

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»

ОТЧЕТ  
по лабораторной работе № 1

на тему:

ПРОСТЕЙШИЕ ШИФРЫ

Выполнил  
Студент гр. 451001

Држевецкий Никита  
Александрович

Руководитель, преподаватель

Болтак С. В.

Минск, 2026

## Условие задачи

### 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.

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.

### Тесты

#### Метод децимаций

Дымовое тестирование

1. Тестовая фраза: **Hello! 123**
2. Ключ: **5**
3. Таблица, которая содержит весь алфавит заданного языка и номер каждой буквы:

Буква	Номер
A	0
B	1
C	2
D	3
E	4
F	5
G	6
H	7
I	8
J	9
K	10
L	11
M	12
N	13
O	14
P	15
Q	16
R	17
S	18
T	19

U	20
V	21
W	22
X	23
Y	24
Z	25

#### 4. Вычисления:

Формула:

$$E(x) = (x * 5) \bmod 26$$

$$H = 7$$

$$(7 * 5) \bmod 26 = 35 \bmod 26 = 9 \rightarrow J$$

$$E = 4$$

$$(4 * 5) = 20 \rightarrow U$$

$$L = 11$$

$$(11 * 5) = 55 \bmod 26 = 3 \rightarrow D$$

$$L \rightarrow D$$

$$O = 14$$

$$(14 * 5) = 70 \bmod 26 = 18 \rightarrow S$$

Получается: **Judds! 123**

#### 5. Проверка дешифрования:

Формула:

$$D(x) = (x * k^{-1}) \bmod 26$$

Обратный элемент к 5:

$$5 \times 21 \bmod 26 = 1$$

$$k^{-1} = 21$$

Проверка:

$$J = 9$$

$$9 \times 21 \bmod 26 = 7 \rightarrow H$$

$$U = 20$$

$$20 \times 21 \bmod 26 = 4 \rightarrow E$$

$$D = 3$$

$$3 \times 21 \bmod 26 = 11 \rightarrow L$$

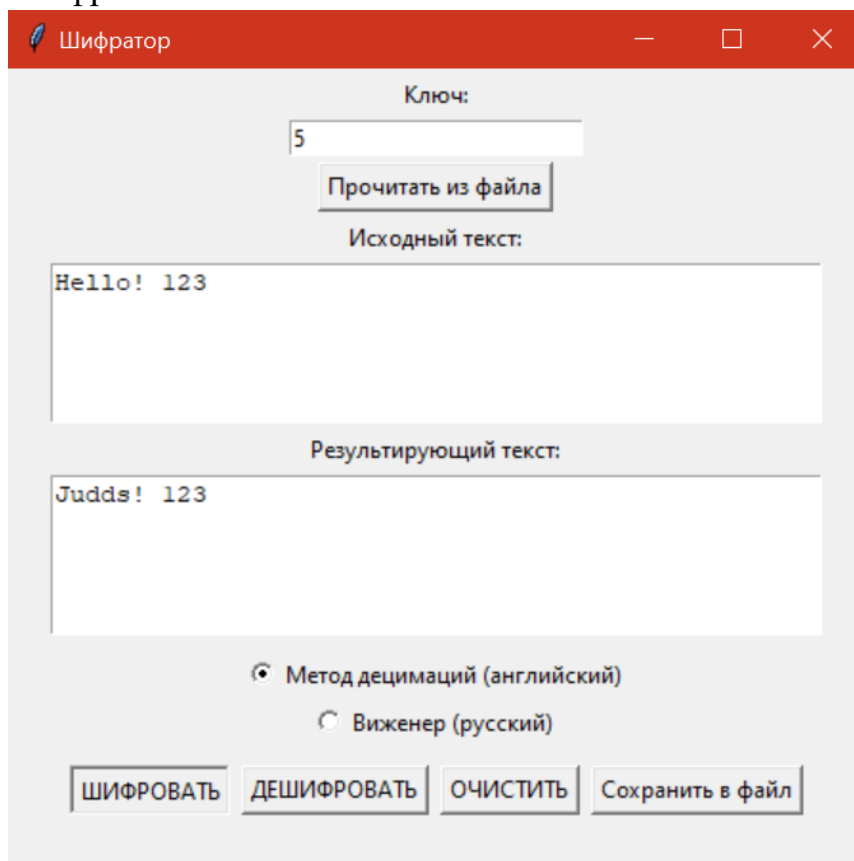
$$D \rightarrow L$$

$$S = 18$$

$$18 \times 21 \bmod 26 = 14 \rightarrow O$$

Скрины:

