УО «Белорусский государственный университет информатики и радиоэлектроники»

Кафедра ПОИТ

Отчет по лабораторной работе №1

по предмету «Теория информации»

Выполнил:

Шиманчук А.О.

гр. 351001

Проверила:

Болтак С.В.

Минск 2025

Вариант 5

Шифр Виженера, самогенерирующийся ключ, текст на русском языке

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **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:**

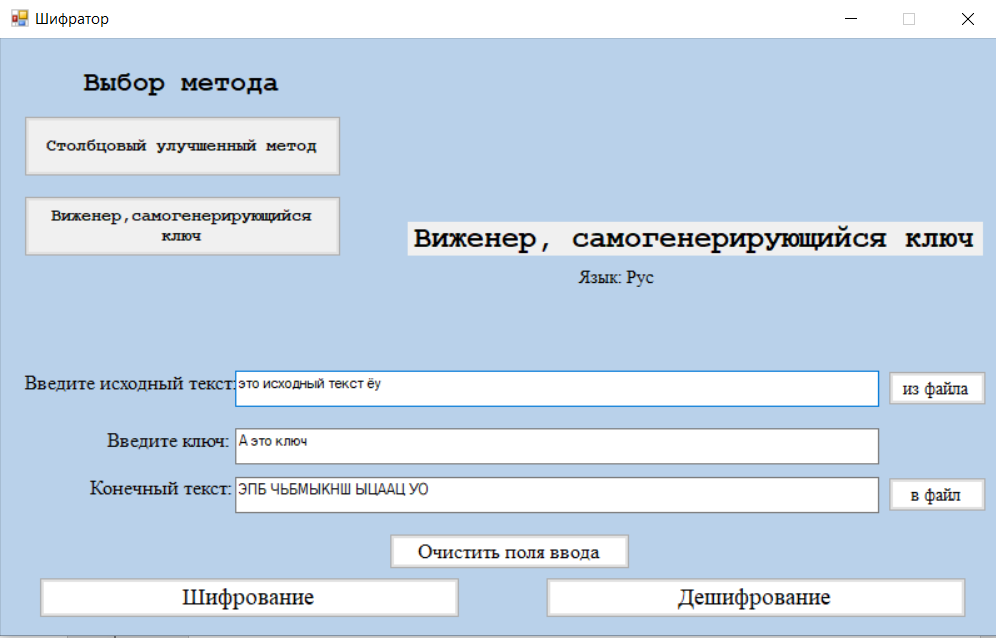
**Дымовое тестирование**

Исходный текст: “это исходный текст ёу”

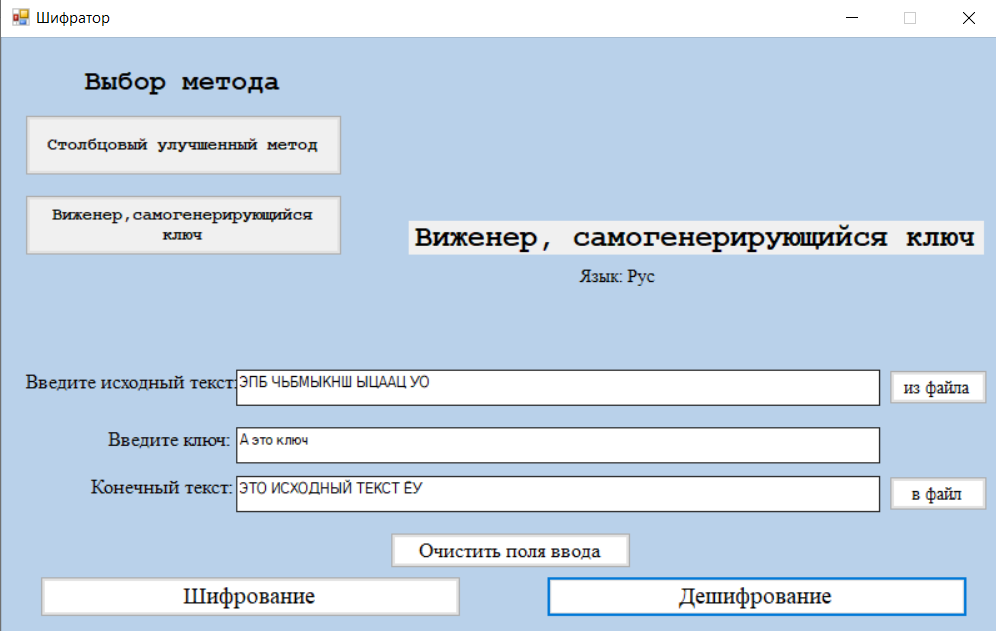
Ключ: “А это ключ”

Зашифрованный текст: “ ЭПБ ЧЬБМЫКНШ ЫЦААЦ УО”

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Э | Т | О | И | С | Х | О | Д | Н | Ы | Й | Т | Е | К | С | Т | Ё | У |
| А | Э | Т | О | К | Л | Ю | Ч | Э | Т | О | И | С | Х | О | Д | Н | Ы |
| Э | П | Б | Ч | Ь | Б | М | Ы | К | Н | Ш | Ы | Ц | А | А | Ц | У | О |



Обратный тест:



В результате обратного теста с дешифрованием конечный текст корректен.

**Тест 2:**

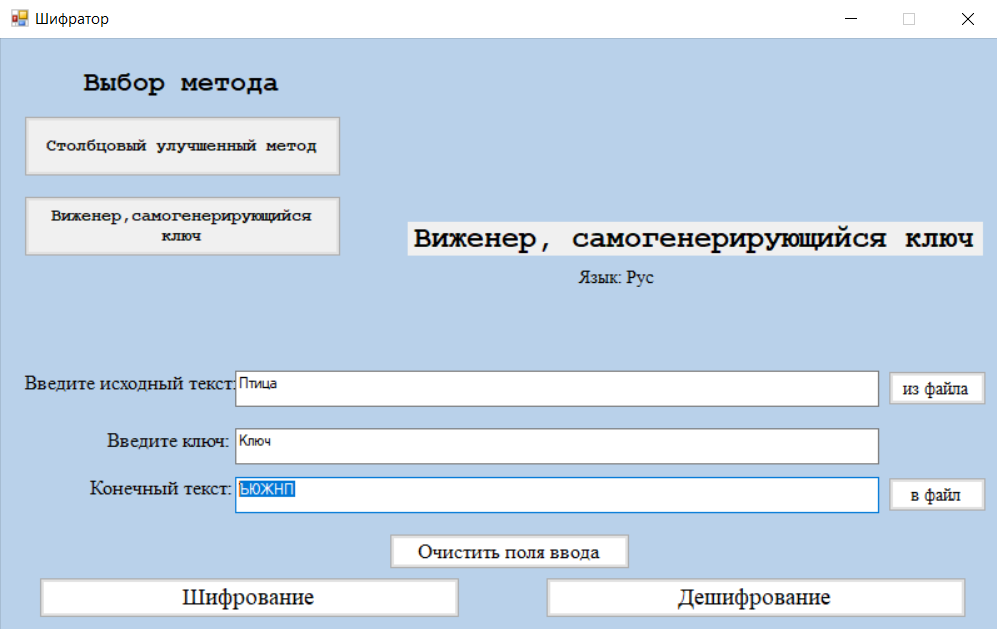
**Тестирование на валидных данных**

Исходный текст: ”Птица ”

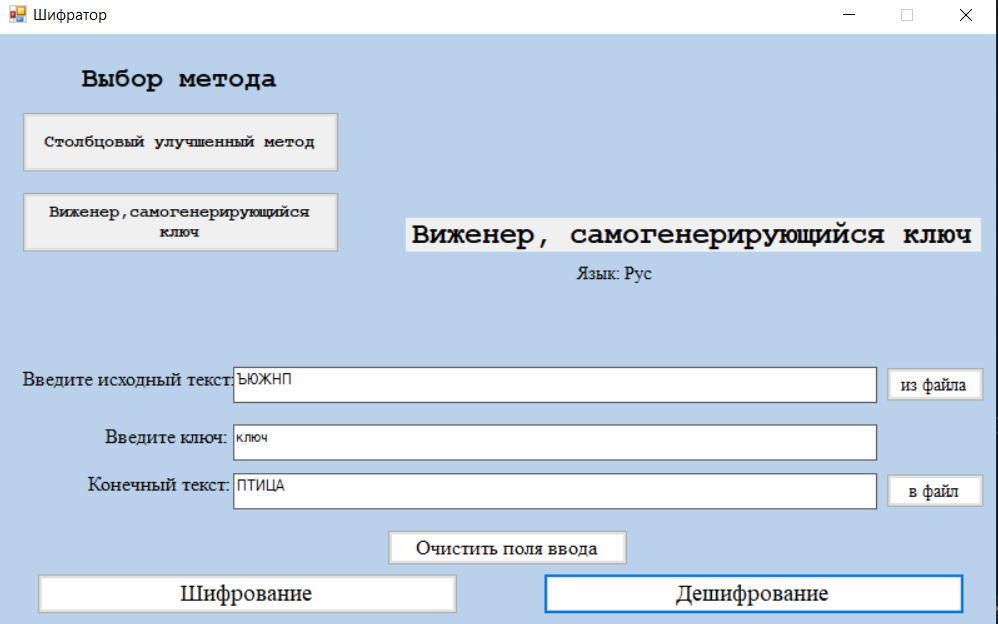
Ключ: “Клюв”

Зашифрованный текст: “ЪЮЖНП”

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| П | Т | И | Ц | А |
| К | Л | Ю | В | П |
| Ъ | Ю | Ж | Н | П |



Обратный тест:

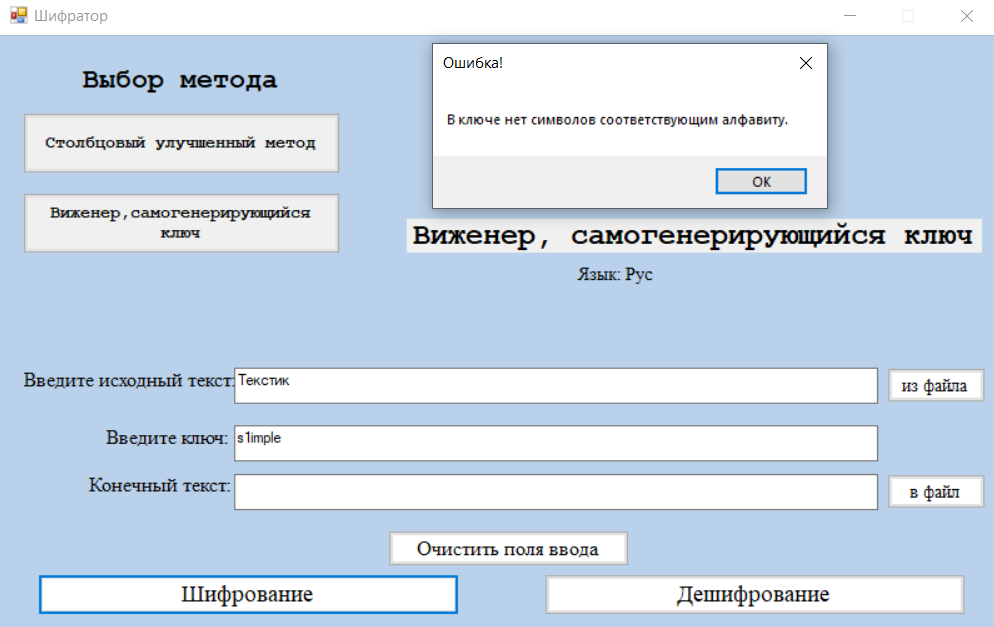


**Tест 3:**

**Тестирование на не валидных данных**

Исходный текст: ”Текстик”

Ключ: “s1mple”



**Столбцовый метод улучшенный, текст на английском языке**

**Тест 1:**

**Дымовое тестирование**

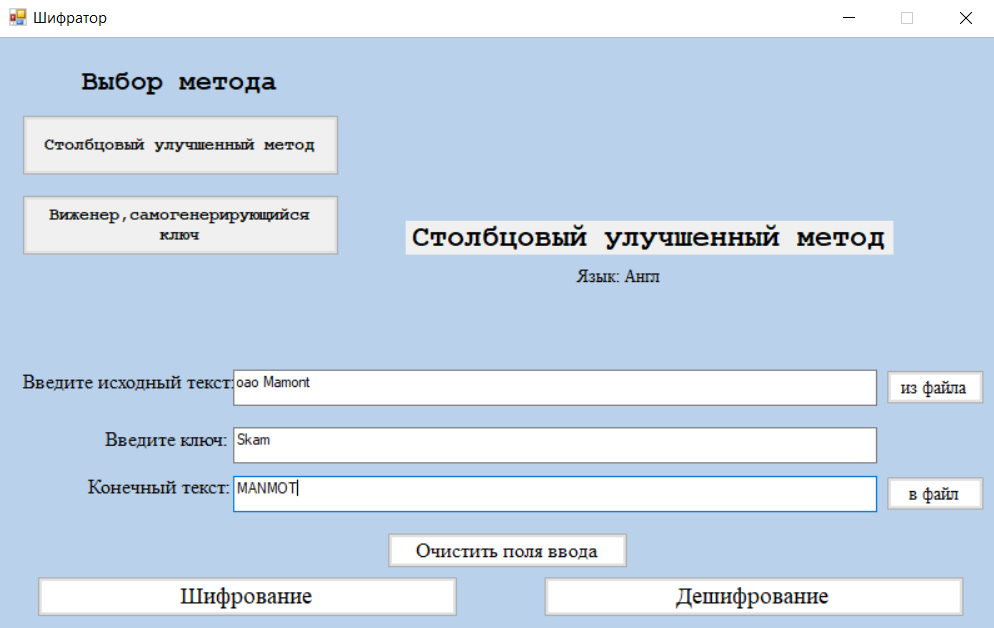
Исходный текст: “оао Mamont”

Ключ: “skam”

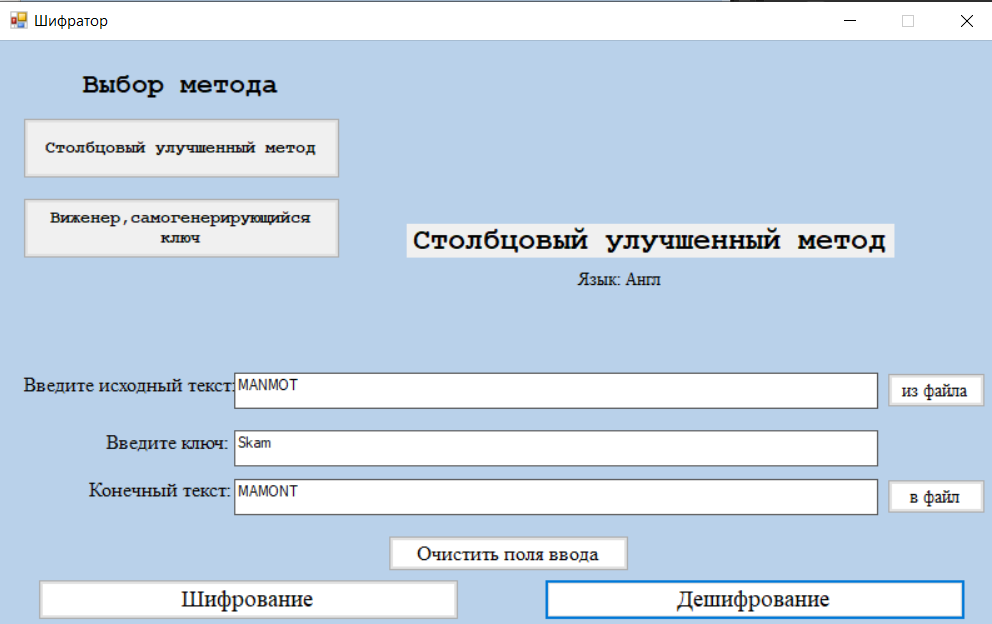
Зашифрованный текст: “ MANMOT”

|  |  |  |  |
| --- | --- | --- | --- |
| S | K | A | M |
| 4 | 2 | 1 | 3 |
| M | A | M |  |
| O | N |  |  |
| T |  |  |  |

Шифрование:



Дешифрование:



**Тест 2:**

**Тестирование на валидных данных**

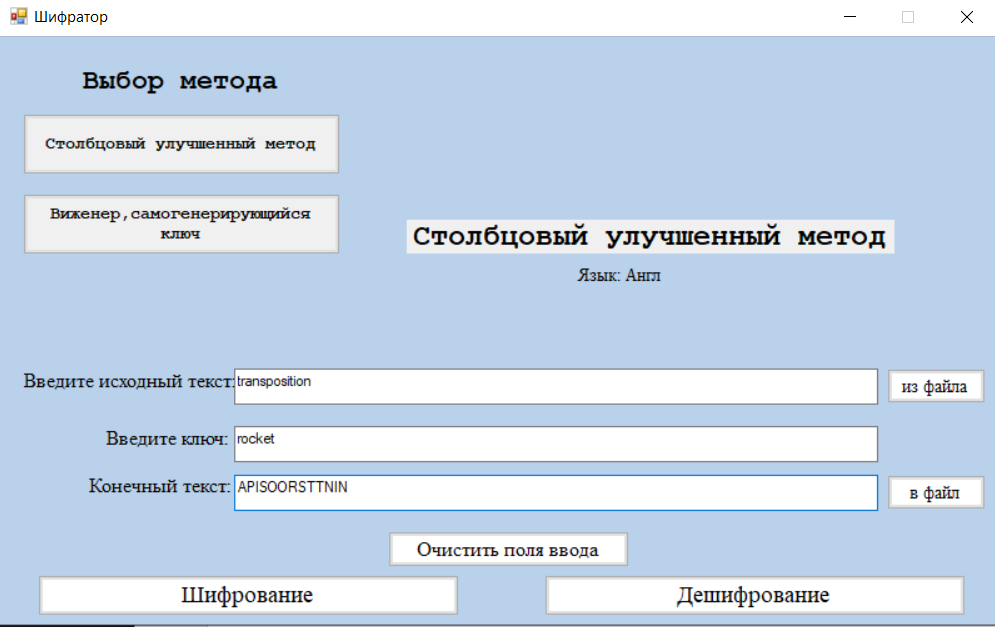
Исходный текст: ”transposition ”

Ключ: “rocket”

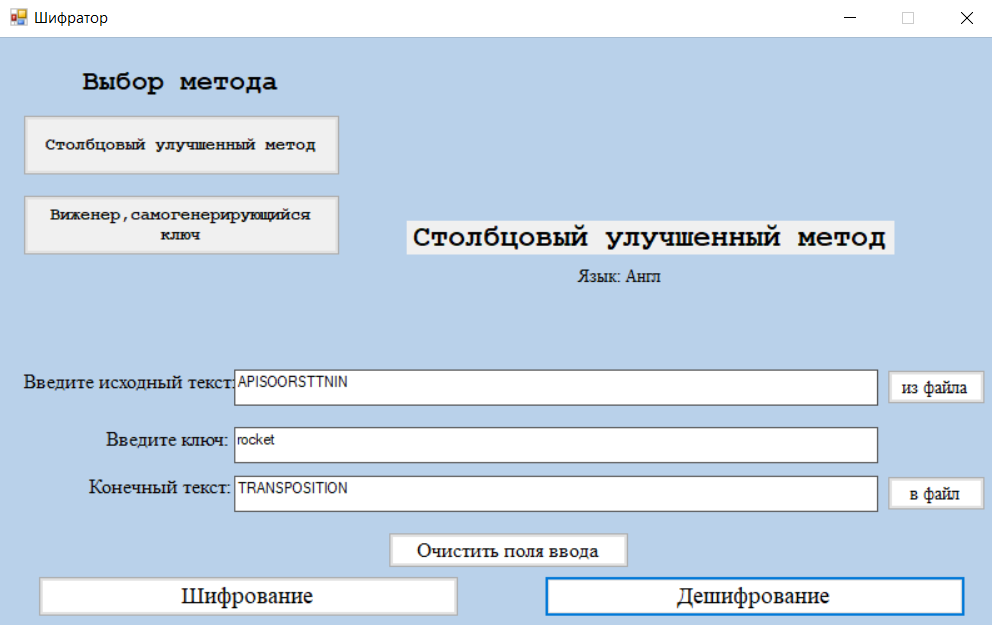
Зашифрованный текст: “ APISOORSTTNIN ”

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| R | O | C | K | E | T |
| 5 | 4 | 1 | 3 | 2 | 6 |
| T | R | A |  |  |  |
| N | S | P | O | S |  |
| I | T | I | O |  |  |
| N |  |  |  |  |  |

Шифрование:



Дешифрование:



**Тест 3:**

**Тестирование не на валидных данных**

Исходный текст: ”Text ”

Ключ: “ключ”

