УО «Белорусский государственный университет информатики и радиоэлектроники»

Кафедра ПОИТ

Тесты к лабораторной работе № 1

по предмету «Теория информации»

Вариант 6

Выполнил:

Жигимонт А.Н.

гр. 351003

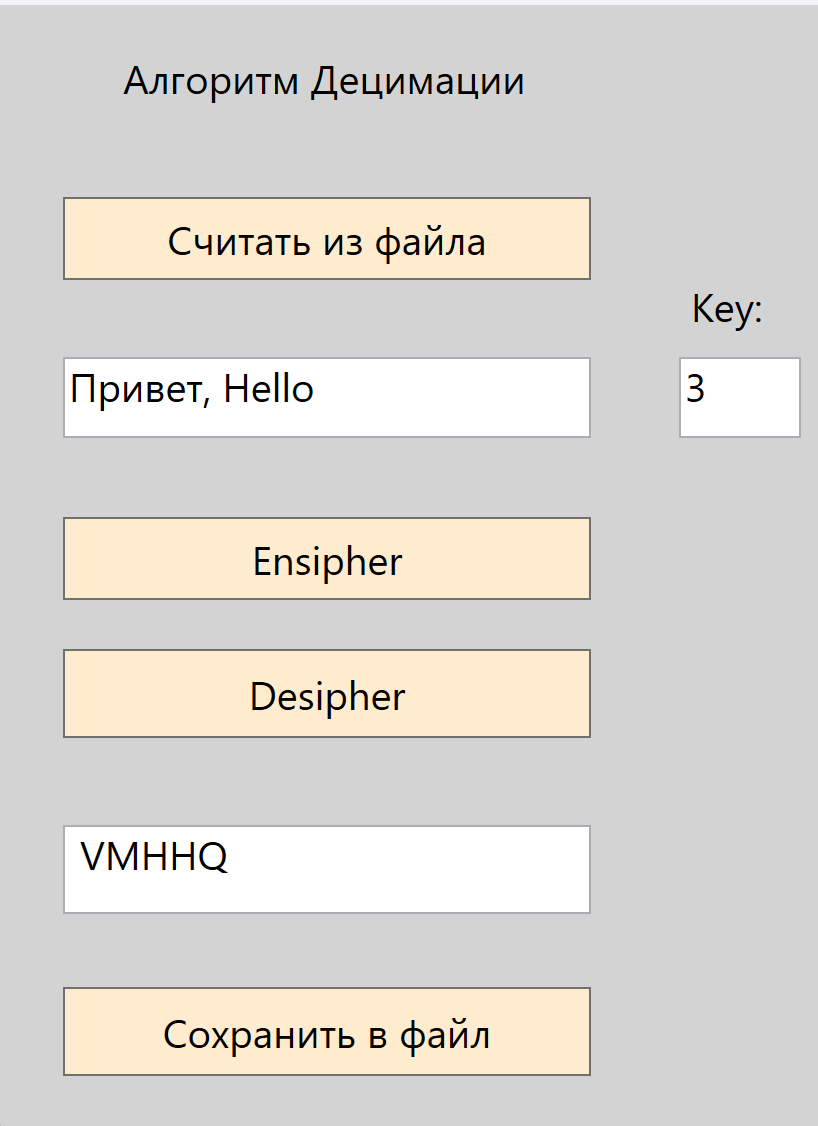
Проверила:

Болтак С.В.

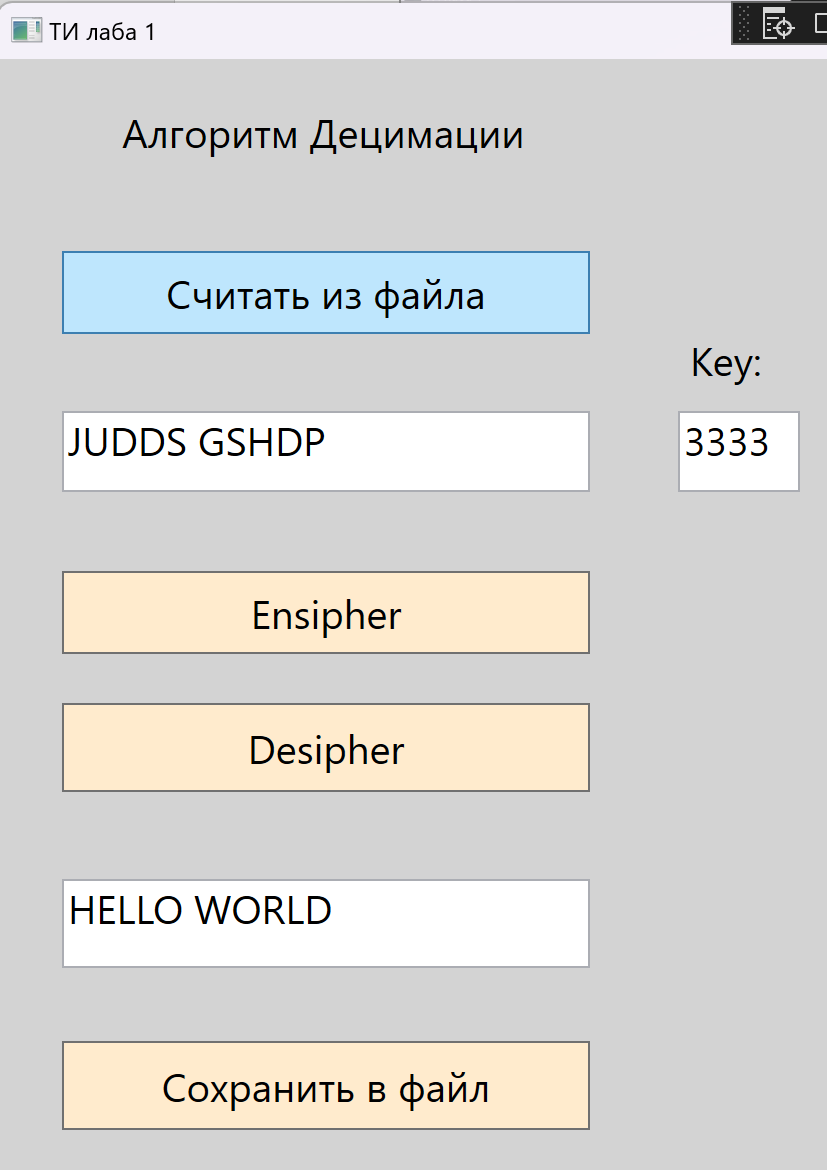
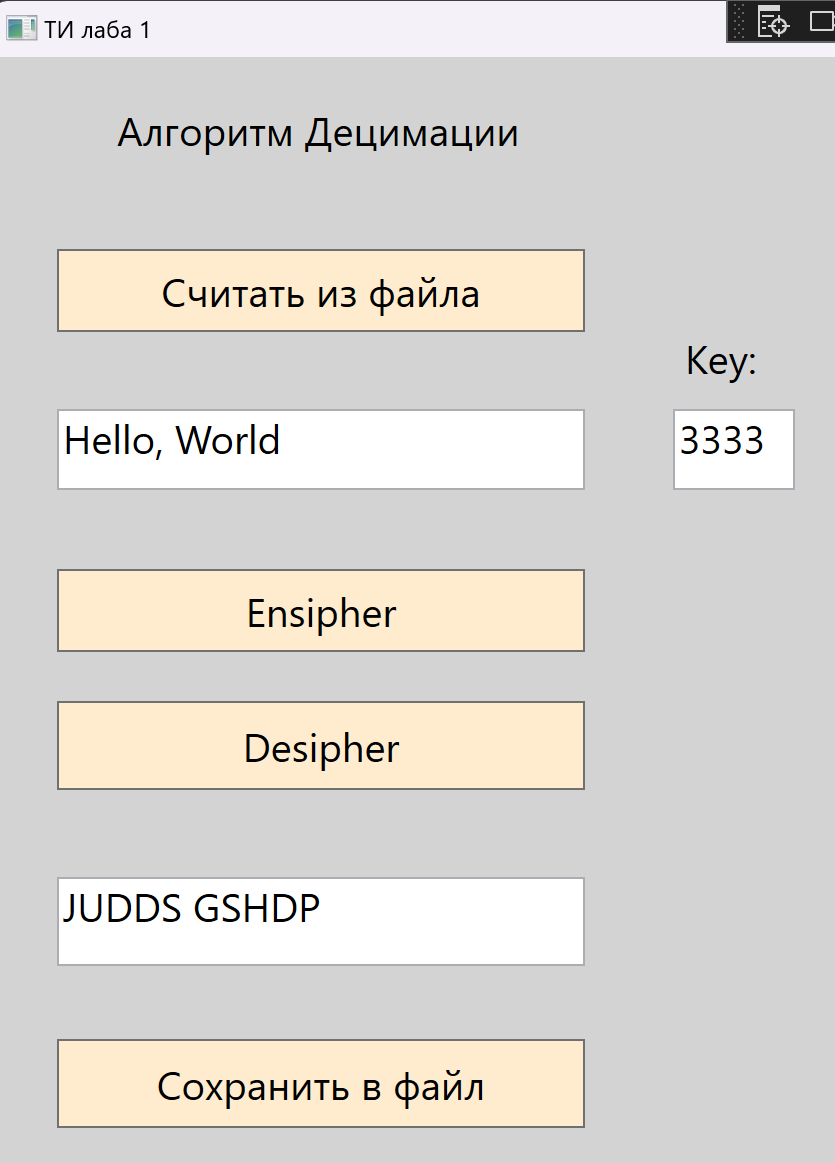
Минск, 2025

**Метод децимаций**

*Дымовое тестирование:*

**

*Ломаем на валидных данных:*

**

Для шифрования методом децимаций по формуле  
  c = (a ⋅ k) mod n

при условии, что:  
 • n = 26  
 • k = 3333.

Заметим, что сначала удобно привести ключ к остатку от деления на 26:  
  3333 mod 26 = 5

То есть эквивалентное преобразование выглядит как:  
  c = (a ⋅ 5) mod 33,  
где a – номер буквы исходного алфавита, нумеруемого от 0 до 25.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Исходная буква | Индекс | Вычисление | Результат (индекс) | Зашифрованная буква |
| A | 0 | 5 \* 0 mod 26 = 0 | 0 | A |  |
| B | 1 | 5 \* 1 mod 26 = 5 | 5 | F |  |
| C | 2 | 5 \* 2 mod 26 = 10 | 10 | K |  |
| D | 3 | 5 \* 3 mod 26 = 15 | 15 | P |  |
| E | 4 | 5 \* 4 mod 26 = 20 | 20 | U |  |
| F | 5 | 5 \* 5 mod 26 = 25 | 25 | Z |  |
| G | 6 | 5 \* 6 mod 26 = 4 | 4 | E |  |
| H | 7 | 5 \* 7 mod 26 = 9 | 9 | J |  |
| I | 8 | 5 \* 8 mod 26 = 14 | 14 | O |  |
| J | 9 | 5 \* 9 mod 26 = 19 | 19 | T |  |
| K | 10 | 5 \* 10 mod 26 = 24 | 24 | Y |  |
| L | 11 | 5 \* 11 mod 26 = 3 | 3 | D |  |
| M | 12 | 5 \* 12 mod 26 = 8 | 8 | I |  |
| N | 13 | 5 \* 13 mod 26 = 13 | 13 | N |  |
| O | 14 | 5 \* 14 mod 26 = 18 | 18 | S |  |
| P | 15 | 5 \* 15 mod 26 = 23 | 23 | X |  |
| Q | 16 | 5 \* 16 mod 26 = 2 | 2 | C |  |
| R | 17 | 5 \* 17 mod 26 = 7 | 7 | H |  |
| S | 18 | 5 \* 18 mod 26 = 12 | 12 | M |  |
| T | 19 | 5 \* 19 mod 26 = 17 | 17 | R |  |
| U | 20 | 5 \* 20 mod 26 = 22 | 22 | W |  |
| V | 21 | 5 \* 21 mod 26 = 1 | 1 | B |  |
| W | 22 | 5 \* 22 mod 26 = 6 | 6 | G |  |
| X | 23 | 5 \* 23 mod 26 = 11 | 11 | L |  |
| Y | 24 | 5 \* 24 mod 26 = 16 | 16 | Q |  |
| Z | 25 | 5 \* 25 mod 26 = 21 | 21 | V |  |
|  |  |  |  |  |  |

Таким образом, для исходного текста «Hello World» при использовании данного метода шифрования каждая буква будет заменена согласно указанной таблице (при этом символы, отсутствующие в алфавите, например, пробел и знаки препинания, остаются без изменений).

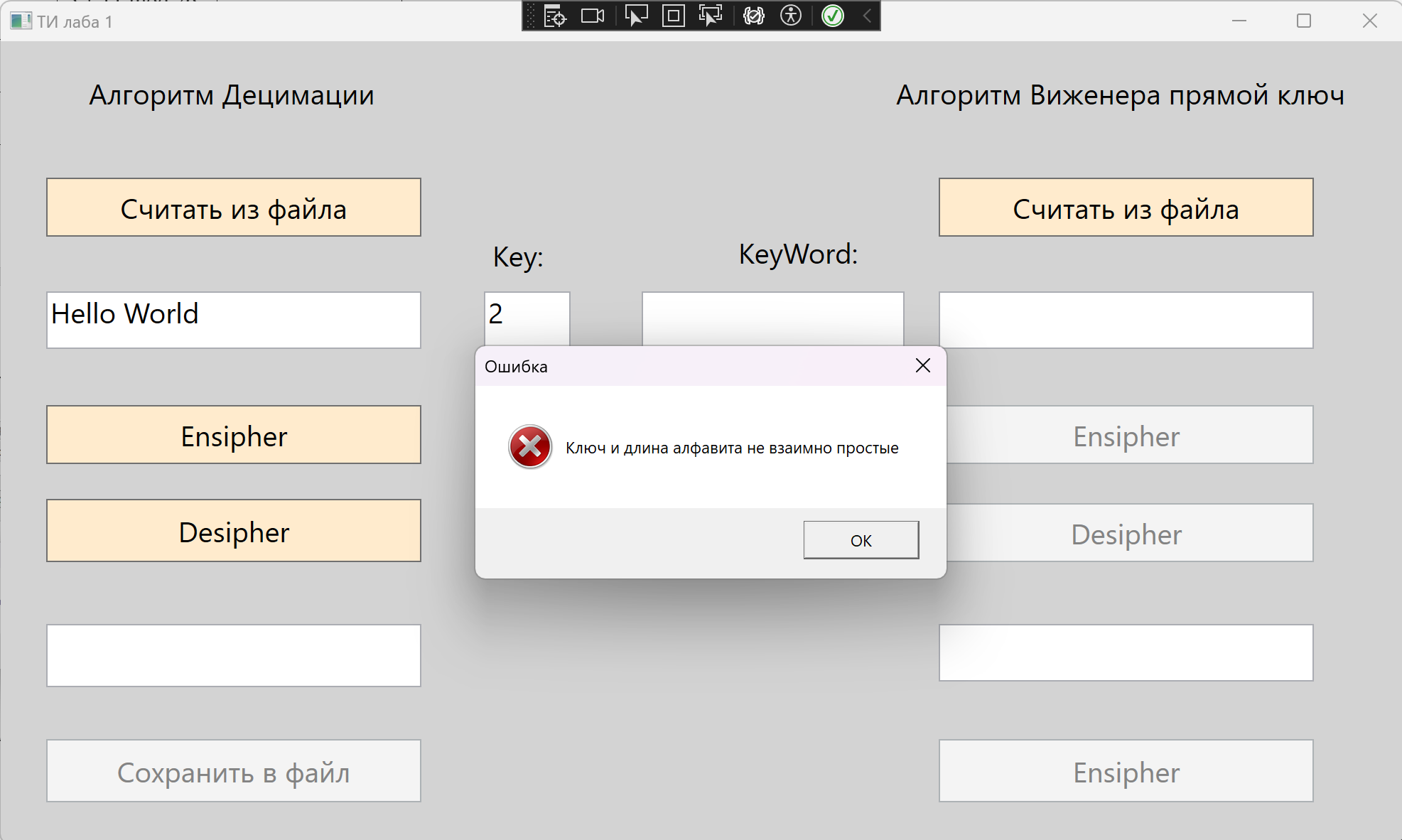
**Исходный текст:**

JUDDS GSHDP

**Зашифрованный текст:**

HELLO WORLD

*Ломаем на не валидных данных:*



**Шифр Виженера, самогенерирующийся ключ**

*Дымовое тестирование: Показываем, что программа работает.*

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

Таблица преобразований для русского алфавита

Исходный текст:

Привет Мир

Ключ:

Ключ

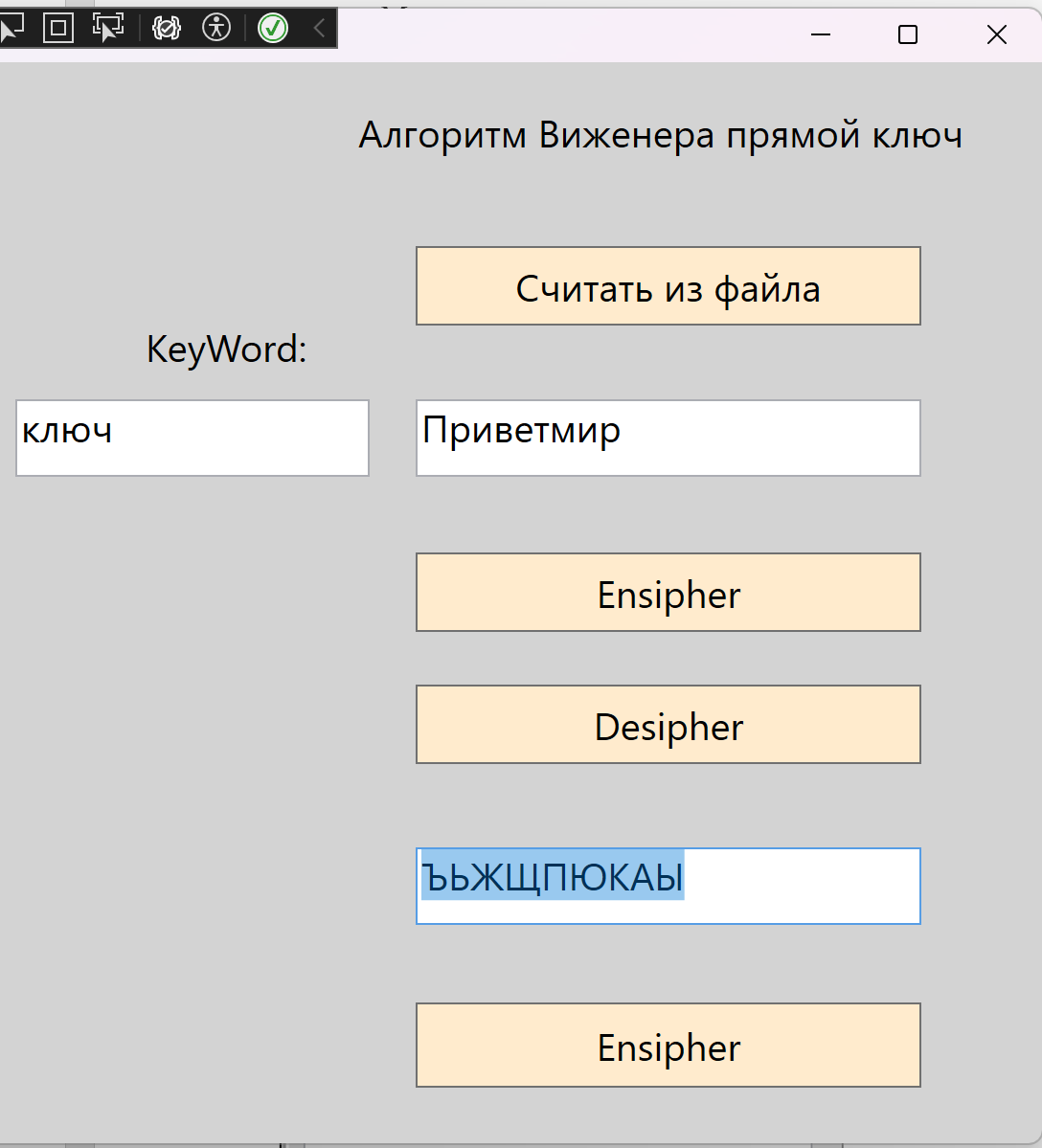
Сгенерированный ключ:

КЛЮЧКЛЮЧК

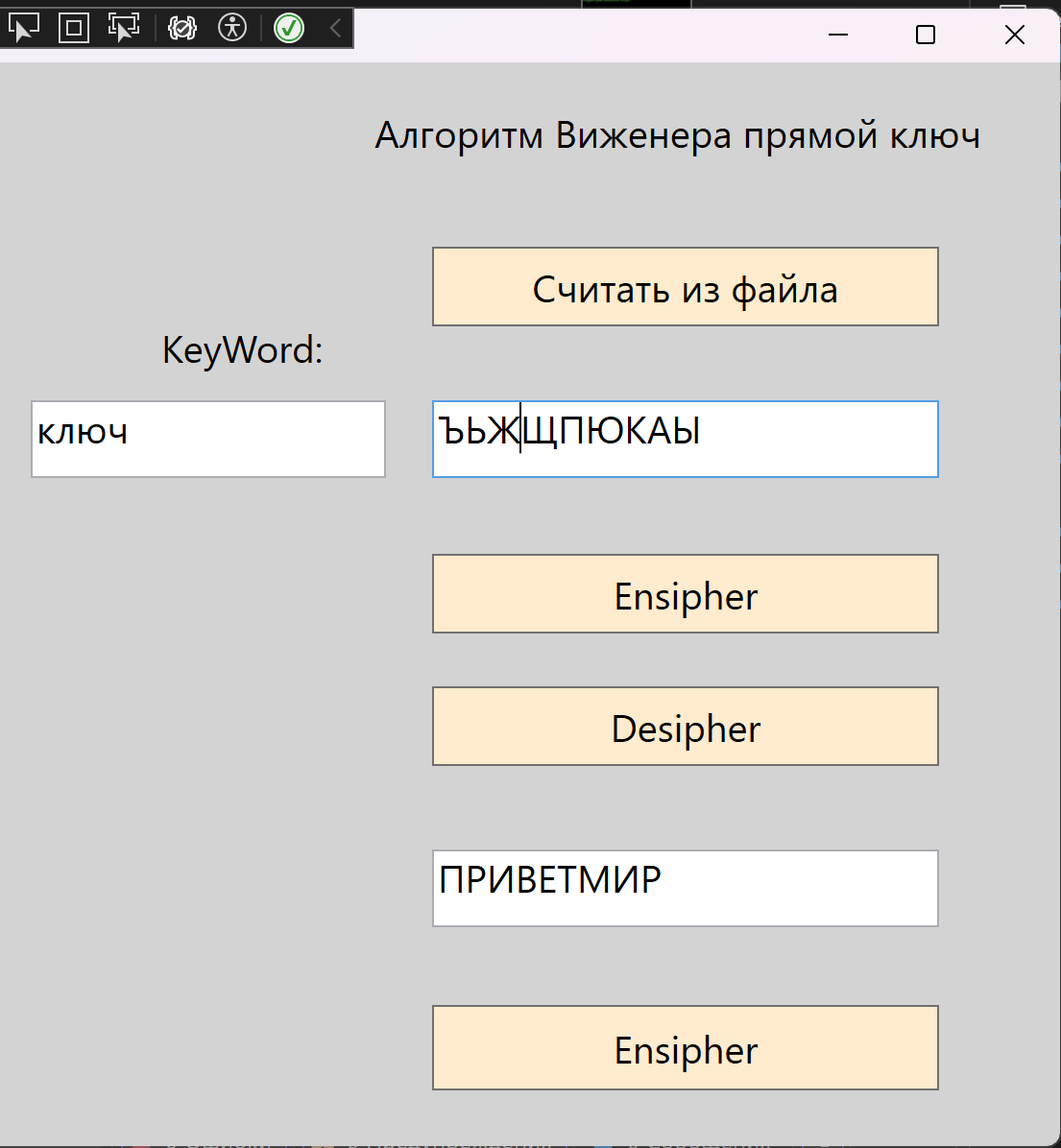
Зашифрованный текст:

ЪЬЖЩПЮКАЫ

Результат работы программы:



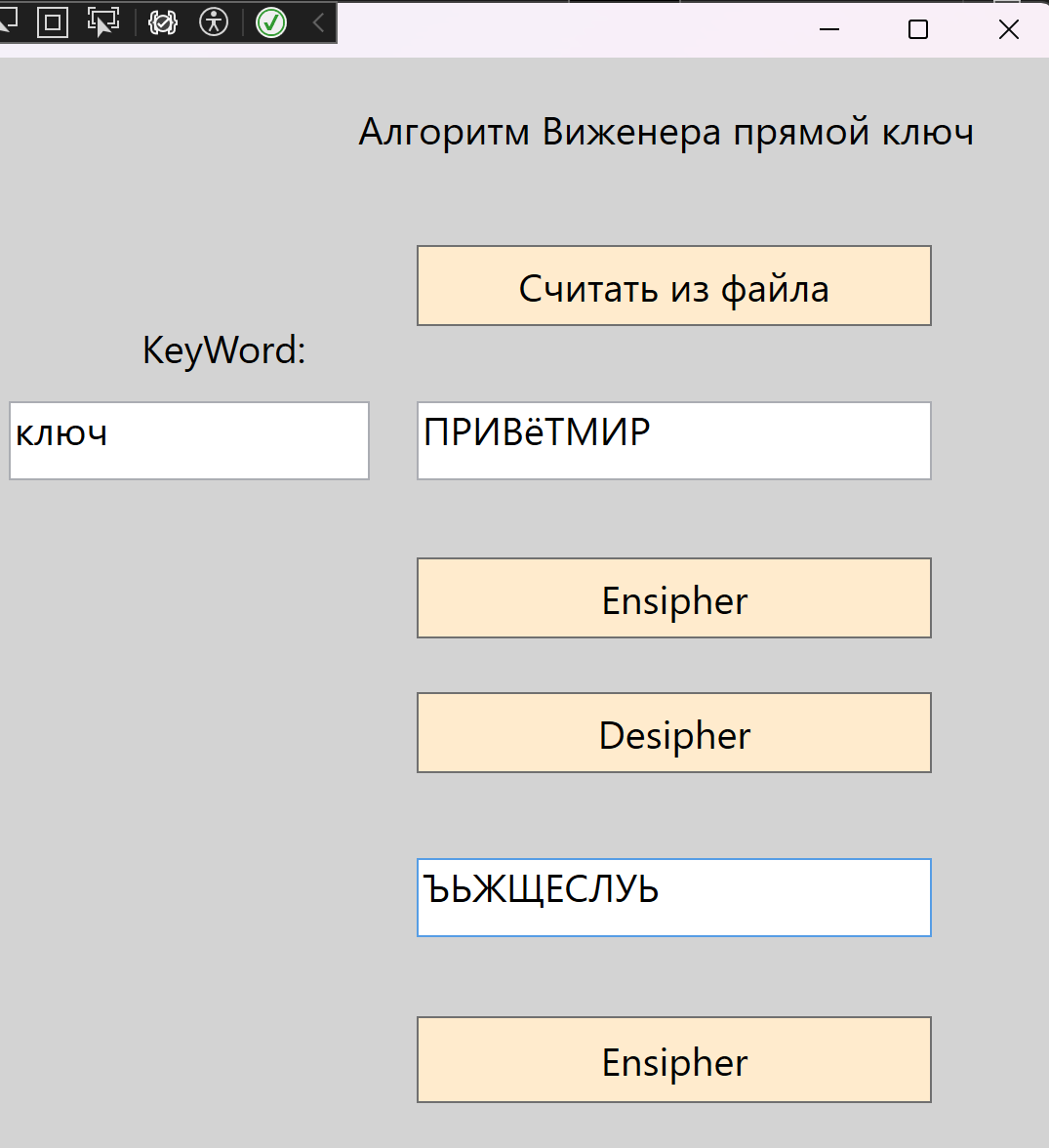
Пример шифрования



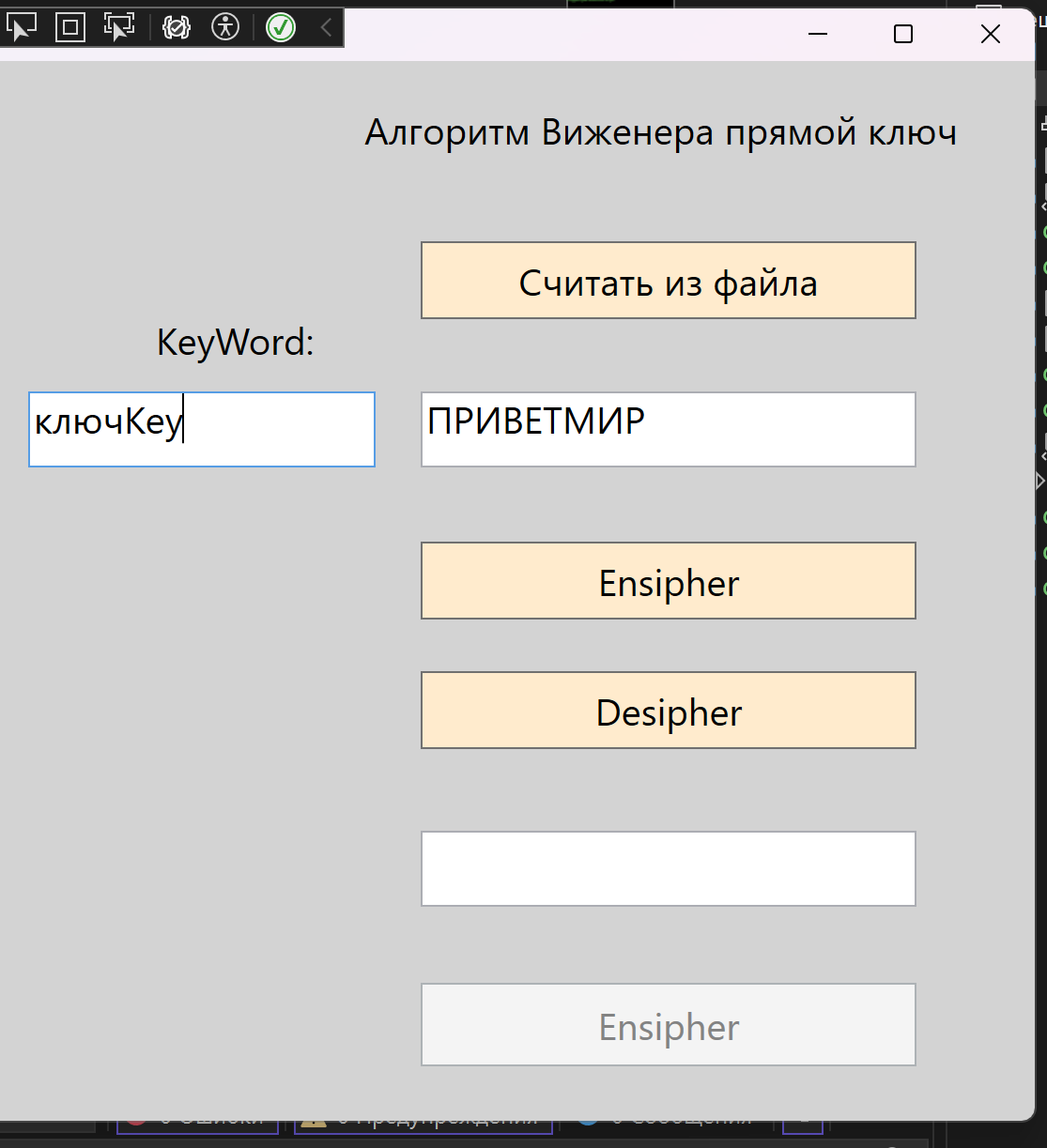
Пример дешифровки

*Ломаем на валидных данных:*

Все вышеизложенное проделываем для фразы, содержащей букву ё.



*Ломаем на не валидных данных:*

**