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

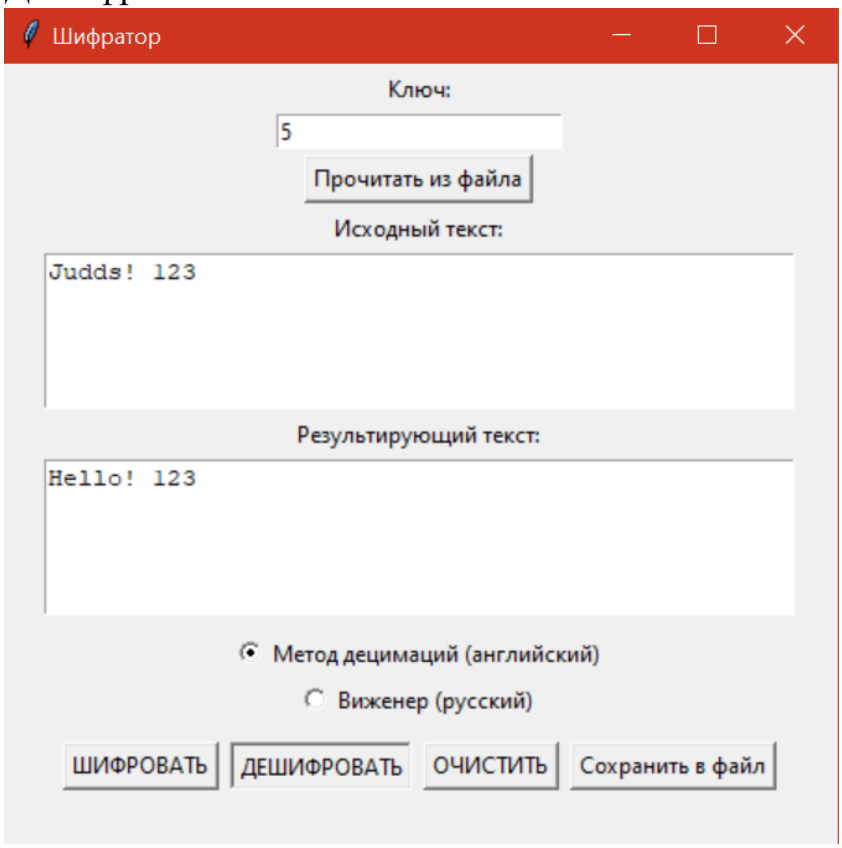
$D \rightarrow L$

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

Скрины:

Шифрование:

Дешифрование:



Ломаем на валидных данных.

Ключ меньше длины алфавита:

Ключ = 3

Шифрование:

Формула:

E(x) = (x * 3) mod 26

H = 7

(7 * 3) = 21 → V

E = 4

(4 * 3) = 12 → M

L = 11

(11 * 3) = 33 mod 26 = 7 → H

L → H

O = 14

(14 * 3) = 70 mod 26 = 16 → 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

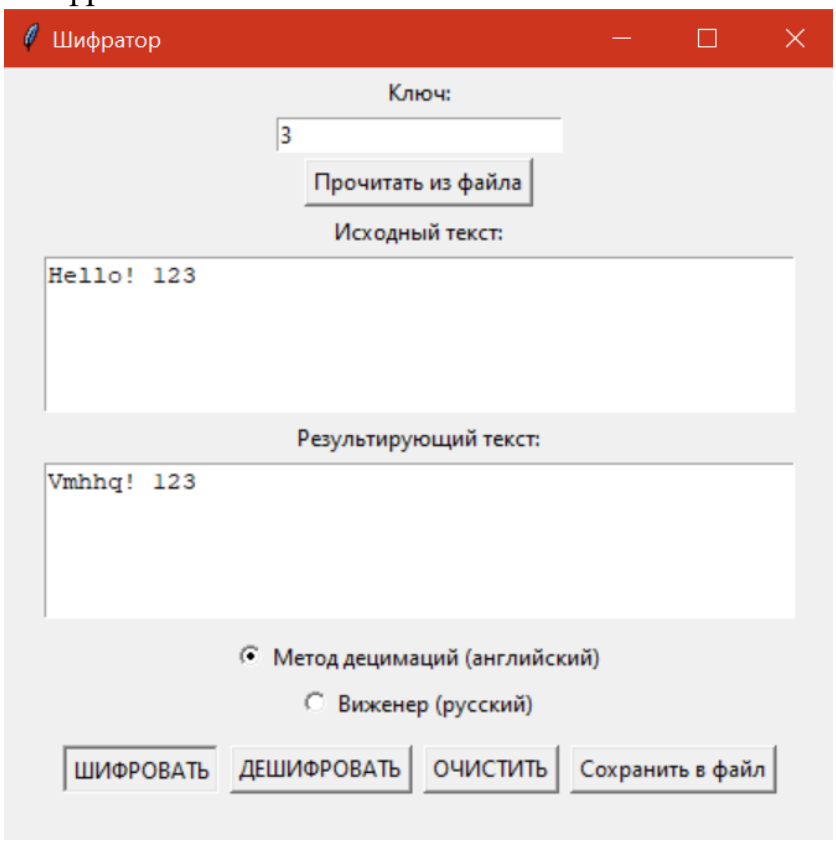
H = 7
$7 \times 3 \bmod 26 = 11 \rightarrow$ L

H → L

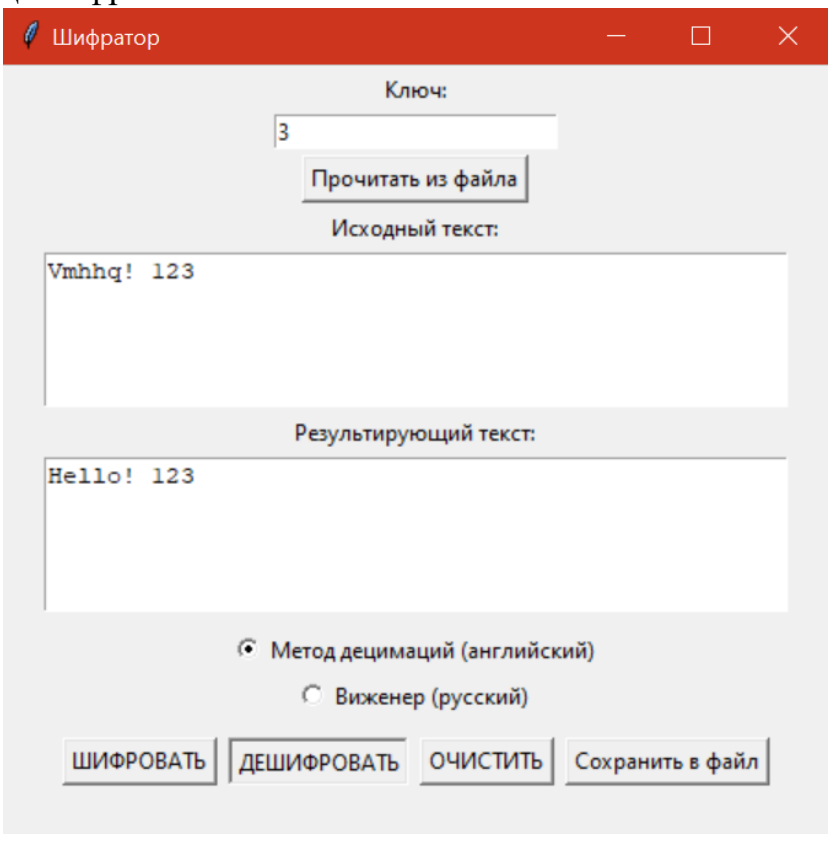
Q = 16
$16 \times 3 \bmod 26 = 14 \rightarrow$ O

Скрины:

Шифрование:



Дешифрование:

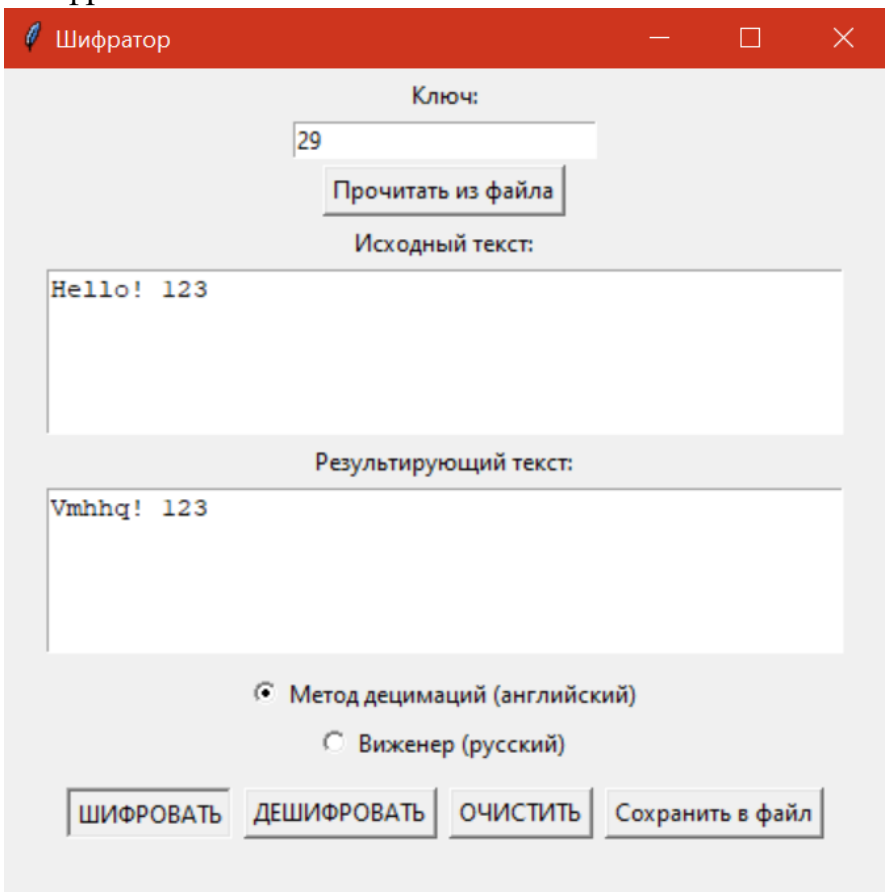


Ключ больше длины алфавита:
Ключ = 29
Шифрование:
Формула:
E(x) = (x * 29) mod 26

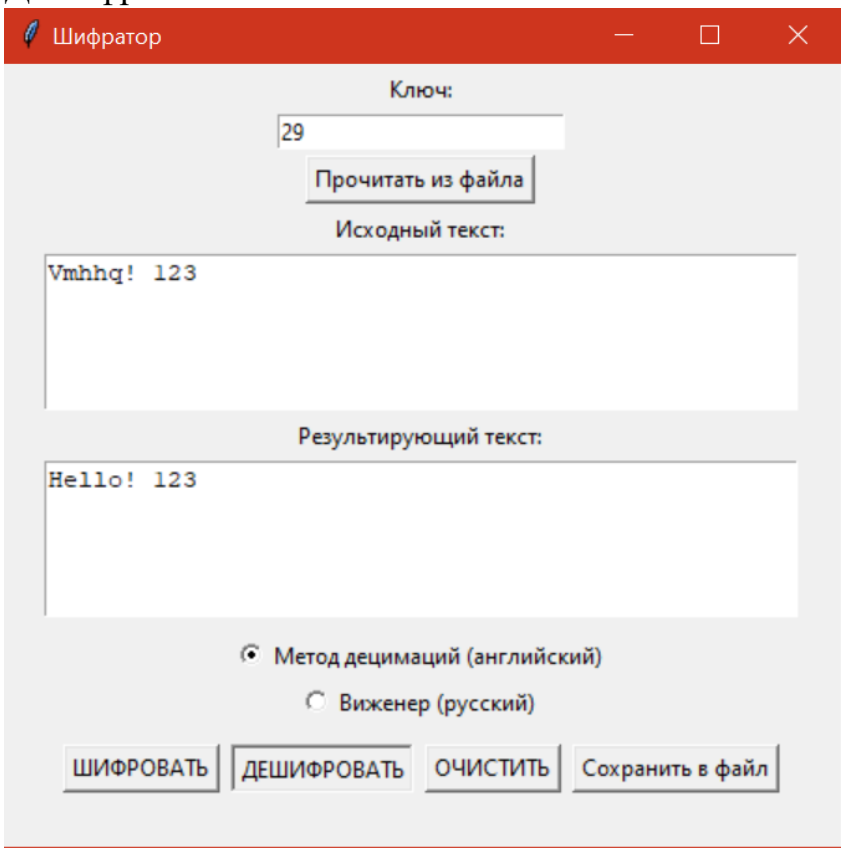
Вычисления будут такие же как в прошлом примере, потому что вычисления идут по модулю 26
29 mod 26 = 3
Ключ = 29 = 3

Скрины:

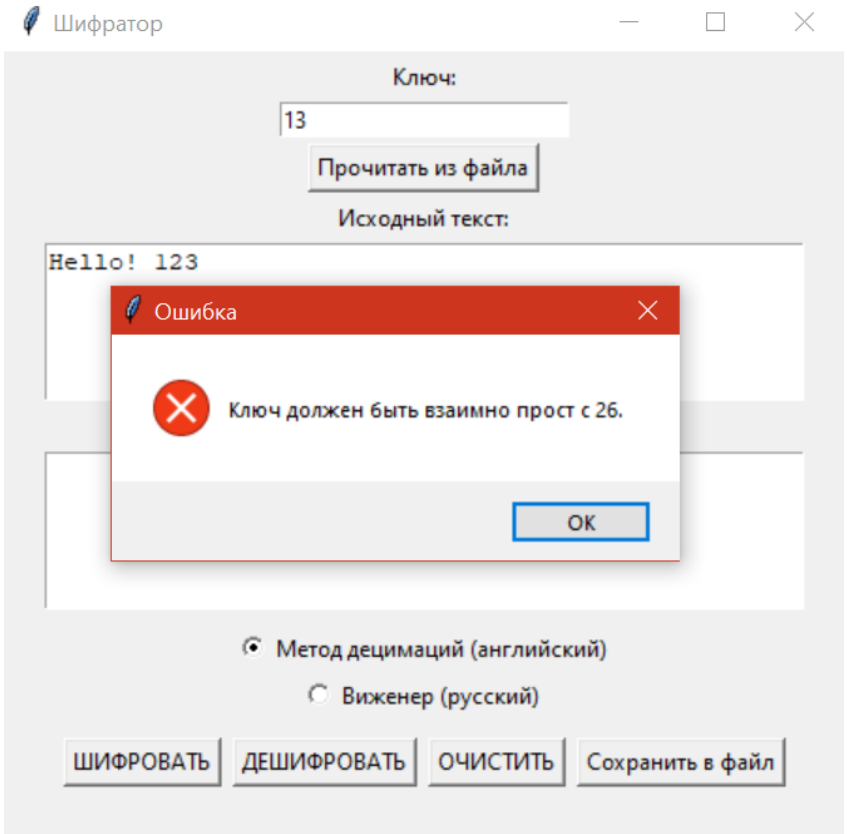
Шифрование:



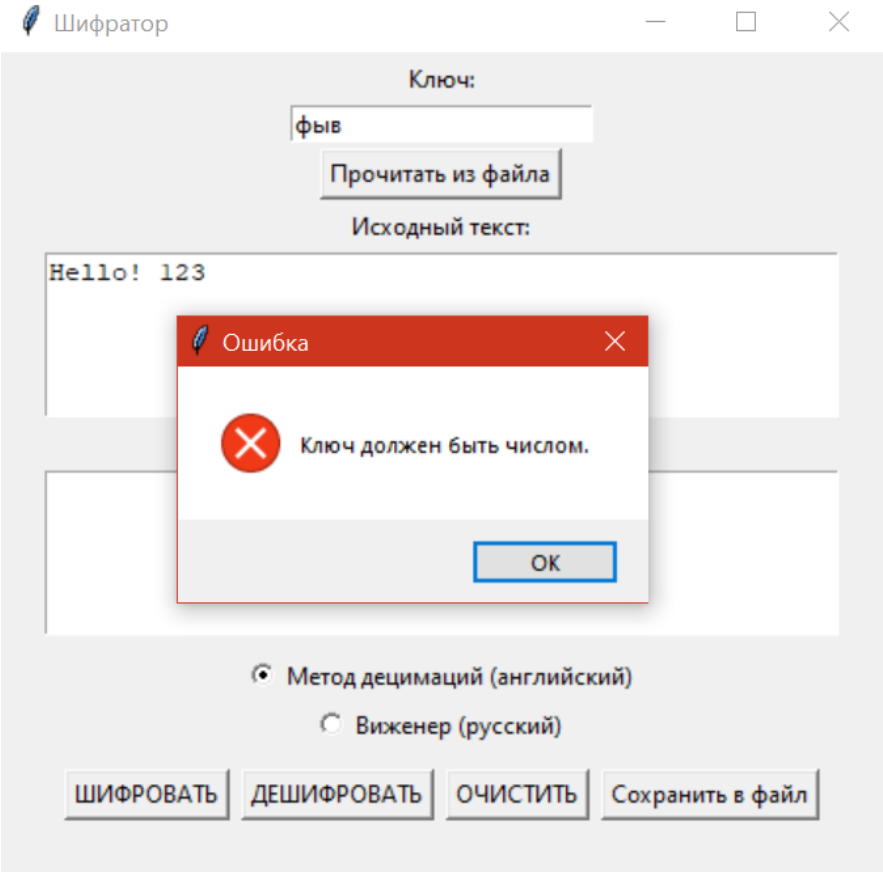
Дешифрование:



Ломаем на не валидных данных:
Ключ = 13
Ключ должен быть взаимно прост с 26»



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	ч
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	ч	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

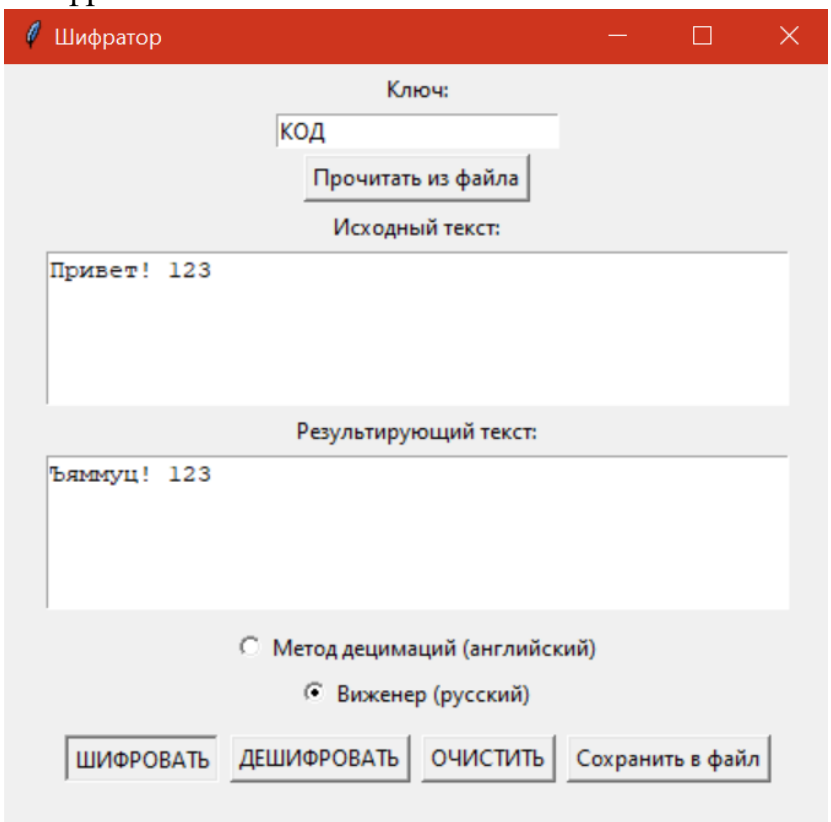
И, Д
Их пересечение по таблице → М

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:

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

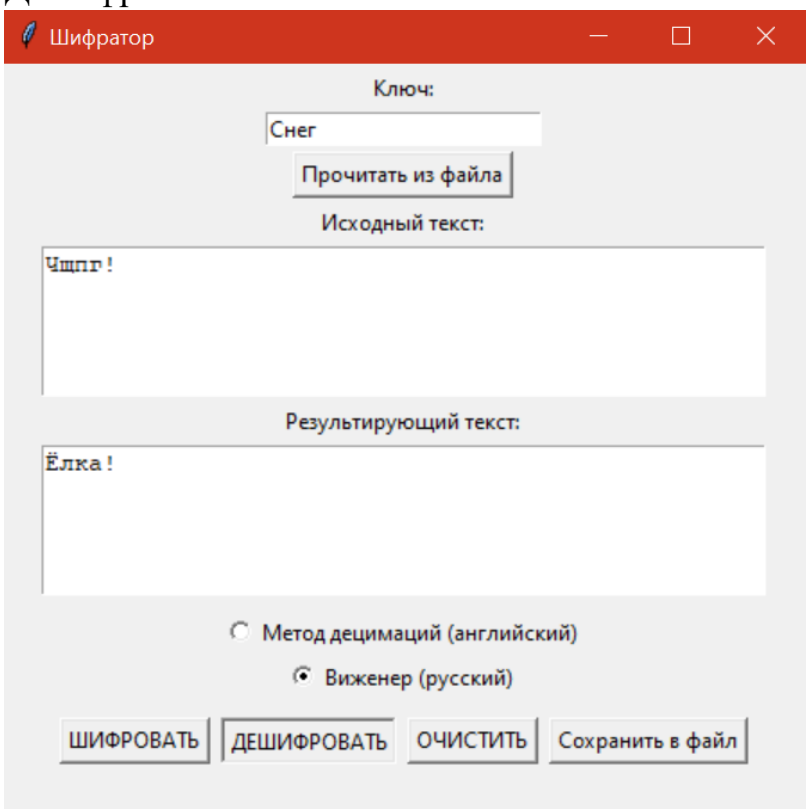
К, Е
Их пересечение по таблице → П

А, Г
Их пересечение по таблице → Г

Получается: **Чщпг!**
Скрины:

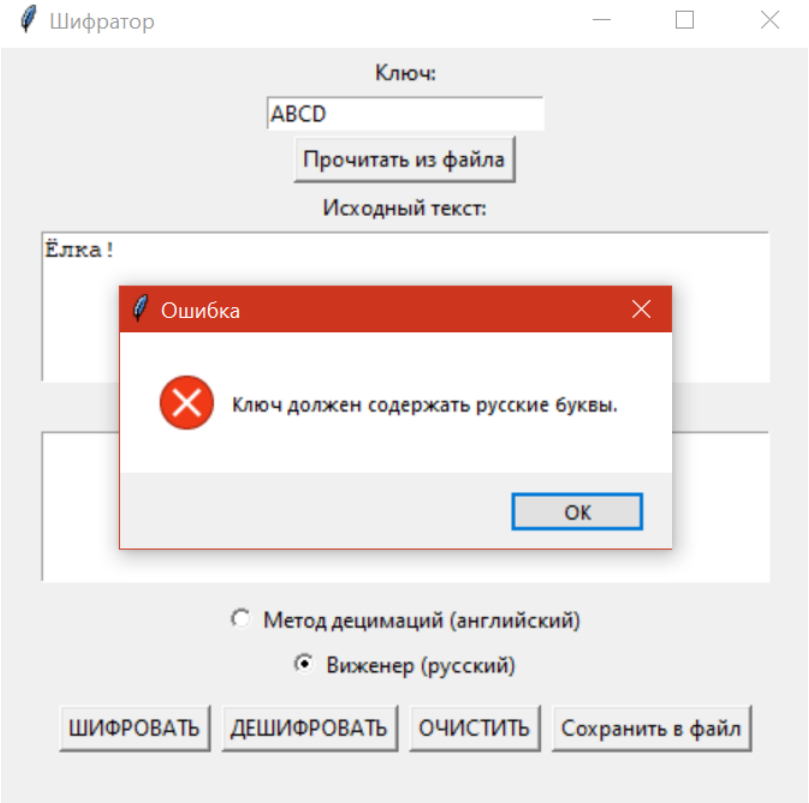
Шифрование:

Дешифрование:

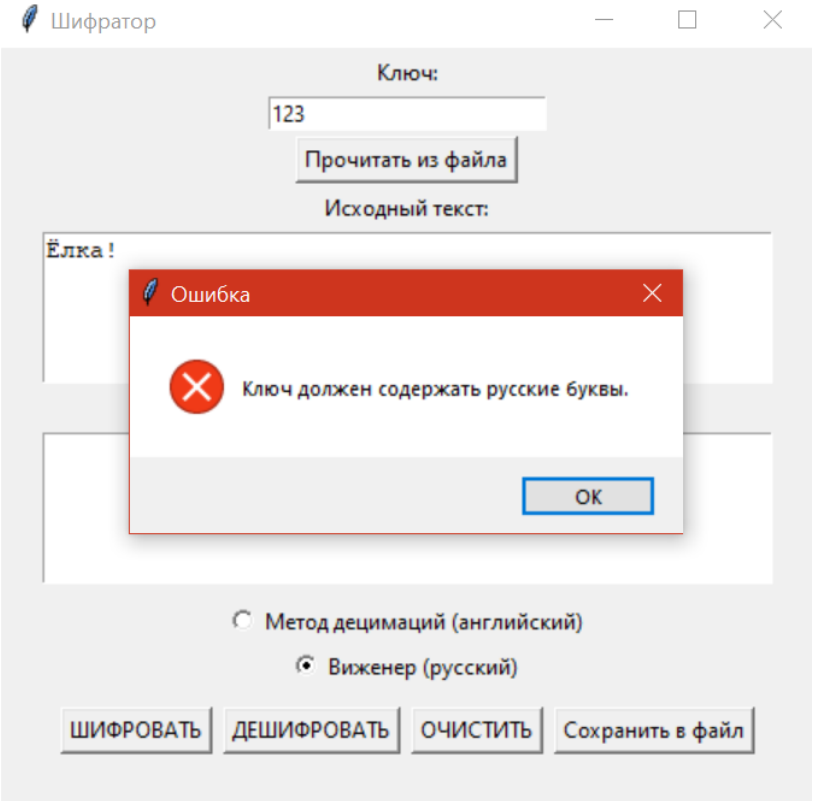


Ломаем на не валидных данных
Ключи, содержащие недопустимые значения:

Ключ: ABCD
Ключ должен содержать русские буквы
Скрин:

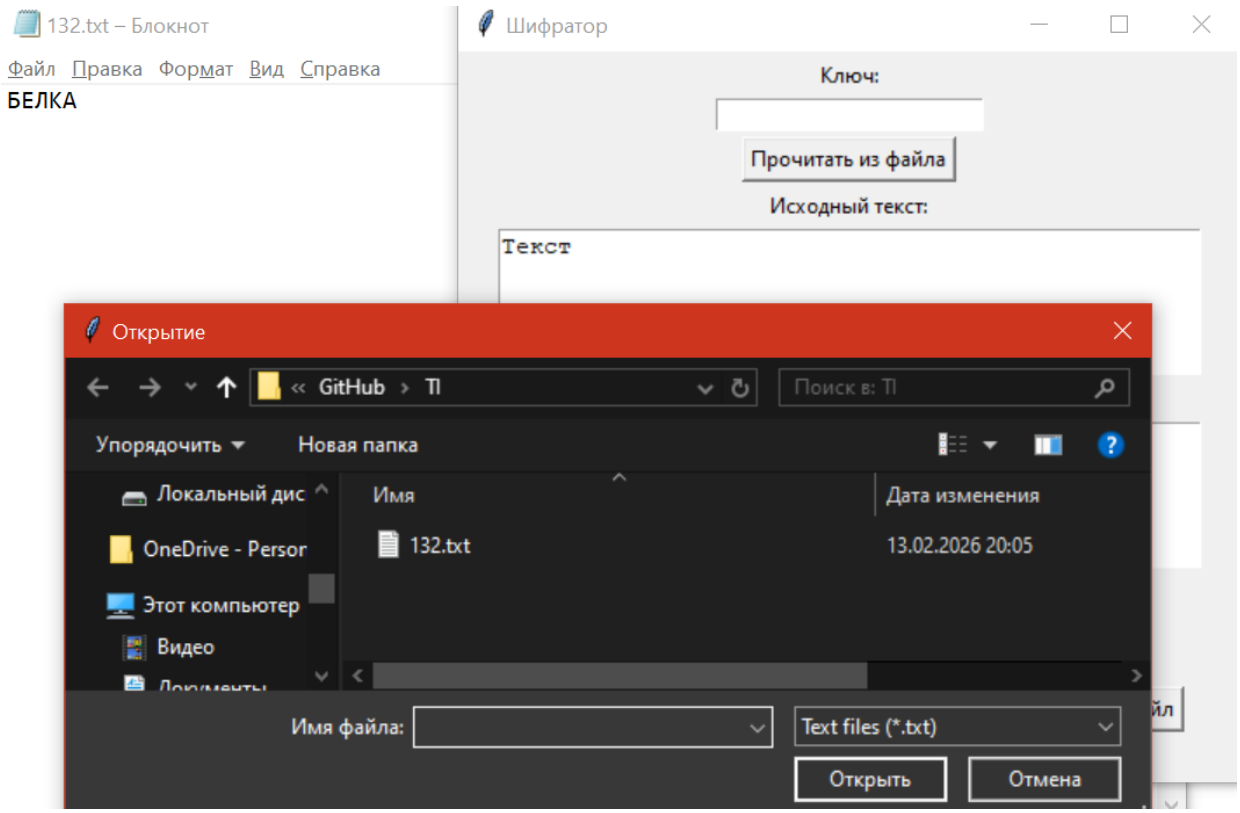


Ключ: 123

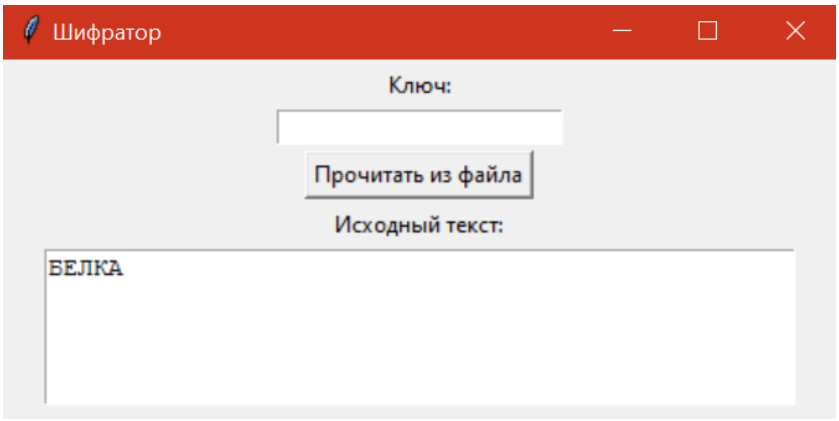


Работа с файлами

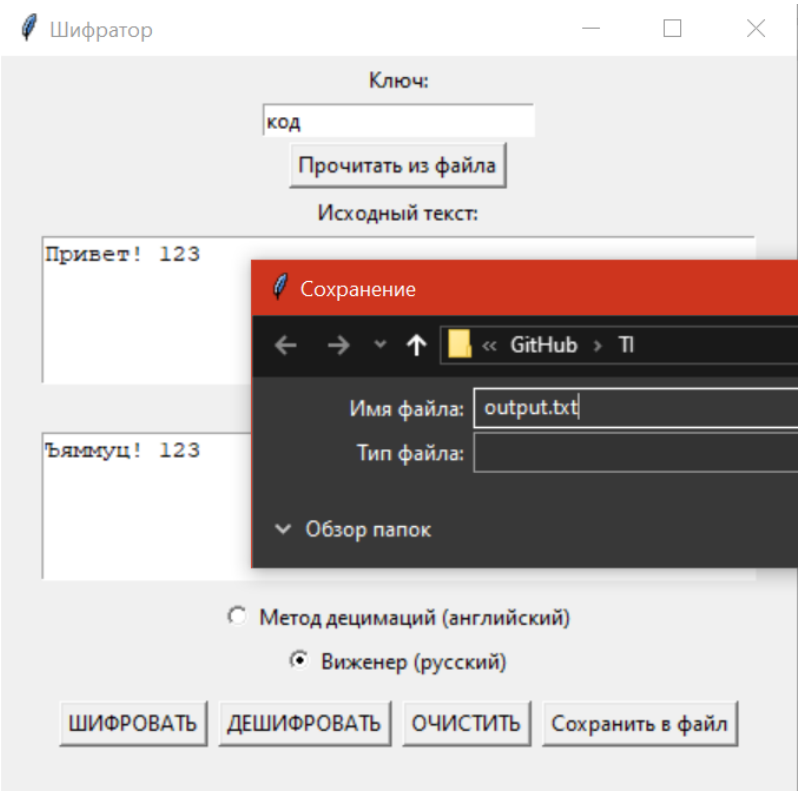
Скрин выбора файла для ввода тестовой фразы:



После загрузки:



Скрин выбора файла для сохранения результирующего текста:



Скрин открытого файла: