Министерство образования Республики Беларусь

Учреждение образования

БелорусскиЙ государственный университет

информатики и радиоэлектроники

Факультет компьютерных систем и сетей

Кафедра программного обеспечения информационных технологий

|  |
| --- |
|  |
|  |

ОТЧЕТ

по лабораторной работе

на тему:

ПРОСТЕЙШИЕ АЛГОРИТМЫ ШИФРОВАНИЯ

|  |  |  |
| --- | --- | --- |
| Выполнил  Студент гр. 351001 |  | Р.С. Головко |
| Проверил |  | С.В. Болтак |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

Минск, 2025

**Вариант 8**

**Задание**:

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

- **Метод децимаций** текст на русском языке;

- алгоритм **Виженера, самогенерирующийся 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.

Таблица алфавита с индексами для обоих алгоритмов:

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

|а |б |в |г |д |е |ё |ж |з |и |й |к |л |м |н |о |п |

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

|0 |1 |2 |3 |4 |5 |6 |7 |8 |9 |10|11|12|13|14|15|16|

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

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

|р |с |т |у |ф |х |ц |ч |ш |щ |ъ |ы |ь |э |ю |я |--|

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

|17|18|19|20|21|22|23|24|25|26|27|28|29|30|31|32|--|

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

**Тесты:**

**Метод децимаций:**

**Тест 1**

Текст: Буква ё (после запуска преобразуется в “букваё”)

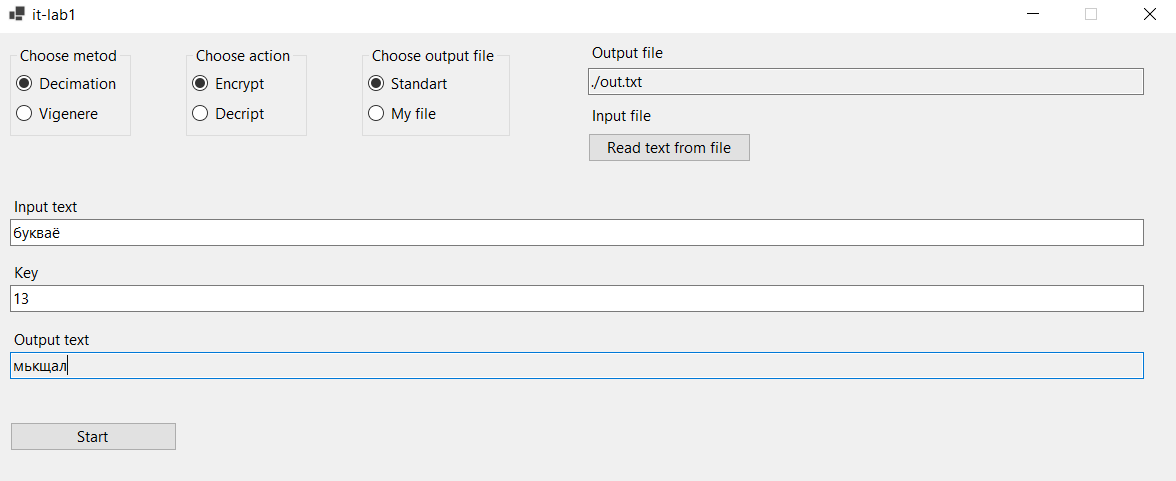
Ключ: 1ключ3 (после запуска преобразуется в “13”)

Операция: шифрование

У -> Ь

(20 (У) \* 13) % 33 = 29 (Ь)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Б - 1 | У - 20 | К - 11 | В - 2 | А - 0 | ё - 6 |
| М - 13 | Ь - 29 | К - 11 | Щ - 26 | А - 0 | Л - 12 |

****

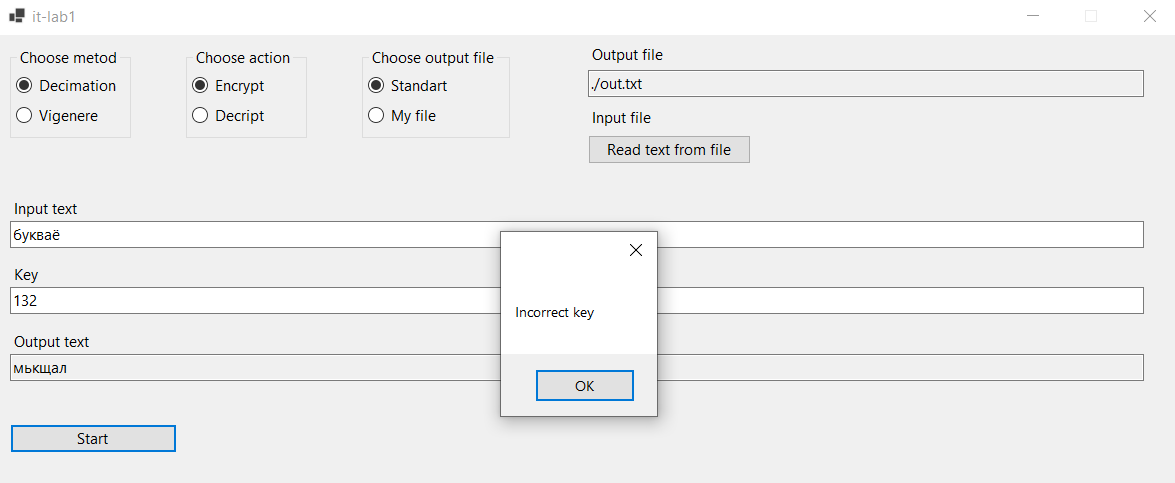
**Тест 2**

Текст: букваё

Ключ: 132

Операция: Шифрование

Ошибка ключа



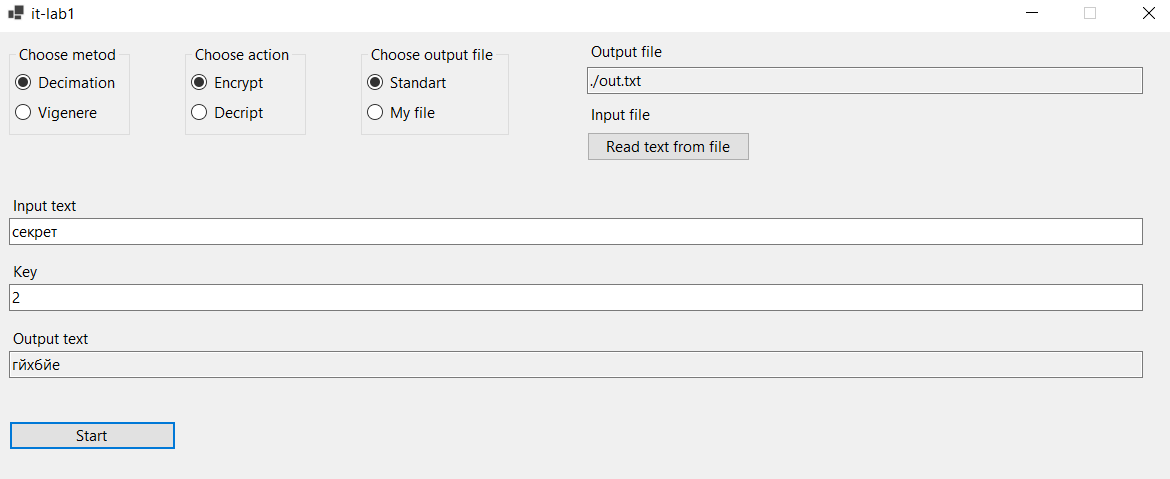
**Тест 3**

Текст: секрет

Ключ: -2 (после запуска преобразуется в “2”)

Операция: Шифрование

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| С - 18 | Е - 5 | К - 11 | Р - 17 | Е - 5 | Т - 19 |
| Г - 3 | Й - 10 | Х – 22 | Б - 1 | Й - 10 | Е - 5 |



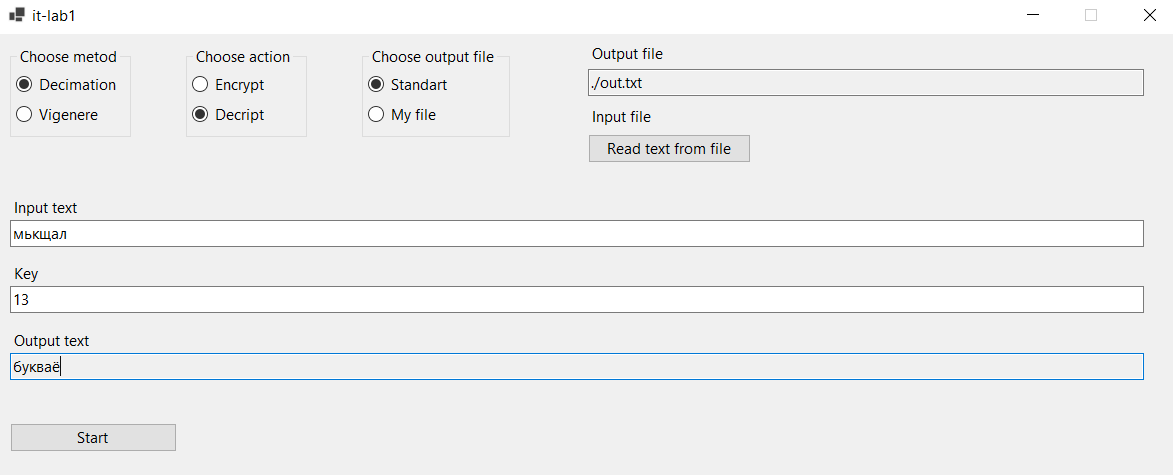
**Тест 4**

Текст: гйхбйе

Ключ: 2

Операция: Дешифрование

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Г - 3 | Й - 10 | Х – 22 | Б - 1 | Й - 10 | Е - 5 |
| С - 18 | Е - 5 | К - 11 | Р - 17 | Е - 5 | Т - 19 |



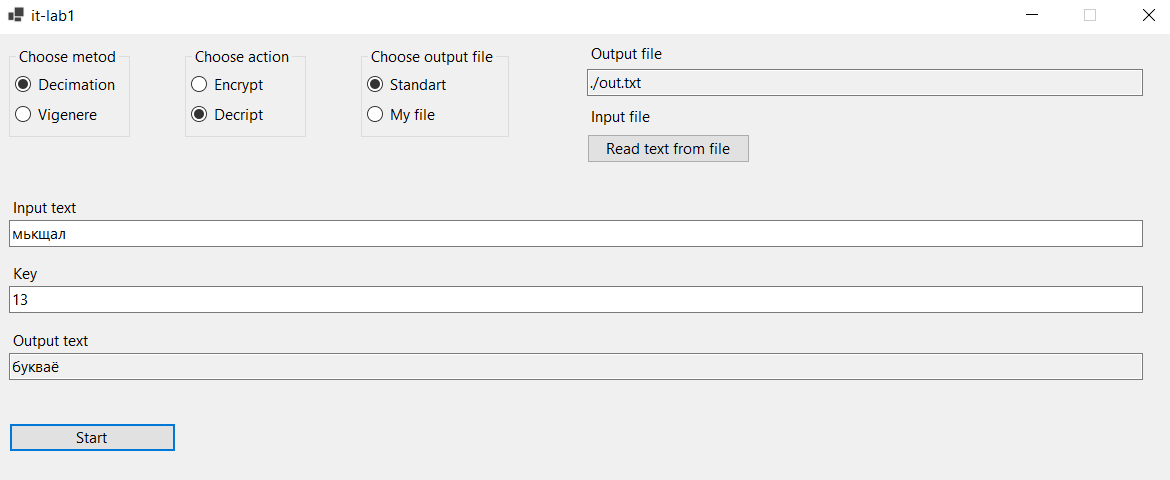
**Тест 5**

Текст: мькщал

Ключ: 13

Операция: дешифрование

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| М - 13 | Ь - 29 | К - 11 | Щ - 26 | А - 0 | Л - 12 |
| Б - 1 | У - 20 | К - 11 | В - 2 | А - 0 | ё - 6 |



**Метод Виженера**

Таблица для шифрования

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| / | 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 |

**Тест 1**

Текст: Виженер с буквой ё

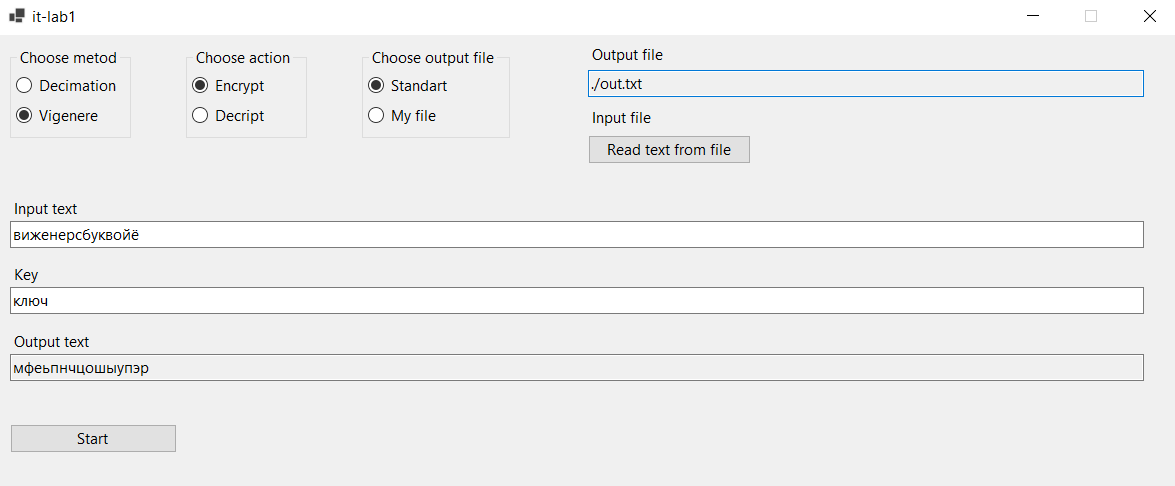
Ключ: ключ

Операция: шифрование

В -> К

(2 (В) + 11 (К)) % 33 = 13 (М)

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| в | и | ж | е | н | е | р | с | б | у | к | в | о | й | ё |
| к | л | ю | ч | в | и | ж | е | н | е | р | с | б | у | к |
| м | ф | е | ь | п | н | ч | ц | о | ш | ы | у | п | э | р |



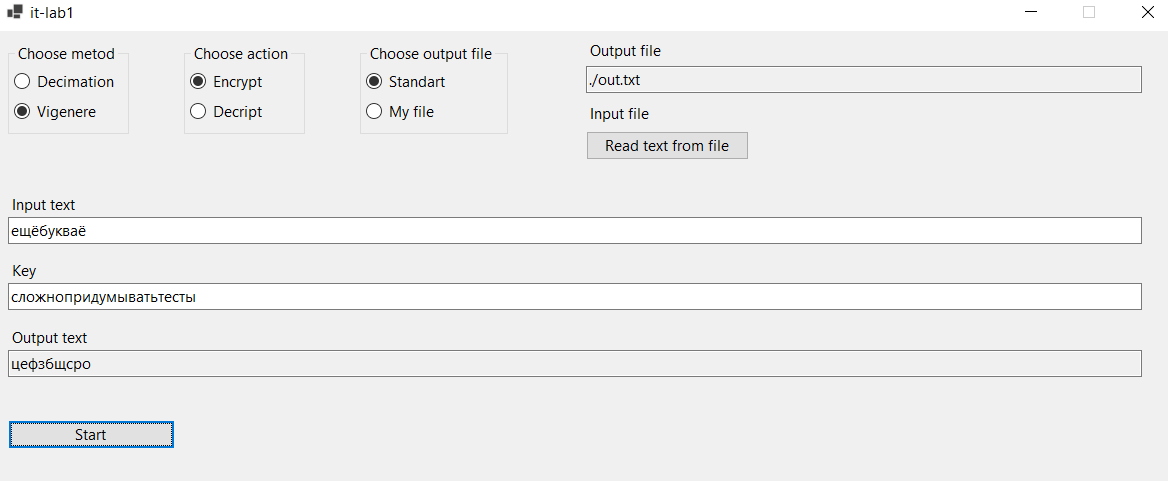
**Тест 2**

Текст: ещё буква ё

Ключ: сложно придумывать тесты

Операция: шифрование

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| е | щ | ё | б | у | к | в | а | ё |
| с | л | о | ж | н | о | п | р | и |
| ц | е | ф | з | б | щ | с | р | о |



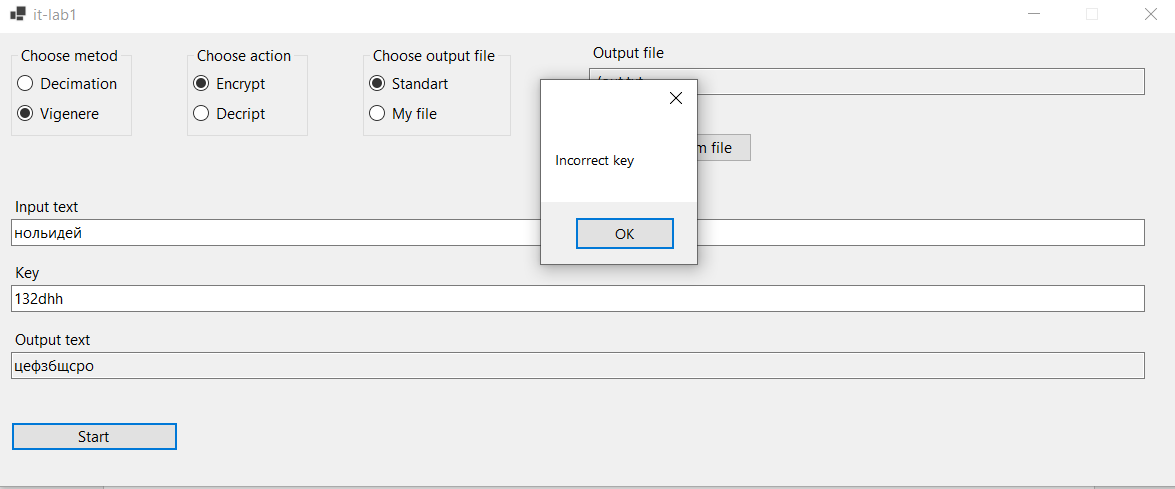
**Тест 3**

Текст: ноль идей

Ключ: 132dhh

Операция: шифрование

Ошибка ключа



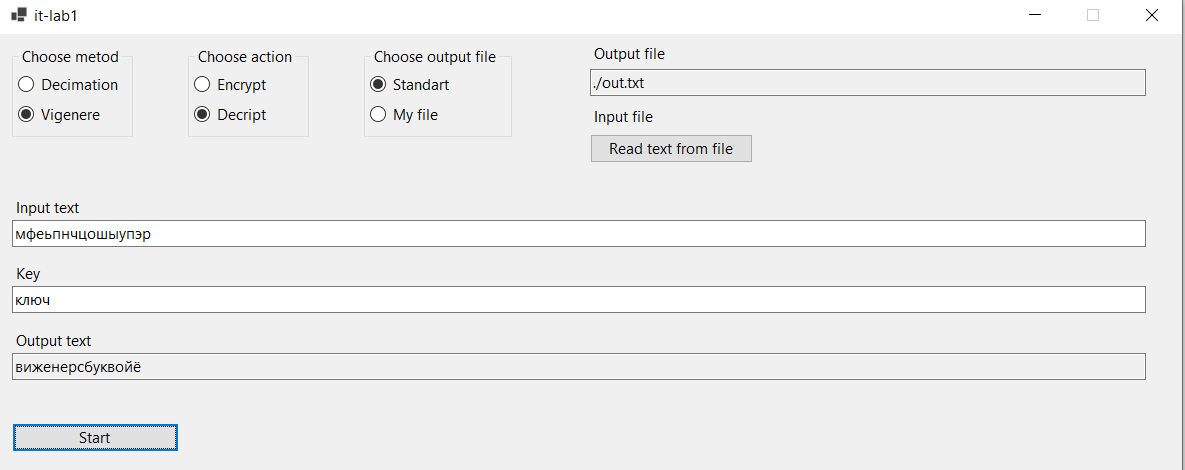
**Тест 4**

Текст: мфеьпнчцошыупэр

Ключ: к2л1юч (преобразуется в “ключ”)

Операция: дешифрование

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| м | ф | е | ь | п | н | ч | ц | о | ш | ы | у | п | э | р |
| к | л | ю | ч | в | и | ж | е | н | е | р | с | б | у | к |
| в | и | ж | е | н | е | р | с | б | у | к | в | о | й | ё |



**Тест 5**

Текст: цефзбщсро

Ключ: сложно придумывать тесты

Операция: дешифрование

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ц | е | ф | з | б | щ | с | р | о |
| с | л | о | ж | н | о | п | р | и |
| е | щ | ё | б | у | к | в | а | ё |

