

Министерство образования Республики Беларусь
Учреждение образования
«Белорусский государственный университет информатики и
радиоэлектроники»

Факультет компьютерных систем и сетей
Кафедра программного обеспечения информационных технологий

Тесты к лабораторной работе №1

Проверила:
Болтак С. В.

Выполнила:
студент гр. 351001
Перова В. Д

Минск 2025

1. «Столбцовый метод» с одним ключевым словом, текст на русском языке.

1.1 Дымовое тестирование

Тестовая фраза: у многих бывают хобби

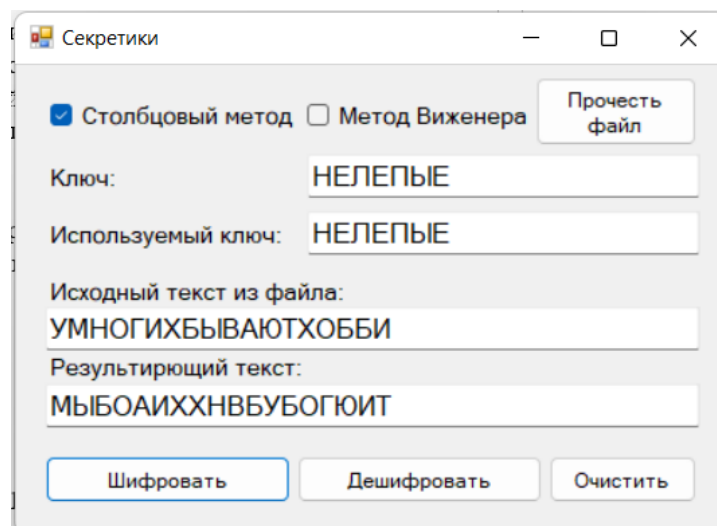
Ключевое слово: нелепые

Составим таблицу, используя ключ и тестовую фразу:

Н	Е	Л	Е	П	Ы	Е
5	1	4	2	6	7	3
У	М	Н	О	Г	И	Х
Б	Ы	В	А	Ю	Т	Х
О	Б	Б	И			

Полученный из таблицы шифротекст: **МЫБОАИХХНВБУБОГЮИТ**

Результат работы программы:



Секретики

☒ Столбцовый метод ☐ Метод Виженера Прочсть файл

Ключ: НЕЛЕПЫЕ

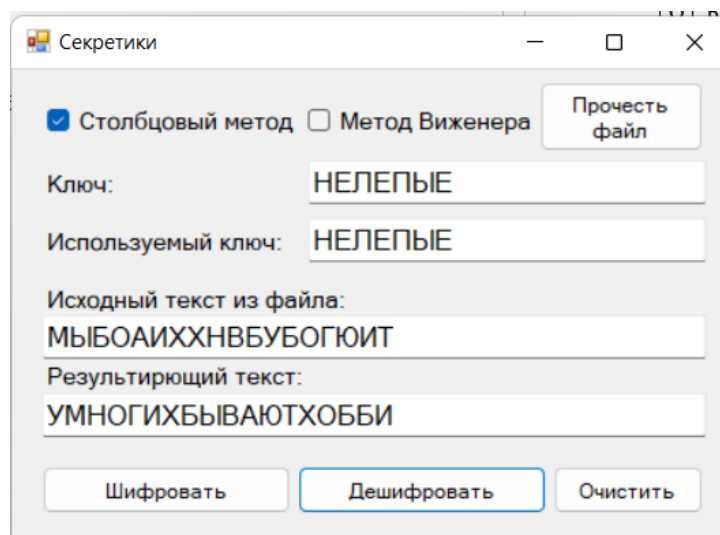
Используемый ключ: НЕЛЕПЫЕ

Исходный текст из файла: УМНОГИХБЫВАЮТХОББИ

Результирующий текст: МЫБОАИХХНВБУБОГЮИТ

Шифровать Дешифровать Очистить

Рисунок 1.1.1 – Шифрование



Секретики

☒ Столбцовый метод ☐ Метод Виженера Прочсть файл

Ключ: НЕЛЕПЫЕ

Используемый ключ: НЕЛЕПЫЕ

Исходный текст из файла: МЫБОАИХХНВБУБОГЮИТ

Результирующий текст: УМНОГИХБЫВАЮТХОББИ

Шифровать Дешифровать Очистить

Рисунок 1.1.2 – Дешифрование

1.2 Тестовая фраза заполняет полностью строчки таблицы

Тестовая фраза: **программирование**

Ключевое слово: **хобби**

Составим таблицу используя ключ и тестовую фразу:

Х	О	Б	Б	И
5	4	1	2	3
Р	И	С	О	В
А	Н	И	Е	К
А	Р	Т	И	Н

Полученный из таблицы шифротекст: **СИТОЕИВКНИНРРАА**

Результат работы программы:

The screenshot shows the 'Секретики' application window. At the top, there are checkboxes for 'Столбцовый метод' (checked) and 'Метод Виженера' (unchecked), and a 'Прочсть файл' button. Below these are input fields for 'Ключ:' and 'Используемый ключ:', both containing 'ХОББИ'. There are also input fields for 'Исходный текст из файла:' containing 'РИСОВАНИЕКАРТИН' and 'Результирующий текст:' containing 'СИТОЕИВКНИНРРАА'. At the bottom, there are three buttons: 'Шифровать' (highlighted with a blue border), 'Дешифровать', and 'Очистить'.

Рисунок 1.2.1 – Шифрование

The screenshot shows the 'Секретики' application window. At the top, there are checkboxes for 'Столбцовый метод' (checked) and 'Метод Виженера' (unchecked), and a 'Прочсть файл' button. Below these are input fields for 'Ключ:' and 'Используемый ключ:', both containing 'ХОББИ'. There are also input fields for 'Исходный текст из файла:' containing 'СИТОЕИВКНИНРРАА' and 'Результирующий текст:' containing 'РИСОВАНИЕКАРТИН'. At the bottom, there are three buttons: 'Шифровать', 'Дешифровать' (highlighted with a blue border), and 'Очистить'.

Рисунок 1.2.2 – Дешифрование

1.3 Последняя строка тестовой фразы заполнена не полностью

Тестовая фраза: **море и волны**

Ключевое слово: **картина**

Составим таблицу используя тестовую фразу и ключевое слово:

К	А	Р	Т	И	Н	А
4	1	6	7	3	5	2
М	О	Р	Е	И	В	О
Л	Н	Ы				

Полученный из таблицы шифротекст: **ОНОИМЛВРЫЕ**

Результат работы программы:

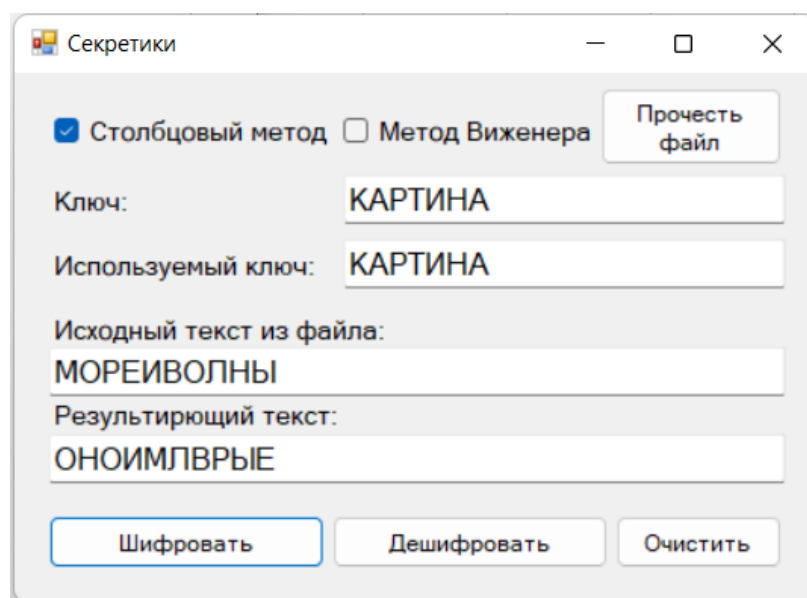


Рисунок 1.3.1 – Шифрование

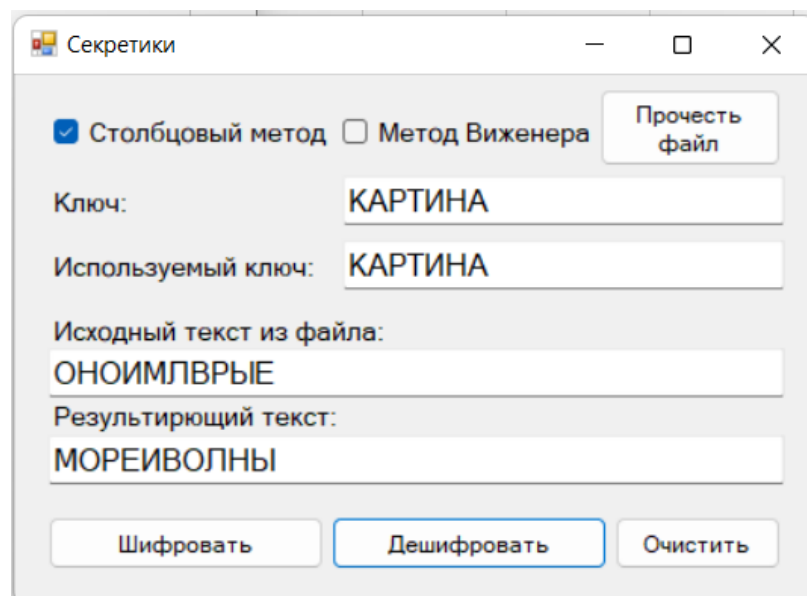


Рисунок 1.3.2 - Дешифрование

1.4 Ломаем на валидных данных

Минимальная длина ключа (ключ состоит из одной буквы).

Тестовая фраза: **программист**

Ключевое слово: **а**

Составим таблицу используя тестовую фразу и ключевое слово (для удобства таблица записана в строку, а не в столбец):

А	1	П	Р	О	Г	Р	А	М	М	И	С	Т
---	---	---	---	---	---	---	---	---	---	---	---	---

Полученный из таблицы шифротекст: **ПРОГРАММИСТ**

Результат работы программы:

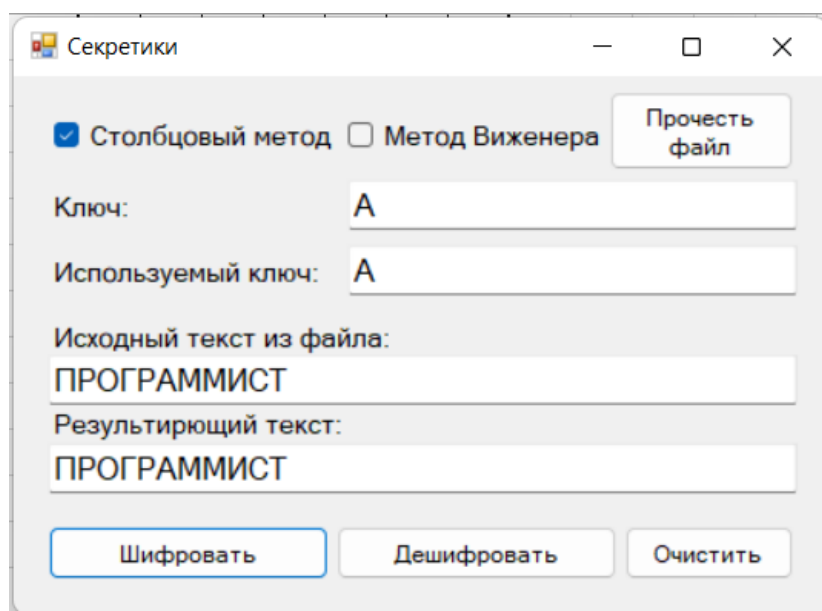


Рисунок 1.4.1 – Шифрование

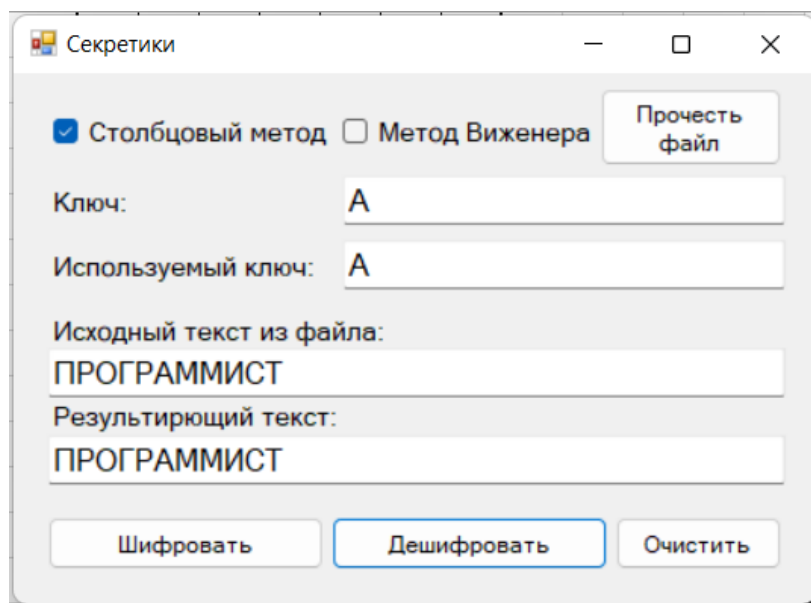


Рисунок 1.4.2 – Дешифрование

Максимальная длина ключа (ключ имеет длину, превышающую тестовое слово).

Тестовая фраза: **слово**

Ключевое слово: **очень длинный ключ**

Составим таблицу используя тестовую фразу и ключевое слово:

О	Ч	Е	Н	Ь	Д	Л	И	Н	Н	Ы	Й	К	Л	Ю	Ч
11	12	2	8	15	1	6	3	9	10	14	4	5	7	16	13
С	Л	О	В	О											

Полученный из таблицы шифротекст: **ОВСЛО**

Результат работы программы:

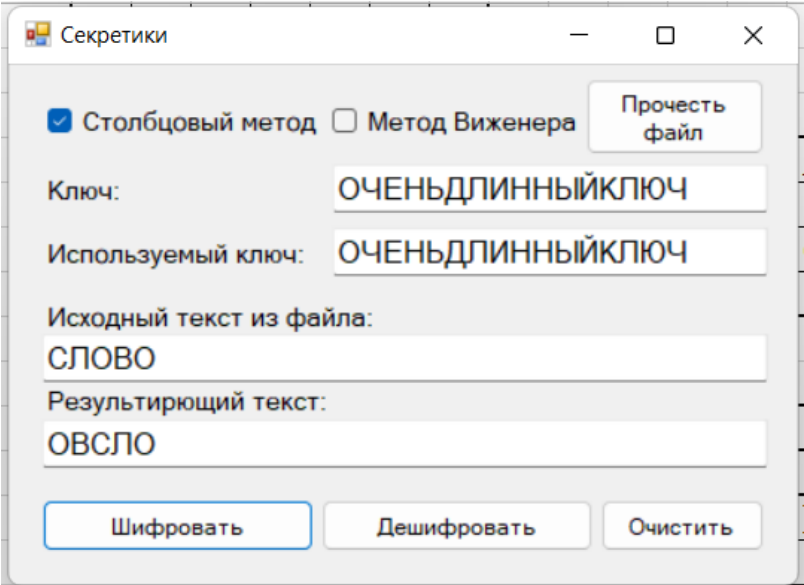


Рисунок 1.4.3 – Шифрование

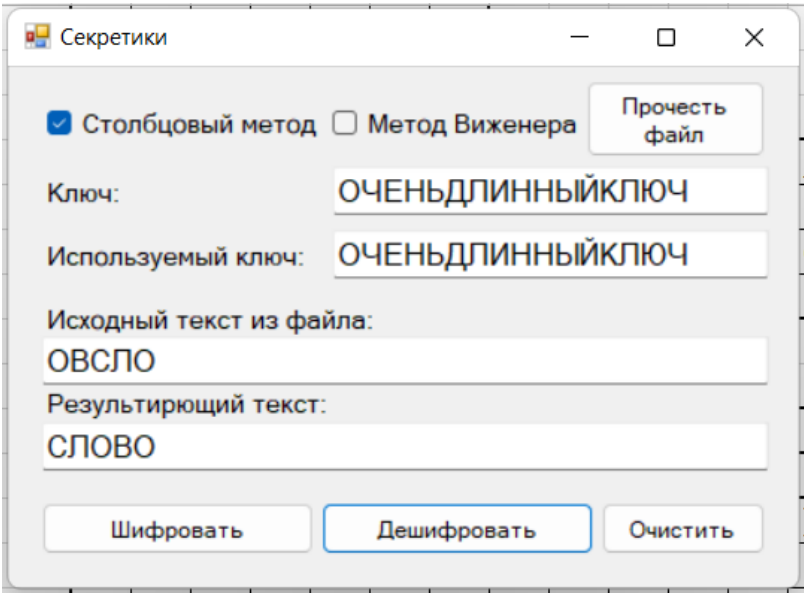


Рисунок 1.4.4 – Дешифрование

Ключ с повторяющимися символами.

Тестовая фраза: **шифрослово**

Ключевое слово: **КККЛЛЮЧ**

Составим таблицу используя тестовую фразу и ключевое слово:

К	К	К	Л	Л	Ю	Ч
1	2	3	4	5	7	6
Ш	И	Ф	Р	О	С	Л
О	В	О				

Полученный из таблицы шифротекст: **ШОИВФОРОЛС**

Результат работы программы:

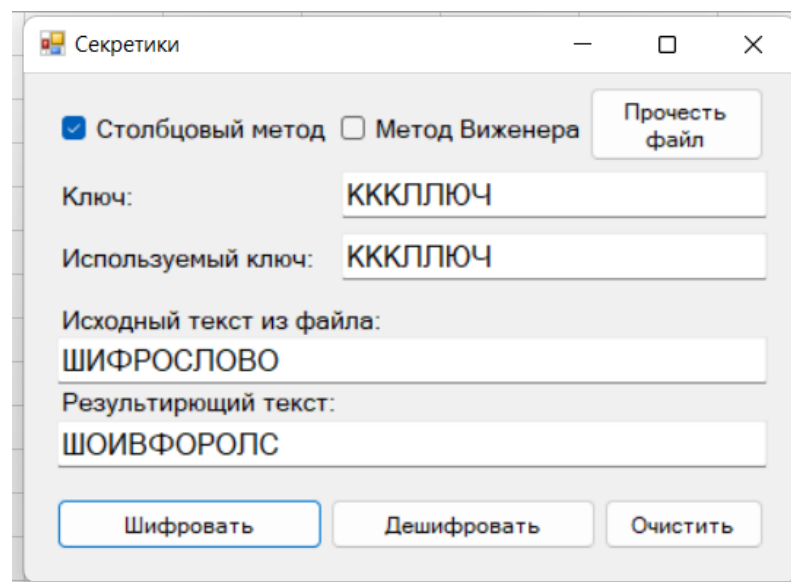


Рисунок 1.4.5 – Шифрование

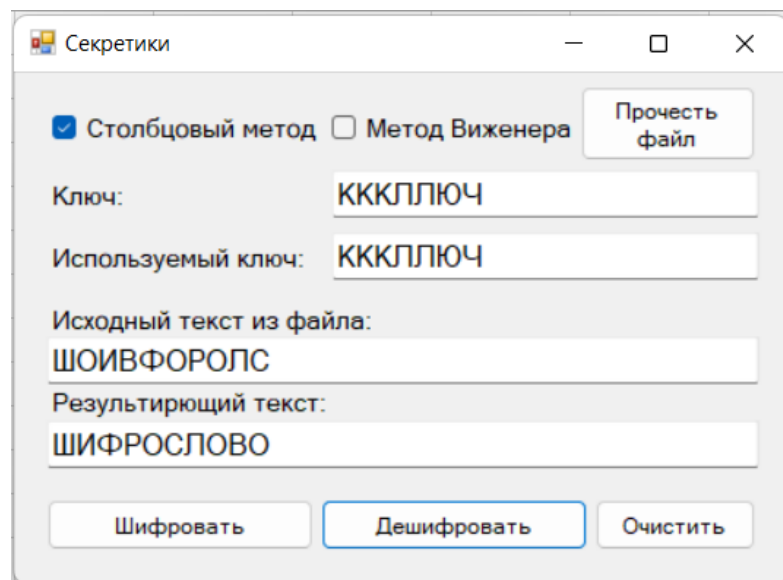


Рисунок 1.4.6 – Дешифрование

1.5 Ломаем на не валидных данных

Пустой ключ.

Тестовая фраза: программист

Ключевое слово:

Результат работы программы:

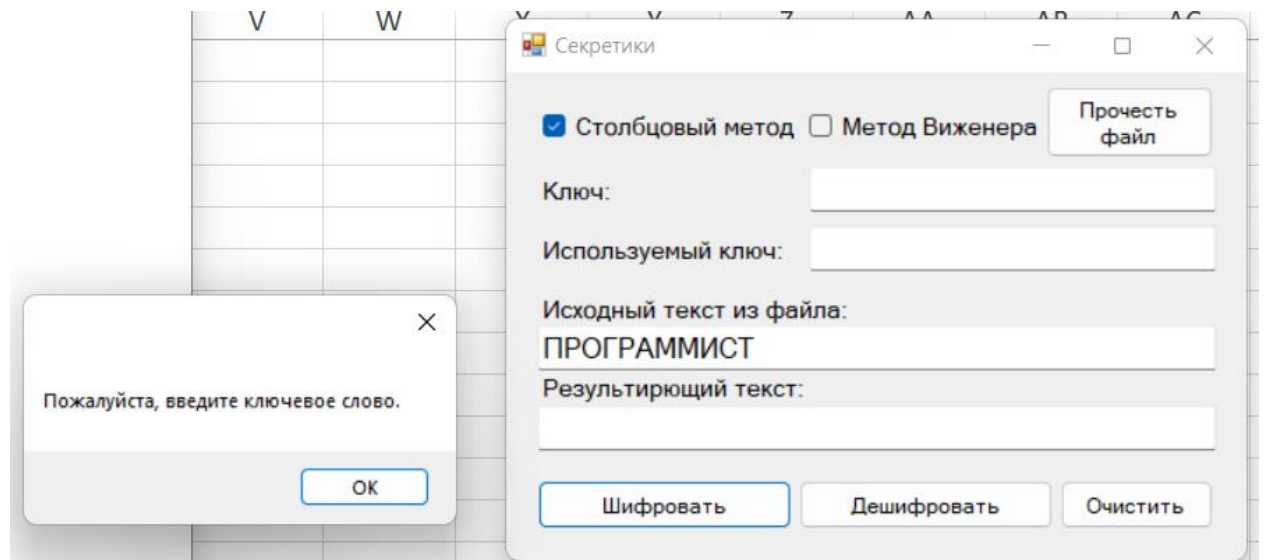


Рисунок 1.4.7 – Шифрование

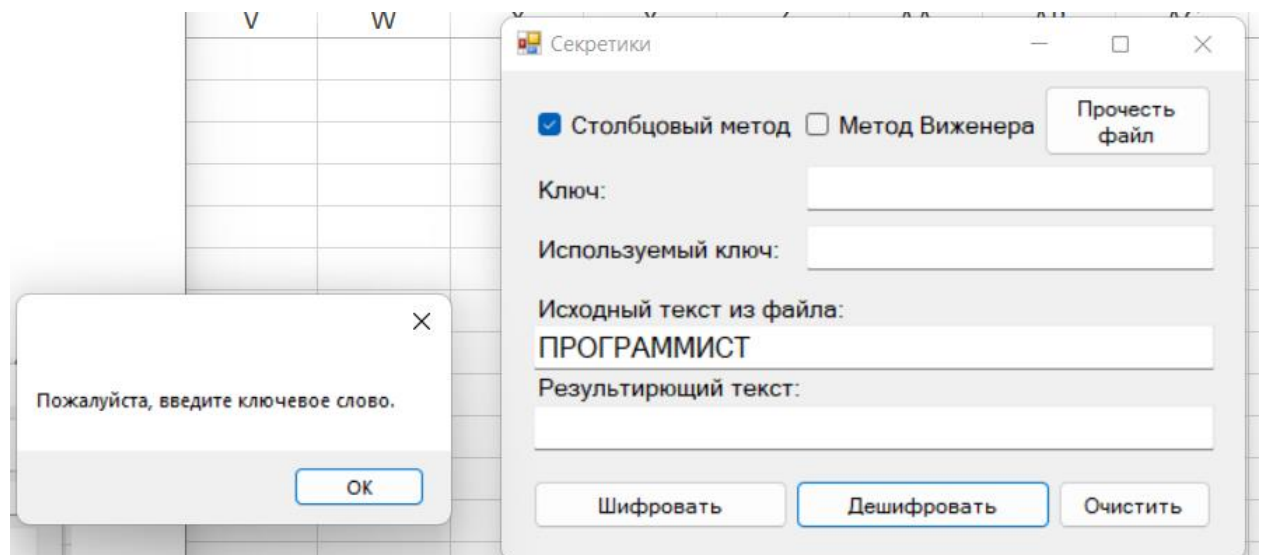


Рисунок 1.4.8 – Дешифрование

Вывод: Программа не начнет выполнять шифрование или дешифрование, пока ячейка ключа не будет заполнена

Ключ с недопустимыми значениями.

Тестовая фраза: **программист**

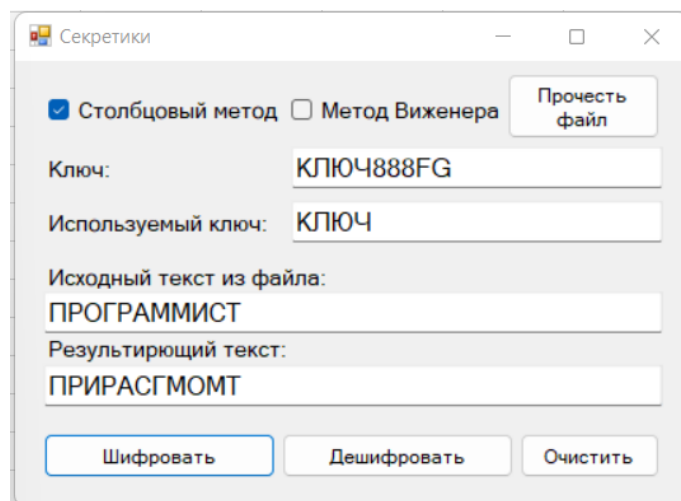
Ключевое слово: **ключ888fg**

Составим таблицу используя тестовую фразу и ключевое слово:

К	Л	Ю	Ч
1	2	4	3
П	Р	О	Г
Р	А	М	М
И	С	Т	

Полученный из таблицы шифротекст: **ПРИРАСГМОМТ**

Результат работы программы:



Секретики

☒ Столбцовый метод ☐ Метод Виженера Прочсть файл

Ключ: КЛЮЧ888FG

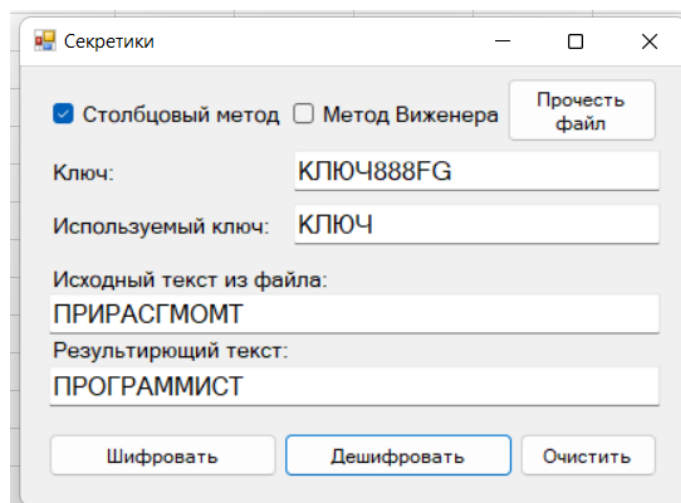
Используемый ключ: КЛЮЧ

Исходный текст из файла: ПРОГРАММИСТ

Результирующий текст: ПРИРАСГМОМТ

Шифровать Дешифровать Очистить

Рисунок 1.4.9 – Шифрование



Секретики

☒ Столбцовый метод ☐ Метод Виженера Прочсть файл

Ключ: КЛЮЧ888FG

Используемый ключ: КЛЮЧ

Исходный текст из файла: ПРИРАСГМОМТ

Результирующий текст: ПРОГРАММИСТ

Шифровать Дешифровать Очистить

Рисунок 1.4.10 – Дешифрование

Вывод: не валидные данные игнорируются при (де)шифровании.

Тестовая фраза: **I have 3 хобби**

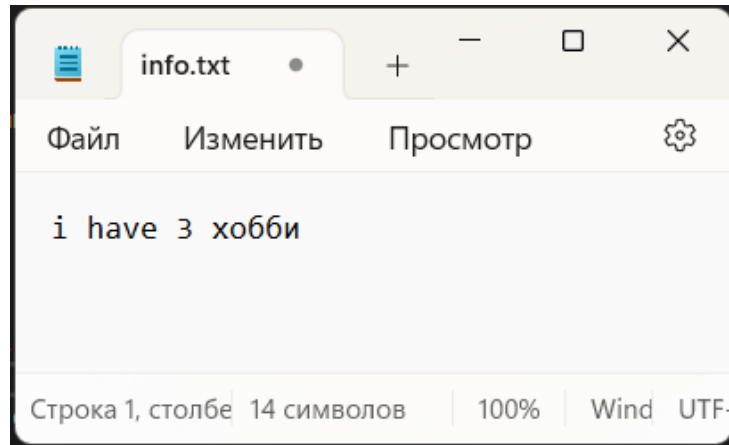
Ключевое слово: **круто**

Составим таблицу, используя ключ и тестовую фразу:

К	Р	У	Т	О
1	3	5	4	2
Х	О	Б	Б	И

Полученный из таблицы шифротекст: **ХИОББ**

Содержимое файла:



Результат работы программы:

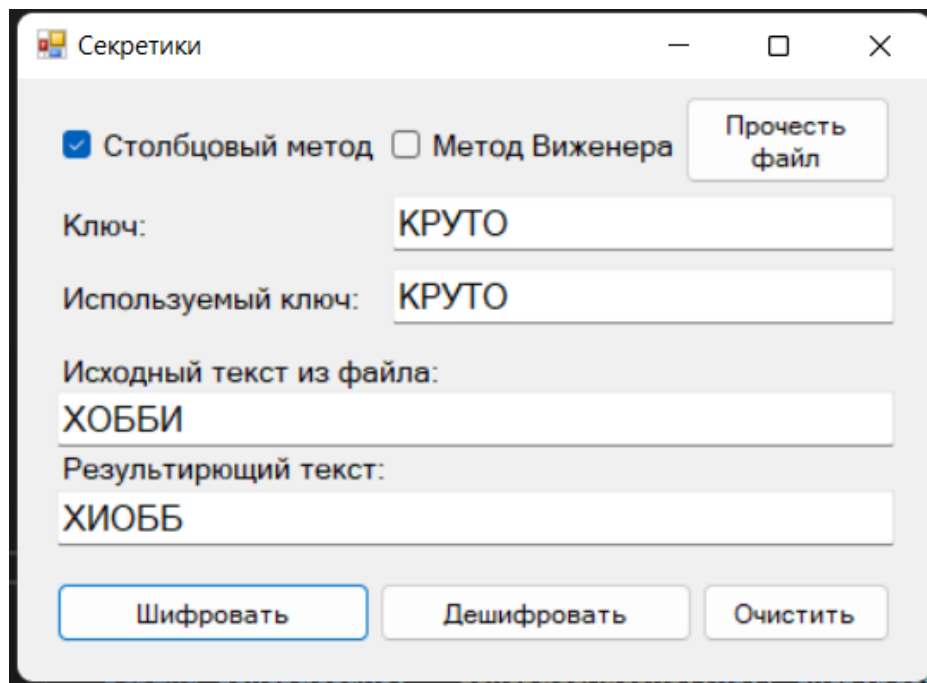


Рисунок 1.4.11 – Шифрование

Вывод: при шифровании, недопустимые значения в исходном тексте игнорируются.

Тестовая фраза (шифротекст): **ХИО22БФБ**

Ключевое слово: **круто**

Для дешифрования расставим порядок букв для ключа:

К	Р	У	Т	О
1	3	5	4	2

Теперь по порядку и подставим наш шифр (игнорируем недопустимые значения):

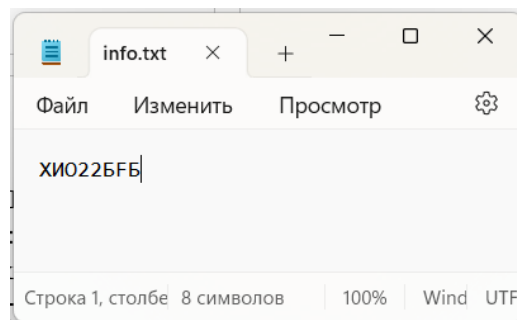
К	О	Р	Т	У
1	2	3	4	5
Х	И	О	Б	Б

Соберем ключ обратно:

К	Р	У	Т	О
1	3	5	4	2
Х	О	Б	Б	И

Полученный из таблицы текст: **ХОББИ**

Содержимое файла:



Результат работы программы:

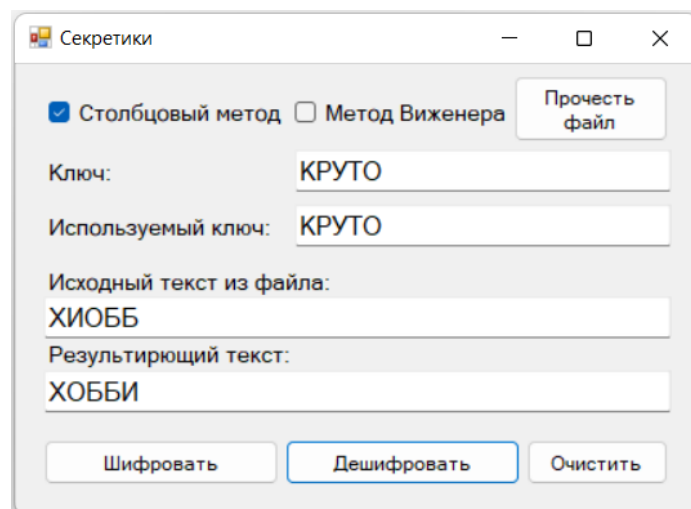


Рисунок 1.4.12 – Дешифрование (недопустимые значения игнорируются)

2.2 Расчётные формулы

2.2.1 Шифрование (1)

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

C_i – Зашифрованный символ на позиции i

P_i – Символ тестовой фразы

K_j – Символ ключа на позиции j

N – Длина алфавита (в русском составляет 33)

Пример (литературные амбиции, творчество):

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	Ъ	Ы	Ь	Э	Ю	Я
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	33

Шаги шифрования:

1. Подготовка данных:

Тестовая фраза:

Л	И	Т	Е	Р	А	Т	У	Р	Н	Ы	Е	А	М	Б	И	Ц	И	И
12	9	19	5	17	0	19	20	17	13	29	5	0	13	1	9	23	9	9

Ключевое слово:

Т	В	О	Р	Ч	Е	С	Т	В	О	Л	И	Т	Е	Р	А	Т	У	Р
19	2	15	17	22	5	18	19	2	15	12	9	19	5	17	0	19	20	17

2. Применение формулы (1):

$$(12 + 19) \bmod 33 = 31$$

$$(9 + 2) \bmod 33 = 11$$

$$(19 + 15) \bmod 33 = 1$$

$$(5 + 17) \bmod 33 = 22$$

$$(17 + 22) \bmod 33 = 6$$

$$(0 + 5) \bmod 33 = 5$$

$$(19 + 18) \bmod 33 = 4$$

$$(20 + 19) \bmod 33 = 6$$

$$(17 + 2) \bmod 33 = 19$$

$$(13 + 15) \bmod 33 = 28$$

$$(29 + 12) \bmod 33 = 8$$

$$(5 + 9) \bmod 33 = 14$$

$$(0 + 19) \bmod 33 = 19$$

$$(13 + 5) \bmod 33 = 18$$

$$(1 + 17) \bmod 33 = 18$$

$$(9 + 0) \bmod 33 = 9$$

$$(23 + 19) \bmod 33 = 9$$

$$(9 + 20) \bmod 33 = 29$$

$$(9 + 17) \bmod 33 = 26$$

3. Общая таблица с результатом:

символ фразы	Pi	символ ключа	Kj	формула	шифр
Л	12	Т	19	31	Ю
И	9	В	2	11	К
Т	19	О	15	1	Б
Е	5	Р	17	22	Ч
Р	17	Ч	22	6	З
А	0	Е	5	5	Е
Т	19	С	18	4	Д
У	20	Т	19	6	Ё
Р	17	В	2	19	Т
Н	13	О	15	28	Ь
Ы	28	Л	12	7	Ж
Е	5	И	9	14	Н
А	0	Т	19	19	Т
М	13	Е	5	18	С
Б	1	Р	17	18	С
И	9	А	0	9	И
Ц	23	Т	19	9	И
И	9	У	20	29	Ь
И	9	Р	17	26	Щ

4. Результат:

Зашифрованный текст: **ЮКБХЗЕДЁТЬЖНТССИИЬЩ**

2.2.2 Дешифрование (2)

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

C_i – Зашифрованный символ на позиции i

P_i – Символ тестовой фразы

K_j – Символ ключа на позиции j

N – Длина алфавита (в русском составляет 33)

Пример (литературные амбиции, творчество):

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	Ъ	Ы	Ь	Э	Ю	Я
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	33

Шаги шифрования:

1. Подготовка данных:

Зашифрованная фраза:

Ю	К	Б	Х	З	Е	Д	Ё	Т	Ь	Ж	Н	Т	С	С	И	И	Ь	Щ
31	11	1	22	6	5	4	6	19	28	8	14	19	18	18	9	9	29	26

Ключевое слово:

Т	В	О	Р	Ч	Е	С	Т	В	О	Ю	К	Б	Х	З	Е	Д	Ё	Т
19	2	15	17	22	5	18	19	2	15	29	11	1	22	8	5	4	6	19

2. Применение формулы (1):

$$(31 - 19 + 33) \bmod 33 = 12$$

$$(11 - 2 + 33) \bmod 33 = 9$$

$$(1 - 15 + 33) \bmod 33 = 19$$

$$(22 - 17 + 33) \bmod 33 = 5$$

$$(6 - 22 + 33) \bmod 33 = 17$$

$$(5 - 5 + 33) \bmod 33 = 0$$

$$(4 - 18 + 33) \bmod 33 = 19$$

$$(6 - 19 + 33) \bmod 33 = 20$$

$$(19 - 2 + 33) \bmod 33 = 17$$

$$(29 - 15 + 33) \bmod 33 = 14$$

Так как мы используем самогенерирующий ключ, то после того, как мы закончили расшифровывать исходный ключ, мы используем часть расшифрованного текста для его продолжения.

$$(7 - 12 + 33) \bmod 33 = 28$$

$$(14 - 9 + 33) \bmod 33 = 5$$

$$(19 - 19 + 33) \bmod 33 = 0$$

$$(18 - 5 + 33) \bmod 33 = 13$$

$$(18 - 17 + 33) \bmod 33 = 1$$

$$(9 - 0 + 33) \bmod 33 = 9$$

$$(9 - 19 + 33) \bmod 33 = 23$$

$$(29 - 20 + 33) \bmod 33 = 9$$

$$(26 - 17 + 33) \bmod 33 = 9$$

3. Общая таблица с результатом:

СИМВОЛ фразы	Pi	СИМВОЛ ключа	Kj	формула	фраза
Ю	31	Т	19	12	Л
К	11	В	2	9	И
Б	1	О	15	19	Т
Х	22	Р	17	5	Е
З	6	Ч	22	17	Р
Е	5	Е	5	0	А
Д	4	С	18	19	Т
Ё	6	Т	19	20	У
Т	19	В	2	17	Р
Ь	29	О	15	14	Н
Ж	7	Л	12	28	Ы
Н	14	И	9	5	Е
Т	19	Т	19	0	А
С	18	Е	5	13	М
С	18	Р	17	1	Б
И	9	А	0	9	И
И	9	Т	19	23	Ц
Ь	29	У	20	9	И
Щ	26	Р	17	9	И

4. Результат:

Расшифрованный текст: **ЛИТЕРАТУРНЫЕАМБИЦИИ**

2.3 Дымовое тестирование

Тестовая фраза: **литературные амбиции**

Ключевое слово: **творчество**

Сгенерированный ключ: **ТВОРЧЕСТВОЛИТЕРАТУР**

Составим таблицу, используя ключ и тестовую фразу:

Л	И	Т	Е	Р	А	Т	У	Р	Н	Ы	Е	А	М	Б	И	Ц	И	И
Т	В	О	Р	Ч	Е	С	Т	В	О	Л	И	Т	Е	Р	А	Т	У	Р
Ю	К	Б	Ч	З	Е	Д	Ё	Т	Ь	Ж	Н	Т	С	С	И	И	Ь	Щ

Полученный из таблицы шифротекст: **ЮКБХЗЕДЁТЬЖНТССИИЬЩ**

Результат работы программы:

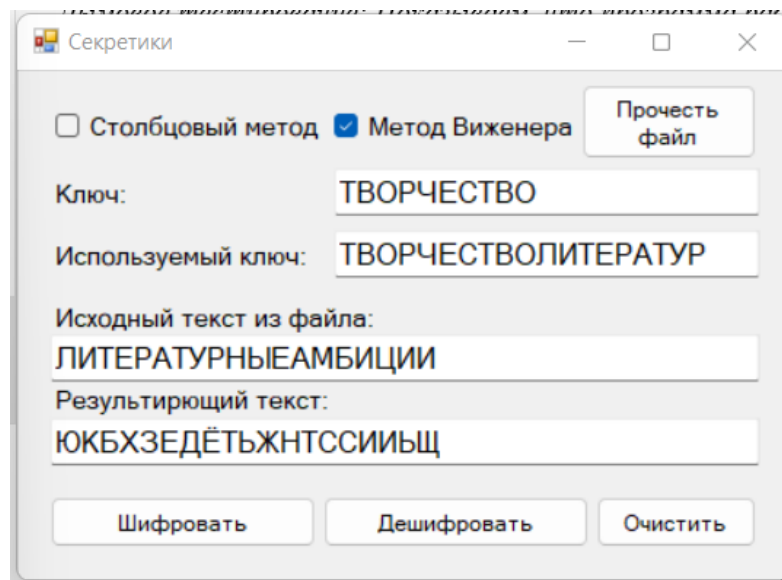


Рисунок 2.3.1 – Шифрование

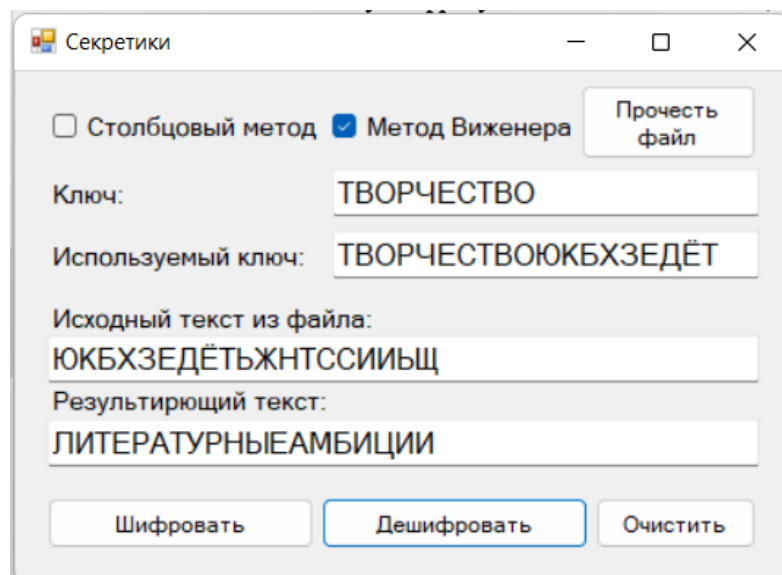


Рисунок 2.3.1 – Дешифрование

2.4 Ломаем на валидных данных (тестовая фраза, содержащая букву Ё)

Тестовая фраза: **ёж и ёлка**

Ключевое слово: **иголка**

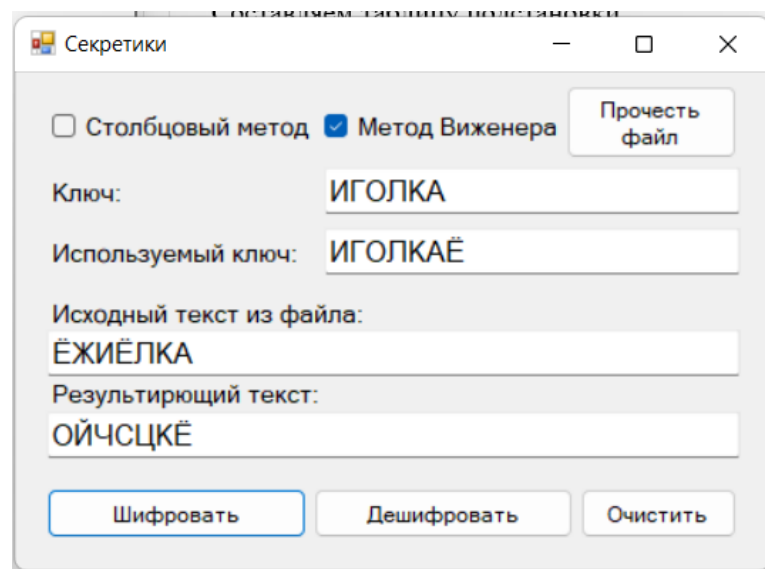
Сгенерированное слово: **ИГОЛКАЁ**

Составим таблицу, используя ключ и тестовую фразу:

Ё	Ж	И	Ё	Л	К	А
И	Г	О	Л	К	А	Ё
О	Й	Ч	С	Ц	К	Ё

Полученный из таблицы шифротекст: **ОЙЧСЦКЁ**

Результат работы программы:



Секретики

☐ Столбцовый метод ☒ Метод Виженера Прочитать файл

Ключ: ИГОЛКА

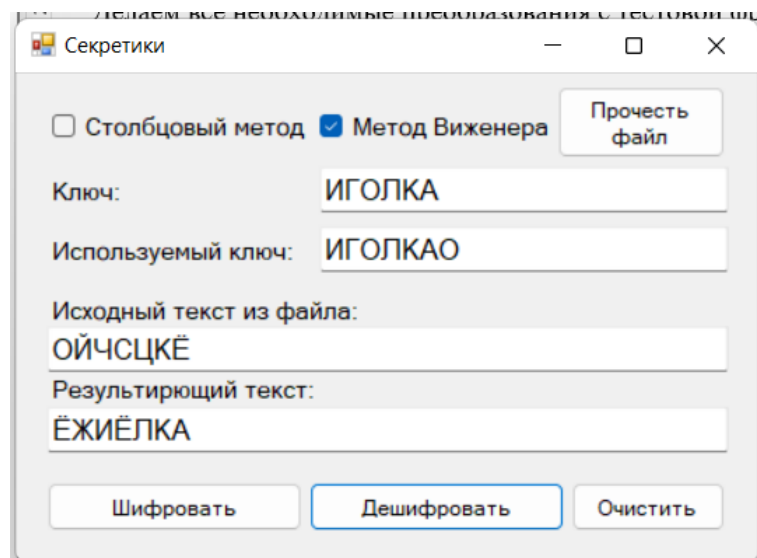
Используемый ключ: ИГОЛКАЁ

Исходный текст из файла: ЁЖИЁЛКА

Результирующий текст: ОЙЧСЦКЁ

Шифровать Дешифровать Очистить

Рисунок 2.4.1 – Шифрование



Секретики

☐ Столбцовый метод ☒ Метод Виженера Прочитать файл

Ключ: ИГОЛКА

Используемый ключ: ИГОЛКАО

Исходный текст из файла: ОЙЧСЦКЁ

Результирующий текст: ЁЖИЁЛКА

Шифровать Дешифровать Очистить

Рисунок 2.4.2 – Дешифрование

2.5 Ломаем на не валидных данных (ключ содержит недопустимые значения)

Тестовая фраза: **несколько значений**

Ключевое слово: **число**

Сгенерированное слово: **ЧИСЛО НЕСКОЛЬКО ЗНА**

Составим таблицу, используя ключ и тестовую фразу:

Н	Е	С	К	О	Л	Ь	К	О	З	Н	А	Ч	Е	Н	И	Й
Ч	И	С	Л	О	Н	Е	С	К	О	Л	Ь	К	О	З	Н	А
Е	Н	Г	Ц	Э	Щ	Б	Ь	Щ	Ц	Щ	Ь	В	У	Х	Ц	Й

Полученный из таблицы шифротекст: **ЕНГЦЭЩБЬЩЦЩЬВУХЦЙ**

Результат работы программы:

Секретики

☐ Столбцовый метод ☒ Метод Виженера Прочсть файл

Ключ: FЧИС9ЛО

Используемый ключ: ЧИСЛО НЕСКОЛЬКО ЗНА

Исходный текст из файла: НЕСКОЛЬКОЗНАЧЕНИЙ

Результирующий текст: ЕНГЦЭЩБЬЩЦЩЬВУХЦЙ

Шифровать Дешифровать Очистить

Рисунок 2.5.1 – Шифрование

Секретики

☐ Столбцовый метод ☒ Метод Виженера Прочсть файл

Ключ: FЧИС9ЛО

Используемый ключ: ЧИСЛО ЕНГЦЭЩБЬЩЦЩЬ

Исходный текст из файла: ЕНГЦЭЩБЬЩЦЩЬВУХЦЙ

Результирующий текст: НЕСКОЛЬКОЗНАЧЕНИЙ

Шифровать Дешифровать Очистить

Рисунок 2.5.2 – Дешифрование