Шифрование:



Шифратор

Ключ:

5

Прочитать из файла

Исходный текст:

Hello! 123

Результирующий текст:

Judds! 123

☒ Метод децимаций (английский)

☐ Виженер (русский)

ШИФРОВАТЬ   ДЕШИФРОВАТЬ   ОЧИСТИТЬ   Сохранить в файл

## Дешифрование:

Шифратор

Ключ:

5

Прочитать из файла

Исходный текст:

Judds! 123

Результирующий текст:

Hello! 123

☒ Метод децимаций (английский)

☐ Вижнер (русский)

ШИФРОВАТЬ ДЕШИФРОВАТЬ ОЧИСТИТЬ Сохранить в файл

Ломаем на валидных данных.

Ключ меньше длины алфавита:

Ключ = 3

Шифрование:

Формула:

$$E(x) = (x * 3) \bmod 26$$

$$H = 7$$

$$(7 * 3) = 21 \rightarrow V$$

$$E = 4$$

$$(4 * 3) = 12 \rightarrow M$$

$$L = 11$$

$$(11 * 3) = 33 \bmod 26 = 7 \rightarrow H$$

$$L \rightarrow H$$

$$O = 14$$

$$(14 * 3) = 70 \bmod 26 = 16 \rightarrow Q$$

Получается: **Vmhhq! 123**

Проверка дешифрования:

Формула:

$$D(x) = (x * k^{-1}) \bmod 26$$

Обратный элемент к 3:

$$3 \times 9 \bmod 26 = 1$$

$$k^{-1} = 9$$

Проверка:

$$V = 21$$

$$21 \times 3 \bmod 26 = 7 \rightarrow H$$

$$M = 12$$

$$12 \times 3 \bmod 26 = 4 \rightarrow E$$

$$H = 7$$

$$7 \times 3 \bmod 26 = 11 \rightarrow L$$

$$H \rightarrow L$$

$$Q = 16$$

$$16 \times 3 \bmod 26 = 14 \rightarrow O$$

Скрины:

Шифрование:

The screenshot shows a window titled 'Шифратор' with a red header bar. It contains the following elements:

- Ключ:** A text input field containing the value '3'.
- Прочитать из файла:** A button located below the key input field.
- Исходный текст:** A text area containing the text 'Hello! 123'.
- Результирующий текст:** A text area containing the encrypted text 'Vmhhq! 123'.
- Method Selection:** Two radio buttons. The first, 'Метод децимаций (английский)', is selected. The second is 'Вижнер (русский)'.
- Buttons:** A row of four buttons at the bottom: 'ШИФРОВАТЬ', 'ДЕШИФРОВАТЬ', 'ОЧИСТИТЬ', and 'Сохранить в файл'.

Дешифрование:

This screenshot shows the same 'Шифратор' application window, but in the decryption state. The elements are:

- Ключ:** The text input field still contains '3'.
- Прочитать из файла:** The button remains below the key input field.
- Исходный текст:** The text area now contains the encrypted text 'Vmhhq! 123'.
- Результирующий текст:** The text area contains the decrypted text 'Hello! 123'.
- Method Selection:** The radio button for 'Метод децимаций (английский)' remains selected.
- Buttons:** The same row of four buttons is present at the bottom.

Ключ больше длины алфавита:

Ключ = 29

Шифрование:

Формула:

$E(x) = (x * 29) \bmod 26$

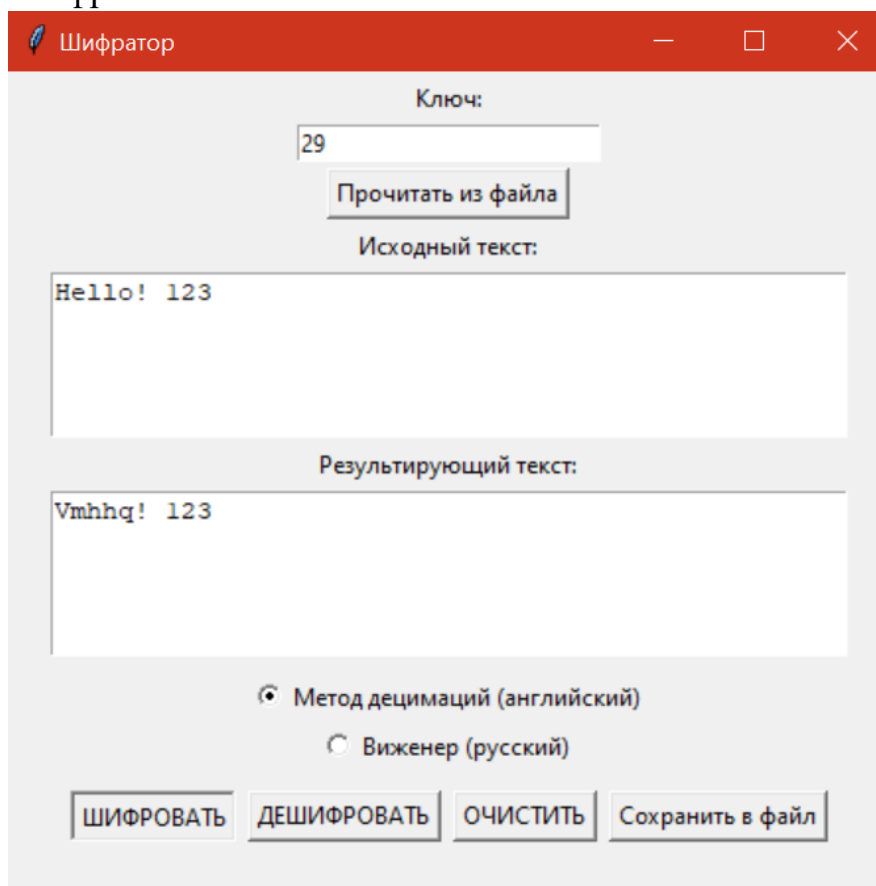
Вычисления будут такие же как в прошлом примере, потому что вычисления идут по модулю 26

$29 \bmod 26 = 3$

Ключ = 29 = 3

Скрины:

Шифрование:



Шифратор

Ключ:

29

Прочитать из файла

Исходный текст:

Hello! 123

Результирующий текст:

Vmhhq! 123

☒ Метод децимаций (английский)

☐ Вижнер (русский)

ШИФРОВАТЬ   ДЕШИФРОВАТЬ   ОЧИСТИТЬ   Сохранить в файл



## Дешифрование:

The screenshot shows the 'Шифратор' (Cryptor) application window. At the top, the title bar says 'Шифратор'. Below it, there is a 'Ключ:' (Key) section with a text input field containing '29' and a button 'Прочитать из файла' (Read from file). Below this is the 'Исходный текст:' (Original text) section with a text area containing 'Vmhhq! 123'. Below that is the 'Результирующий текст:' (Resulting text) section with a text area containing 'Hello! 123'. At the bottom, there are two radio buttons: 'Метод децимаций (английский)' (selected) and 'Вижнер (русский)'. At the very bottom, there are four buttons: 'ШИФРОВАТЬ' (Encrypt), 'ДЕШИФРОВАТЬ' (Decrypt), 'ОЧИСТИТЬ' (Clear), and 'Сохранить в файл' (Save to file).

Ломаем на не валидных данных:

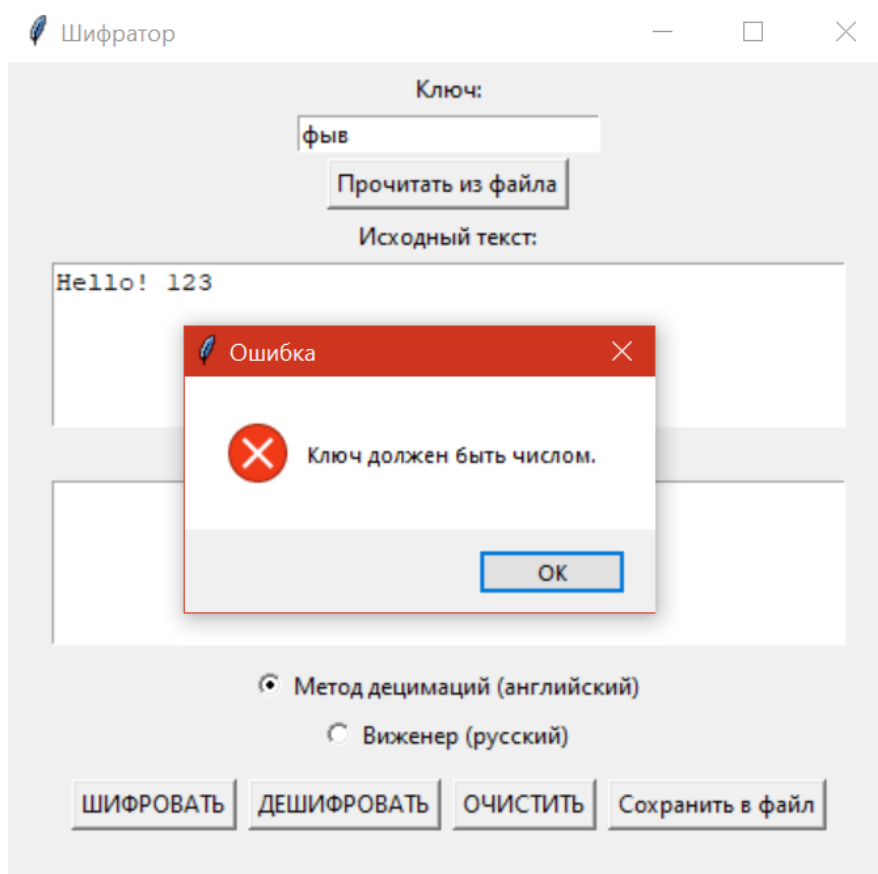
Ключ = 13

Ключ должен быть взаимно прост с 26»

The screenshot shows the 'Шифратор' (Cryptor) application window with the 'Ключ:' (Key) input field set to '13'. The 'Исходный текст:' (Original text) section contains 'Hello! 123'. An error dialog box is overlaid on the window. The dialog box has a red title bar with the text 'Ошибка' (Error) and a close button. It contains a red 'X' icon and the text 'Ключ должен быть взаимно прост с 26.' (Key must be coprime with 26). There is an 'ОК' (OK) button at the bottom right of the dialog box. The rest of the application window, including the radio buttons and bottom buttons, is visible behind the dialog box.

Ключ = «фыв»

Ключ должен быть числом



## Шифр Виженера (прямой)

Дымовое тестирование

1. Тестовая фраза: **Привет! 123**
2. Ключ: **КОД**
- 3.

П	Р	И	В	Е	Т
К	О	Д	К	О	Д

#### 4. 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	ш
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

Вычисления:

П, К

Их пересечение по таблице → Ъ

Р, О

Их пересечение по таблице → Я

И, Д

Их пересечение по таблице → М

В, К

Их пересечение по таблице → М

Е, О

Их пересечение по таблице → У

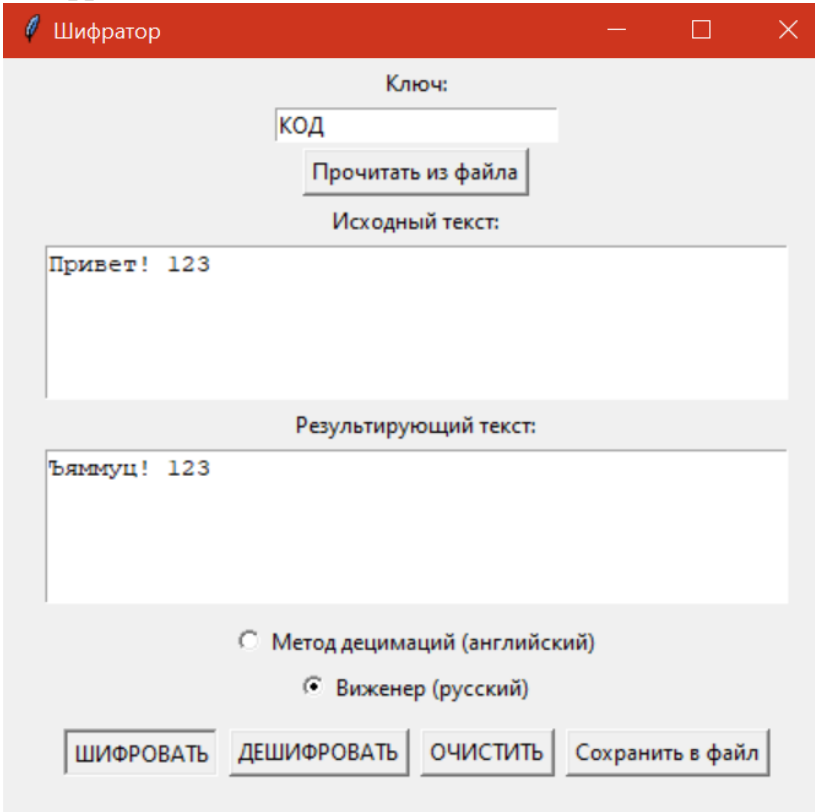
Т, Д

Их пересечение по таблице → Ц

Получается: **Ъяммуц! 123**

Скрины:

Шифрование:



## Дешифрование:

The screenshot shows a window titled "Шифратор" (Cryptor) with a red title bar. Inside, there is a section labeled "Ключ:" (Key) with a text input field containing "КОД" and a button "Прочитать из файла" (Read from file). Below this is a section labeled "Исходный текст:" (Original text) with a text area containing "Ъяммуц! 123". Underneath is a section labeled "Результирующий текст:" (Resulting text) with a text area containing "Привет! 123". At the bottom, there are two radio buttons: "Метод децимаций (английский)" (Decimation method (English)) and "Вижнер (русский)" (Vigenere (Russian)), with the latter being selected. Below the radio buttons are four buttons: "ШИФРОВАТЬ" (Encrypt), "ДЕШИФРОВАТЬ" (Decrypt), "ОЧИСТИТЬ" (Clear), and "Сохранить в файл" (Save to file).

Ломаем на валидных данных:

Тестовая фраза, содержащая букву Ё: **Ёлка!**

Код: Снег

Вычисления:

Ё, С

Их пересечение по таблице → Ч

Л, Н

Их пересечение по таблице → Щ

К, Е

Их пересечение по таблице → П

А, Г

Их пересечение по таблице → Г

Получается: **Чщпг!**

Скрины:

## Шифрование:

The screenshot shows the 'Шифратор' (Cryptor) application window. The title bar is red with the text 'Шифратор' and standard window controls. The main area has a light gray background. At the top, there is a label 'Ключ:' (Key:) above a text input field containing 'Снег'. Below the input field is a button 'Прочитать из файла'. Underneath is a label 'Исходный текст:' (Original text:) above a large text area containing 'Ёлка !'. Below this is a label 'Результирующий текст:' (Resulting text:) above another large text area containing 'Чщпг !'. At the bottom, there are two radio buttons: 'Метод децимаций (английский)' (Vigenere cipher (English)) and 'Вижнер (русский)' (Vigenere cipher (Russian)), with the latter being selected. At the very bottom are four buttons: 'ШИФРОВАТЬ' (Encrypt), 'ДЕШИФРОВАТЬ' (Decrypt), 'ОЧИСТИТЬ' (Clear), and 'Сохранить в файл' (Save to file).

## Дешифрование:

This screenshot shows the same 'Шифратор' application window as above, but with the decryption settings. The 'Ключ:' field still contains 'Снег'. The 'Исходный текст:' field now contains 'Чщпг !'. The 'Результирующий текст:' field now contains 'Ёлка !'. The radio button for 'Вижнер (русский)' remains selected. The buttons at the bottom are the same as in the previous screenshot.

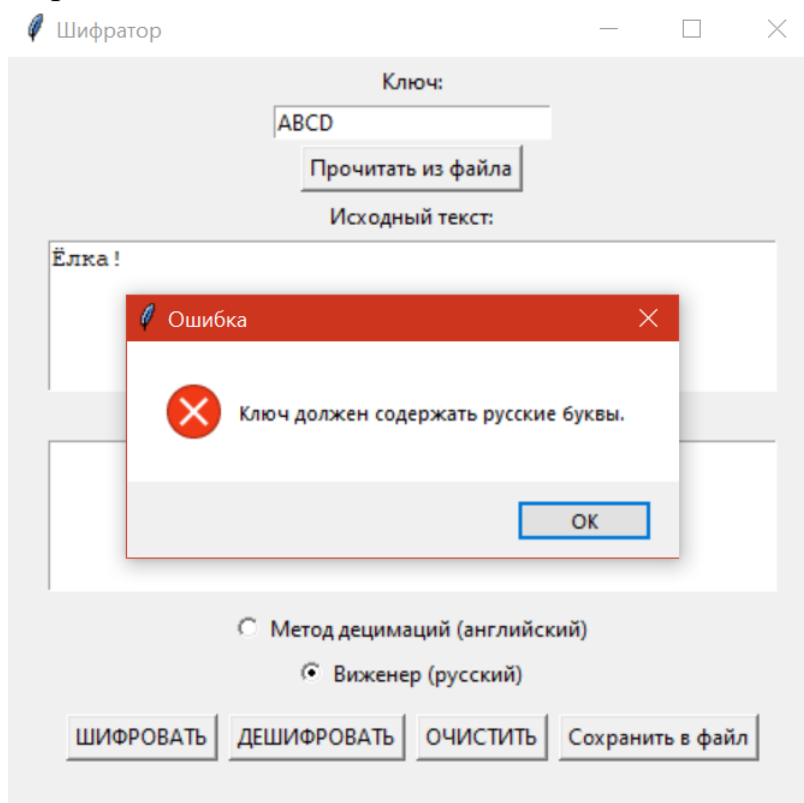
Ломаем на не валидных данных

Ключи, содержащие недопустимые значения:

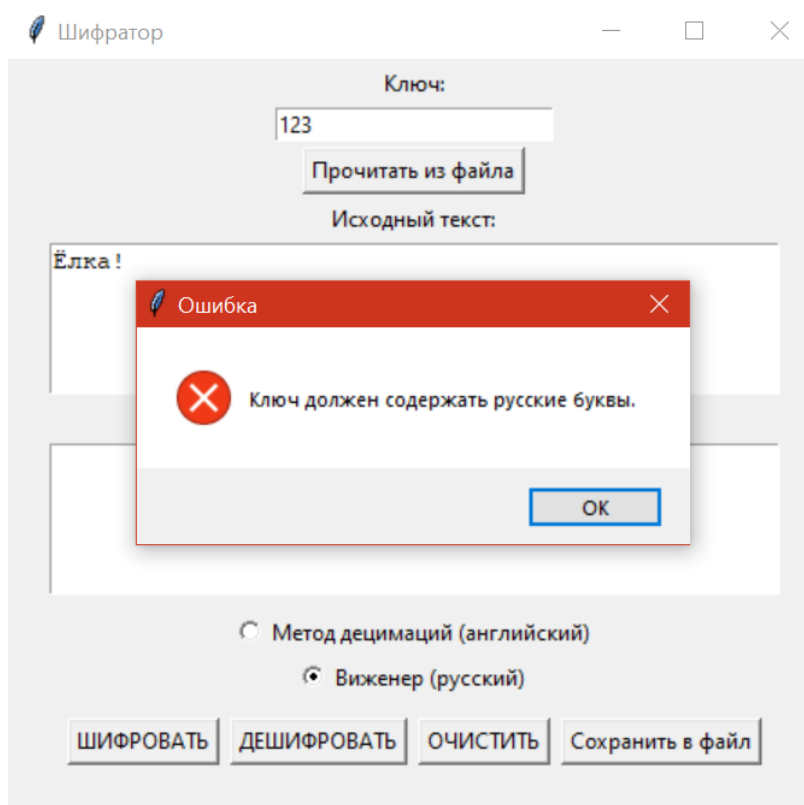
Ключ: ABCD

Ключ должен содержать русские буквы

Скрин:

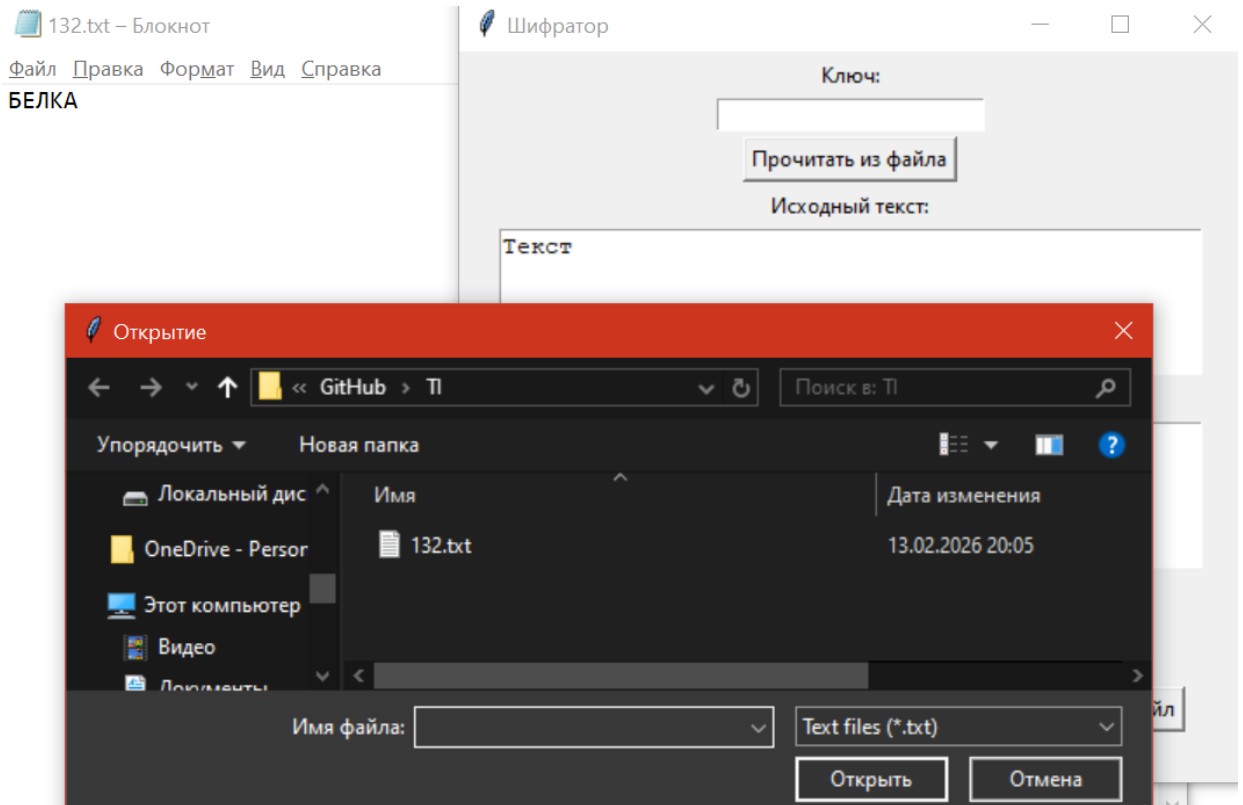


Ключ: 123

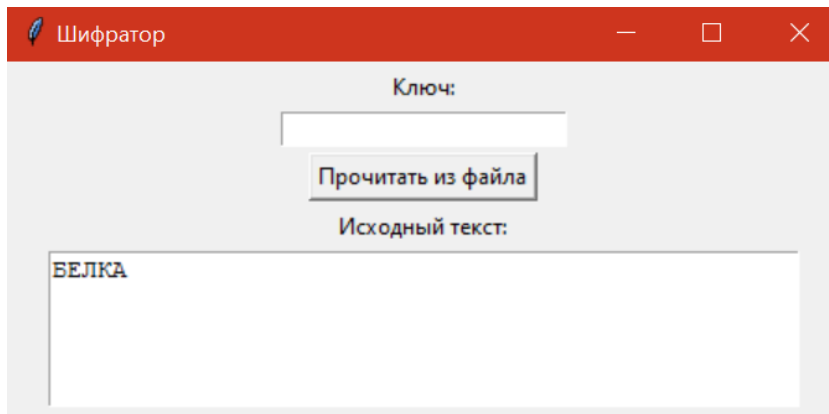


## Работа с файлами

Скрин выбора файла для ввода тестовой фразы:

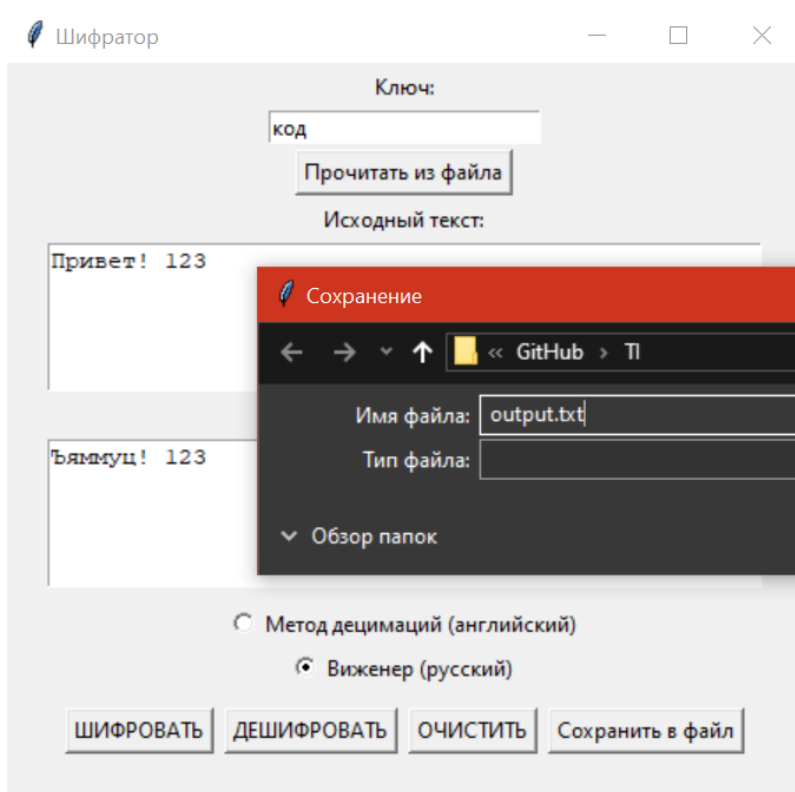


После загрузки:





Скрин выбора файла для сохранения результирующего текста:



Скрин открытого файла:

