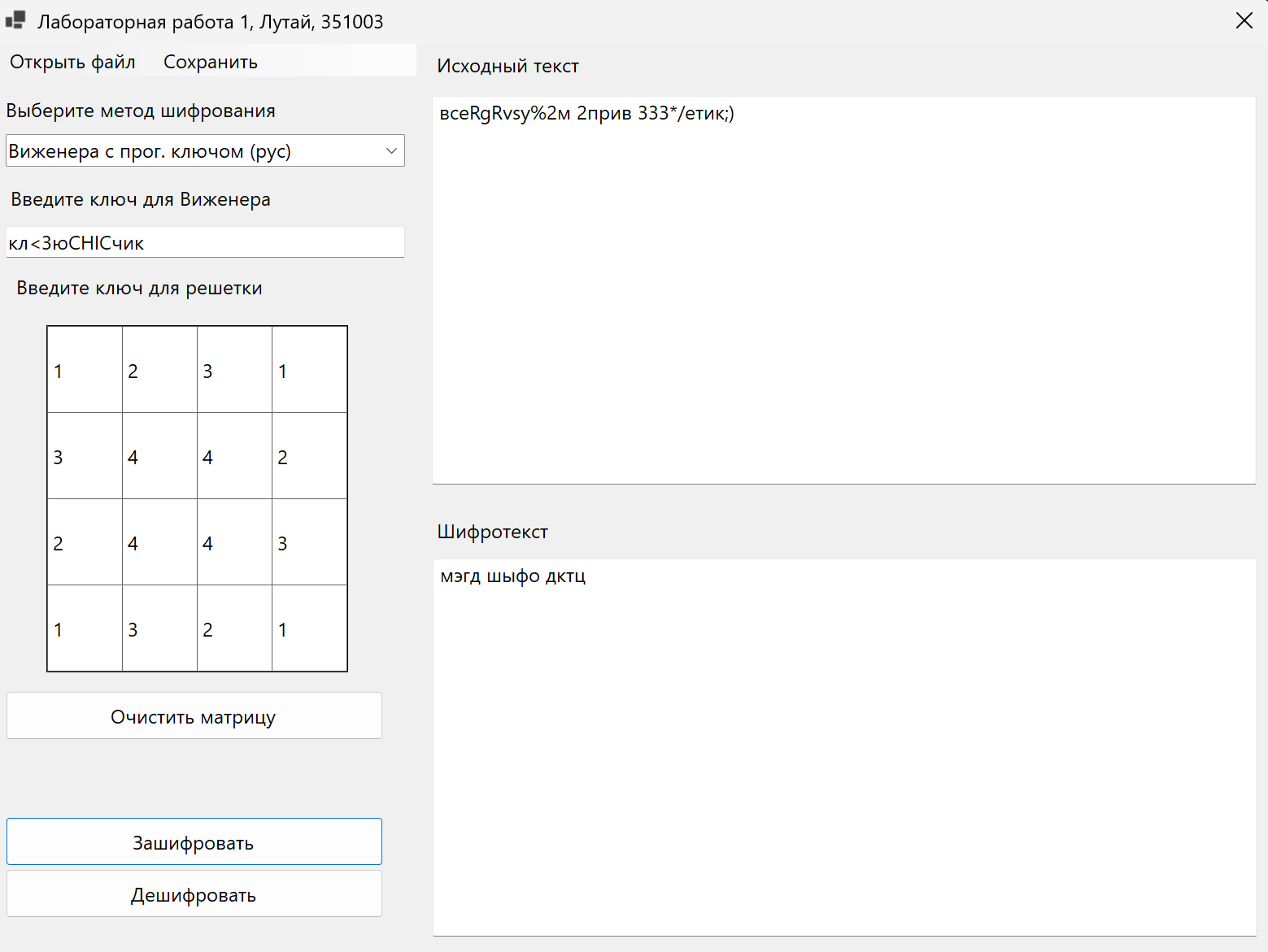
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| в | с | е | м |  | п | р | и | в |  | е | т | и | к |
| к | л | ю | ч |  | и | к | л | м |  | я | ш | й | л |
| м | э | г | д |  | ш | ы | ф | о |  | д | к | т | ц |

Таблица подстановки

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 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 |

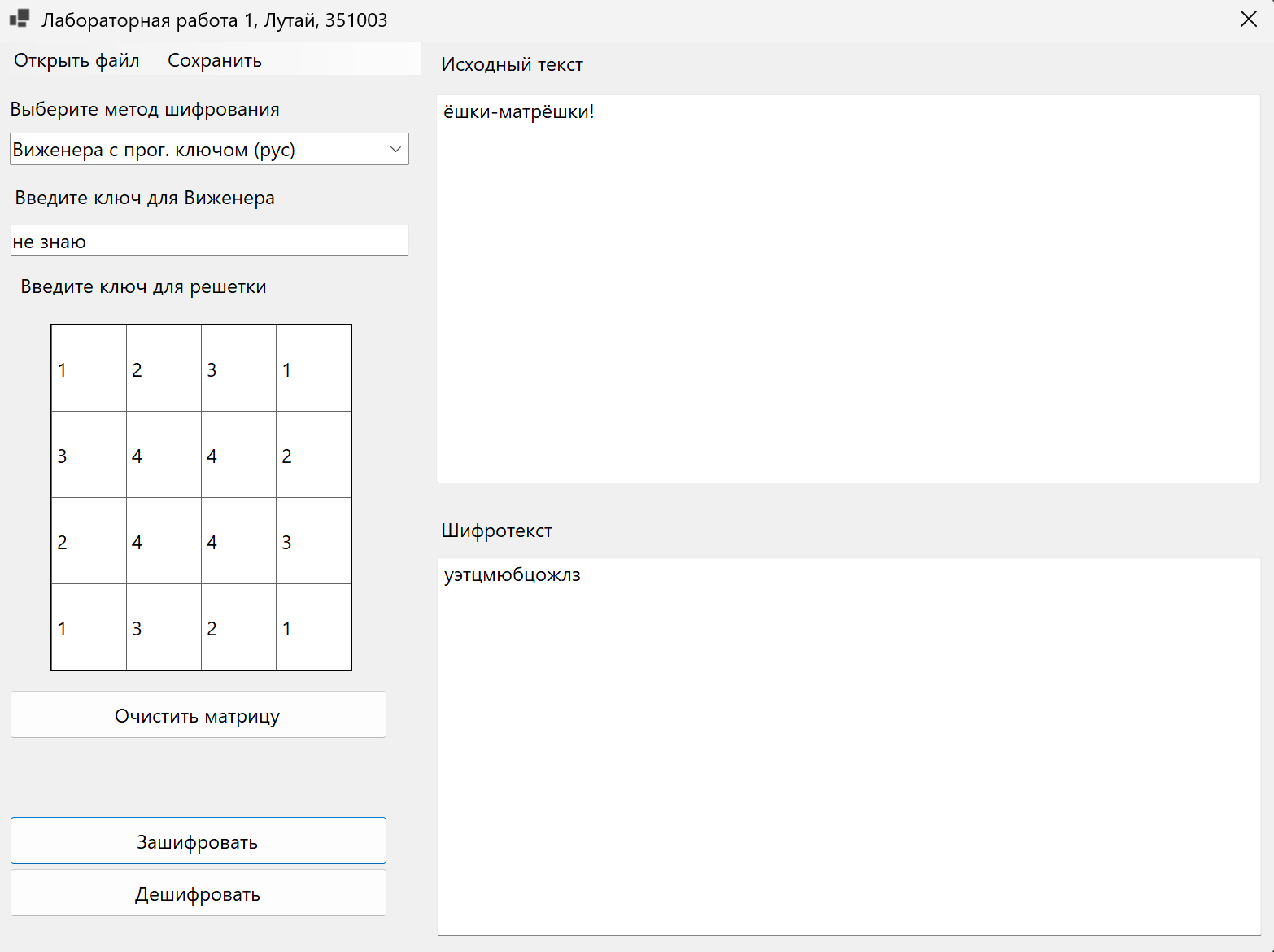
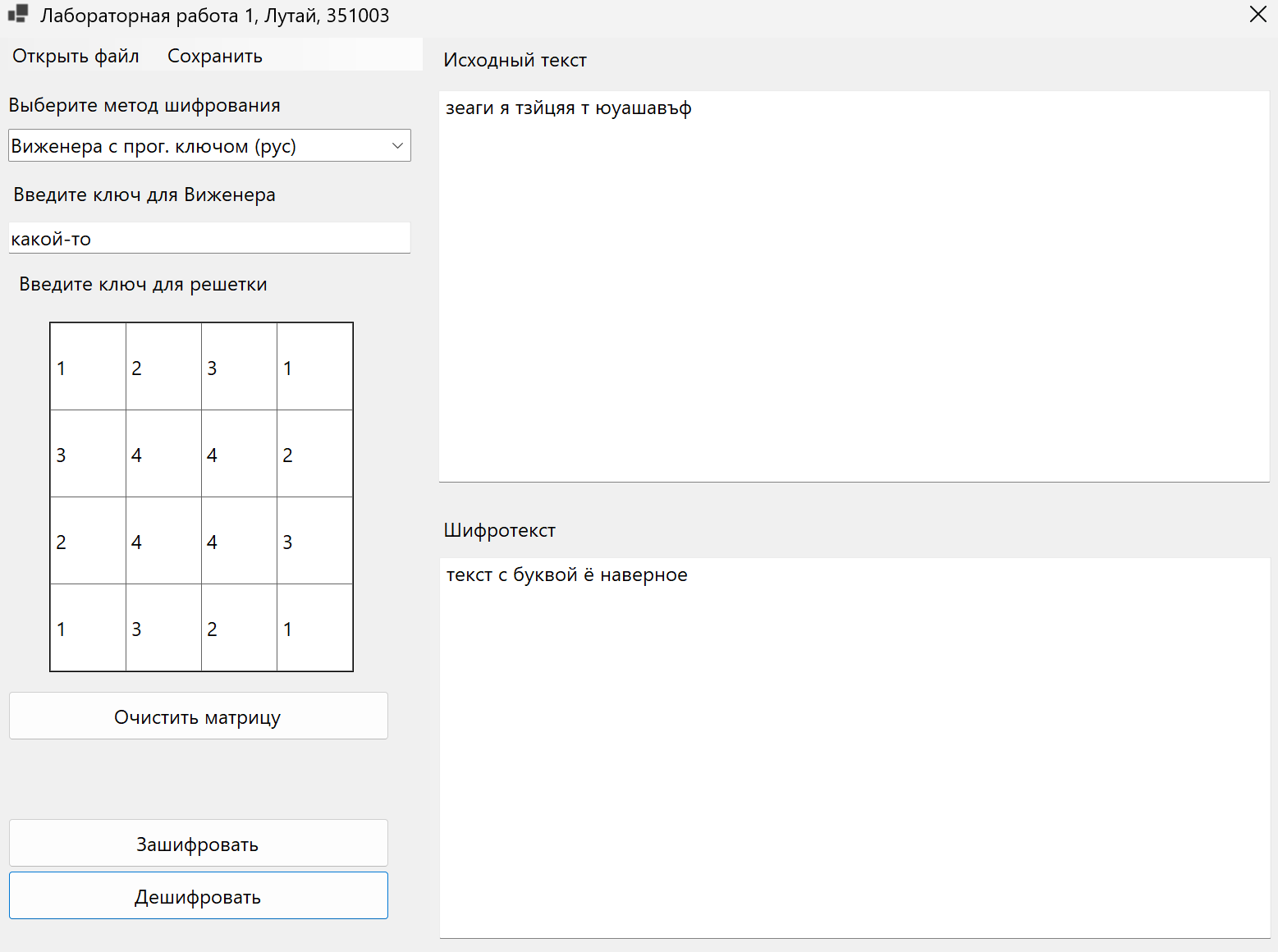
Формула: Ci = (Mi + Ki) mod S, где S – размер алфавита.

Шифрование Дешифрирование



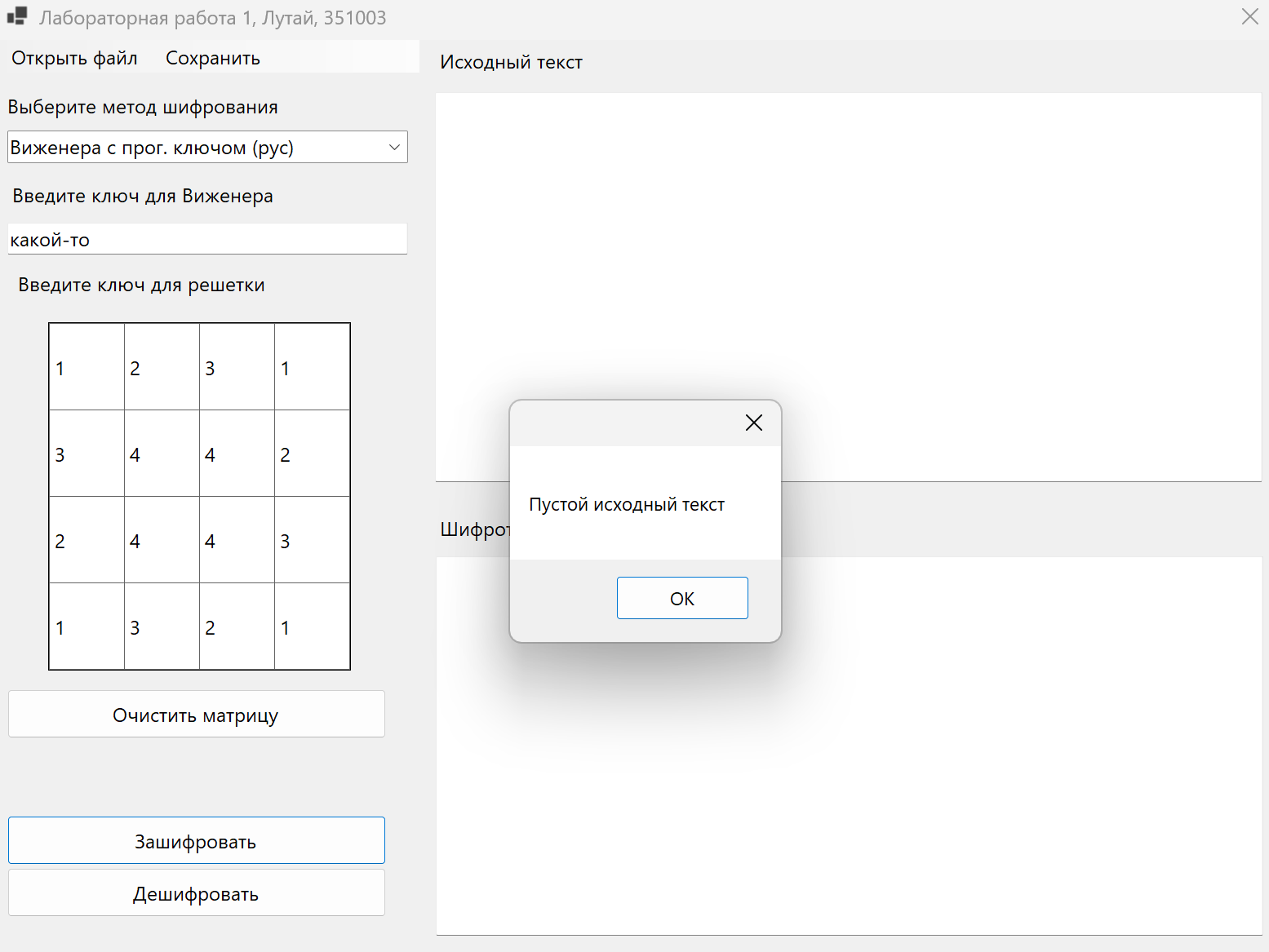
Шифрование и дешифрирование фразы, содержащей букву ё:

Шифрование Дешифрирование

Шифрование и дешифрирование пустых строк:

Шифрование Дешифрирование



Шифрование (и дешифрирование) с пустым ключом:

