Министерство образования Республики Беларусь

Учреждение образования

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

Факультет компьютерных систем и сетей

Кафедра программного обеспечения информационных технологий

Теория информации

ОТЧЕТ

по лабораторной работе 1

Вариант 10

|  |  |
| --- | --- |
| Выполнил  Студент гр. 351002 | Филипенко А. С. |
| Проверил | Болтак С. В. |

Минск 2025

Столбцовый метод с двумя ключевыми словами

1. Дымовое тестирование

Тест 1

**Исходный текст:** пло213145хой приsihfiu123мер

д21ля тест...а

**Полученный шифрующий текст:** ПЛОХОЙ ПРИМЕР ДЛЯ ТЕСТА

**Ключ 1:** такие ключи

**Ключ 2:** получились

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Т | А | К | И | Е | К | Л | Ю | Ч | И |
| 8 | 1 | 5 | 3 | 2 | 6 | 7 | 10 | 9 | 4 |
| П | Л | О | Х | О | Й | П | Р | И | М |
| Е | Р | Д | Л | Я | Т | Е | С | Т | А |

**Шифротекст:** ЛРОЯХЛМАОДЙТПЕПЕИТРС

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| П | О | Л | У | Ч | И | Л | И | С | Ь |
| 6 | 5 | 3 | 8 | 9 | 1 | 4 | 2 | 7 | 10 |
| Л | Р | О | Я | Х | Л | М | А | О | Д |
| Й | Т | П | Е | П | Е | И | Т | Р | С |

**Шифротекст:** ЛЕАТОПМИРТЛЙОРЯЕХПДС

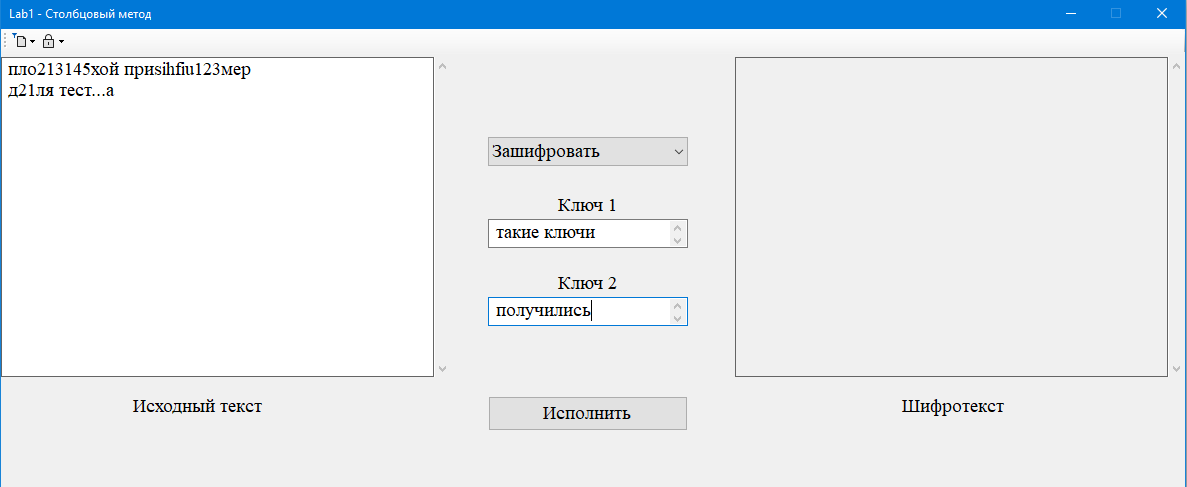


Рис. 1 – Шифрование (до выполнения)

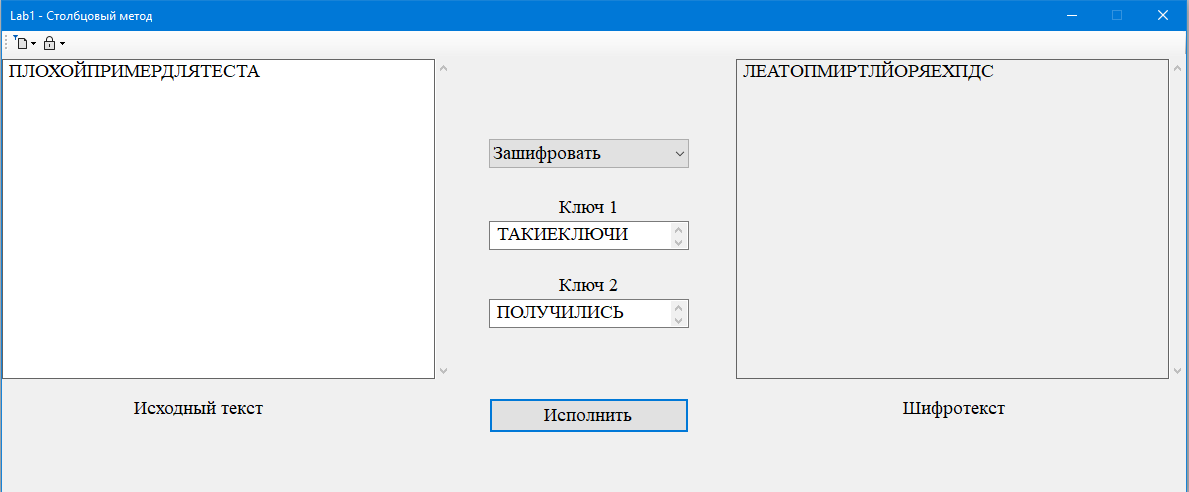


Рис. 2 – Шифрование (после выполнения)

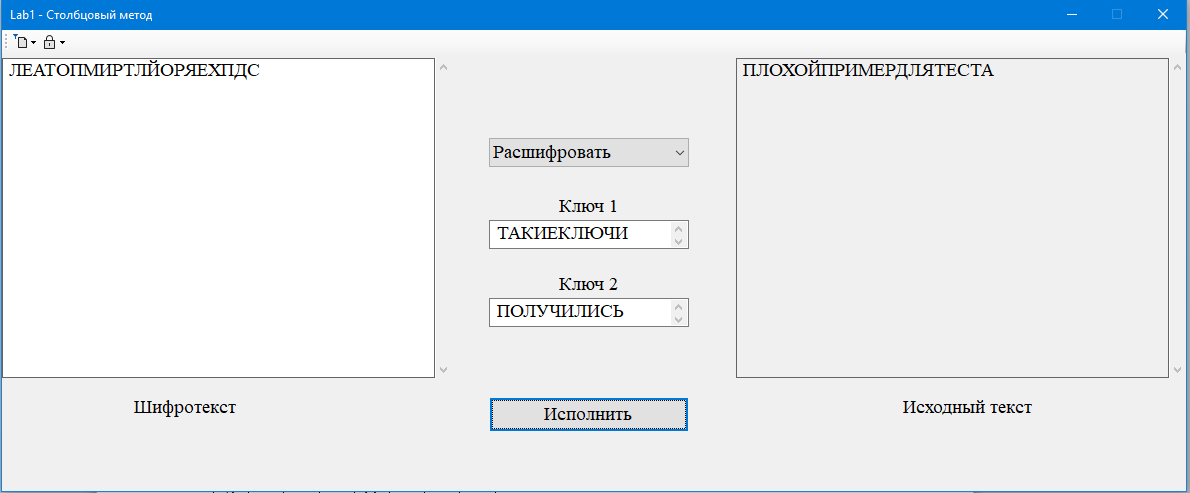


Рис. 3 – Дешифрование

Тест 2

**Исходный текст:** ну..213та000;FAFsкой п римGGGер

**Полученный шифрующий текст:** НУ ТАКОЙ ПРИМЕР

**Ключ 1:** такой

**Ключ 2:** ключик

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Т | А | К | О | Й |
| 5 | 1 | 3 | 4 | 2 |
| Н | У | Т | А | К |
| О | Й | П | Р | И |
| М | Е | Р |  |  |

**Шифротекст:** УЙЕКИТПРАРНОМ

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| К | Л | Ю | Ч | И | К |
| 2 | 4 | 6 | 5 | 1 | 3 |
| У | Й | Е | К | И | Т |
| П | Р | А | Р | Н | О |
| М |  |  |  |  |  |

**Шифротекст:** ИНУПМТОЙРКРЕА

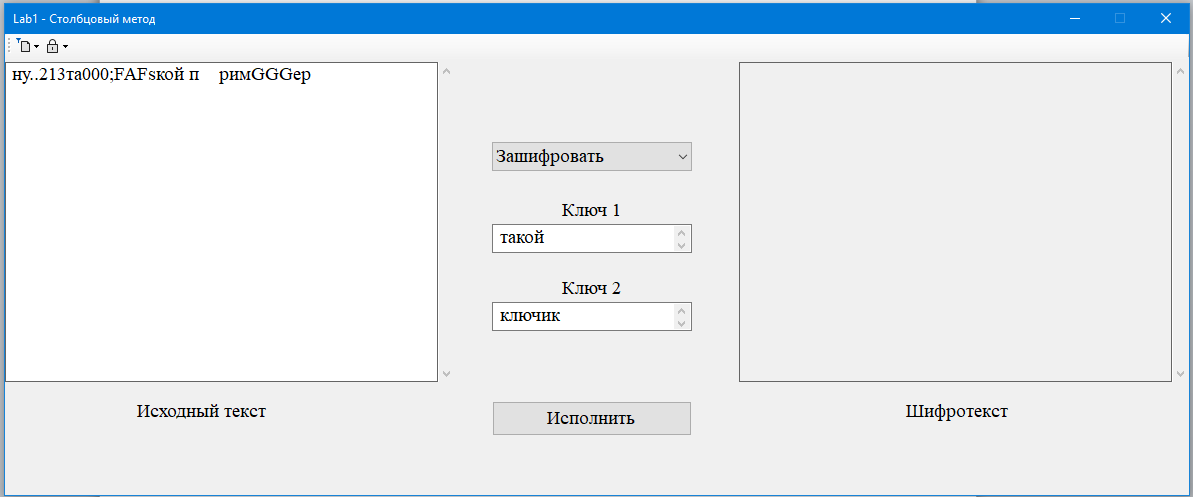


Рис. 4 – Шифрование (до выполнения)

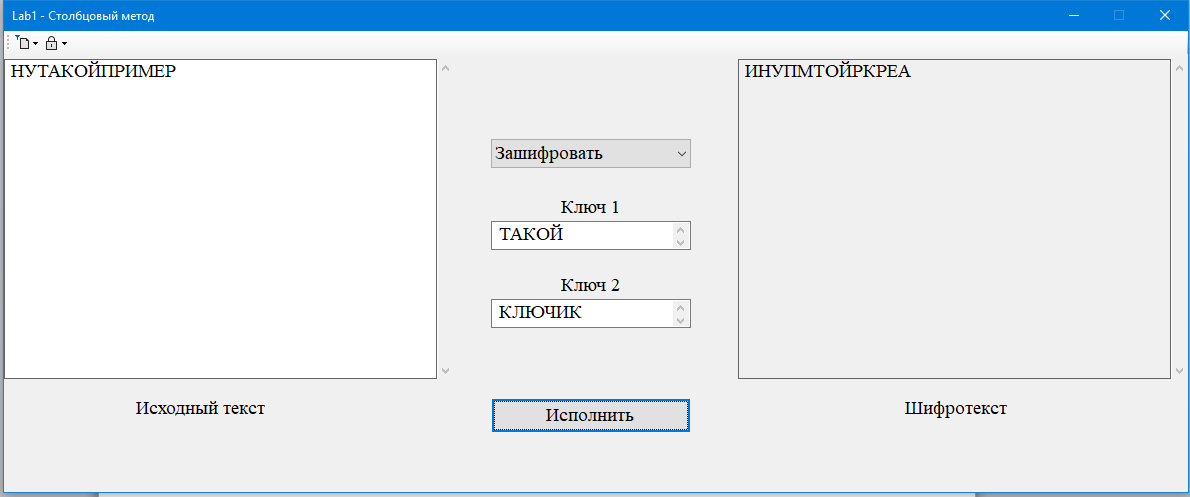


Рис. 5 – Шифрование (после выполнения)

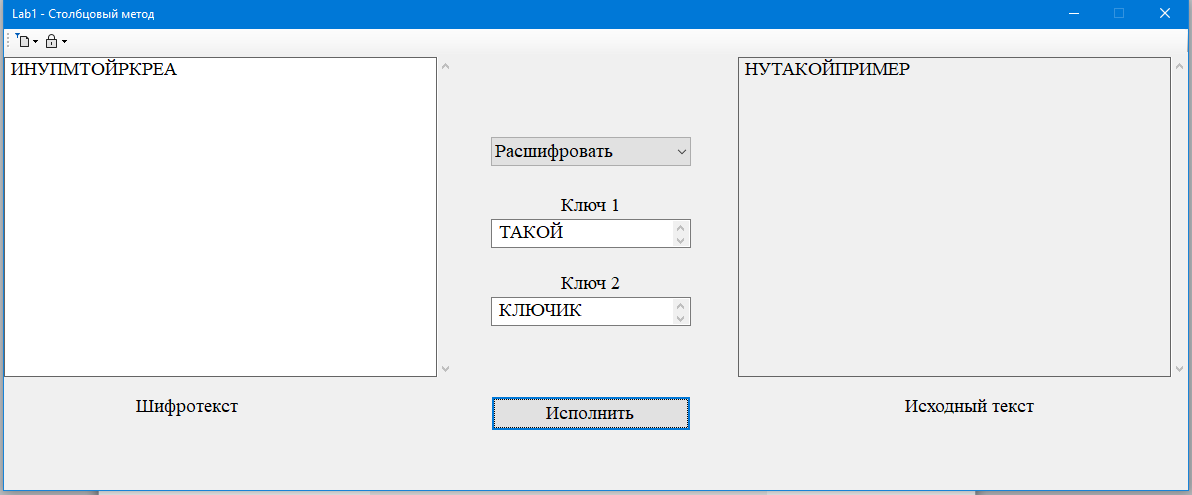


Рис. 6 – Дешифрование

2. Крайние значения ключа

Тест 3

**Исходный текст:** какой-то текст

**Полученный шифрующий текст:** КАКОЙ ТО ТЕКСТ

**Ключ 1:** ключ один

**Ключ 2:** сальто назад и вперед

**Шифротекст:** отсутствует

**Причина:** Ключ не может быть больше шифрующего текста, так как невозможна последующая расшифровка после шифрования.

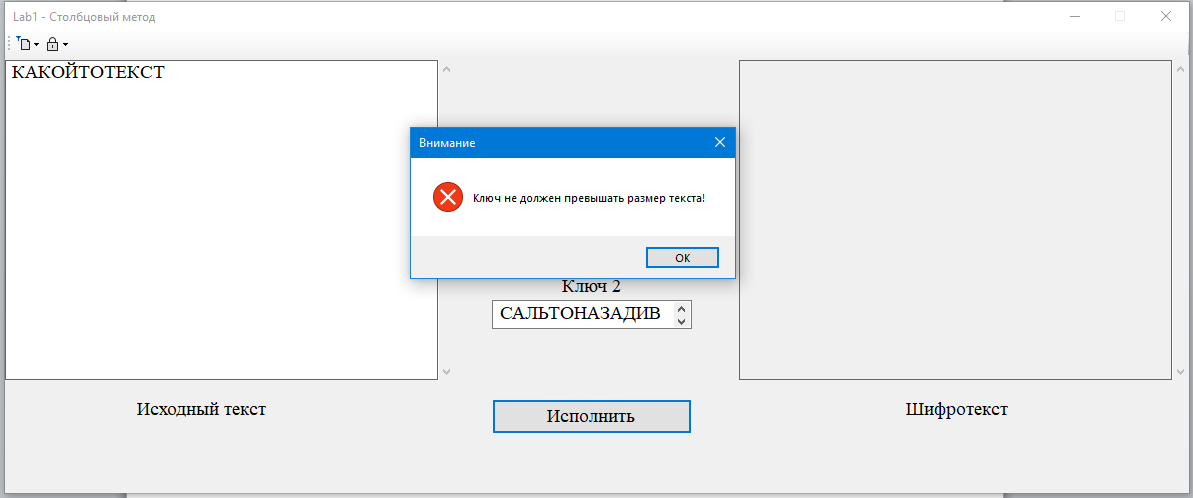


Рис. 7 – Попытка шифрования

Тест 4

**Исходный текст:** какой-то текст

**Полученный шифрующий текст:** КАКОЙ ТО ТЕКСТ

**Ключ 1:** о

**Ключ 2:** сальто

**Шифротекст:** отсутствует

**Причина:** Ключ не может состоять из 1 буквы, так как получится лишь 1 столбец в таблице.

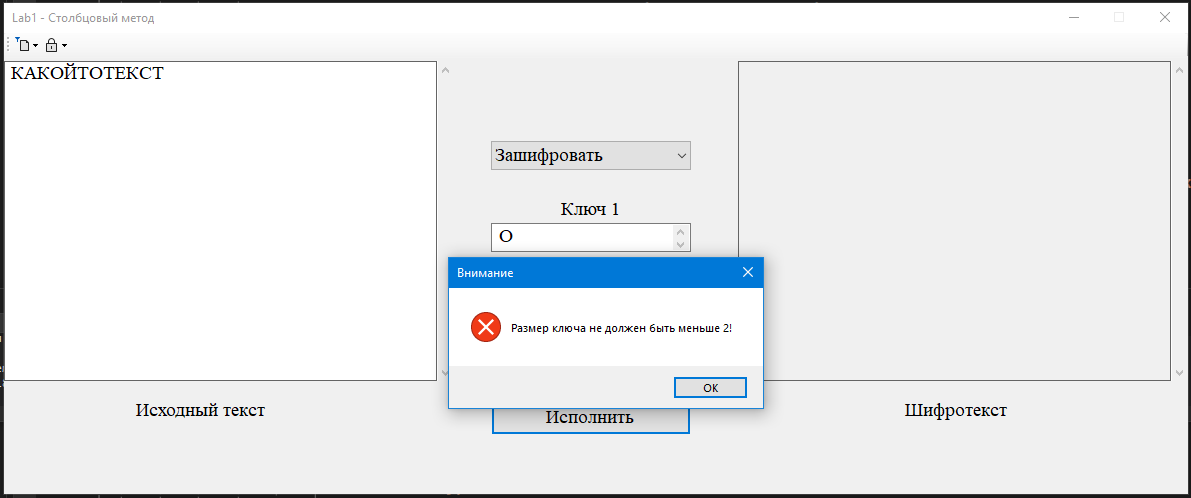


Рис. 8 – Попытка шифрования

3. Недопустимые значения для ключа

Тест 5

**Исходный текст:** бес12поSSдобJJJный-----====прим1231ерLLL

**Полученный шифрующий текст:** БЕСПОДОБНЫЙ ПРИМЕР

**Ключ 1:** класс....123ически й

**Ключ 2:** прим.ер.123чик

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| К | Л | А | С | С | И | Ч | Е | С | К | И | Й |
| 6 | 8 | 1 | 9 | 10 | 3 | 12 | 2 | 11 | 7 | 4 | 5 |
| Б | Е | С | П | О | Д | О | Б | Н | Ы | Й | П |
| Р | И | М | Е | Р |  |  |  |  |  |  |  |

**Шифротекст:** СМБДЙПБРЫЕИПЕОРНО

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| П | Р | И | М | Е | Р | Ч | И | К |
| 6 | 7 | 2 | 5 | 1 | 8 | 9 | 3 | 4 |
| С | М | Б | Д | Й | П | Б | Р | Ы |
| Е | И | П | Е | О | Р | Н | О |  |

**Шифротекст:** ЙОБПРОЫДЕСЕМИПРБН

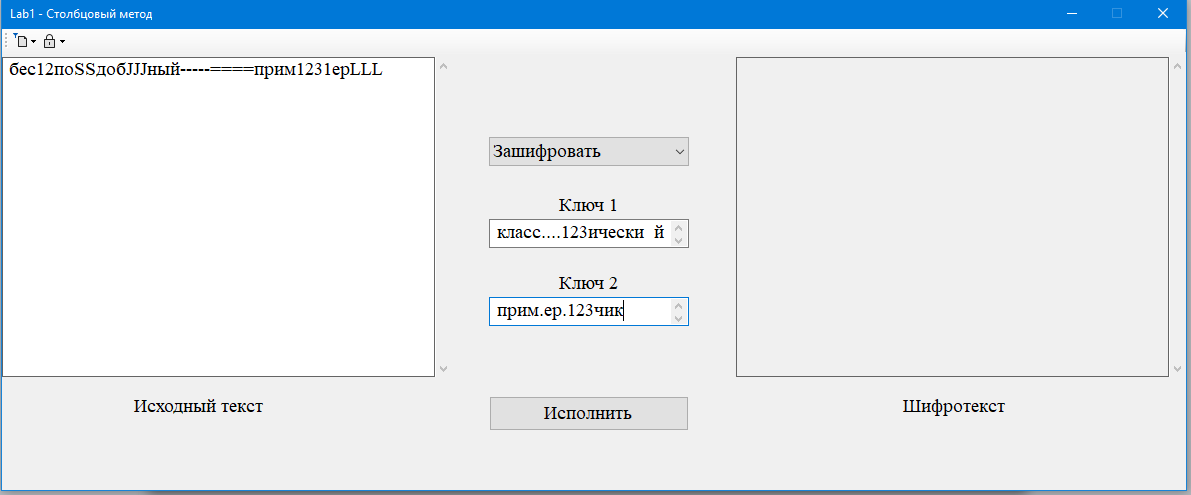


Рис. 9 – Шифрование (до выполнения)

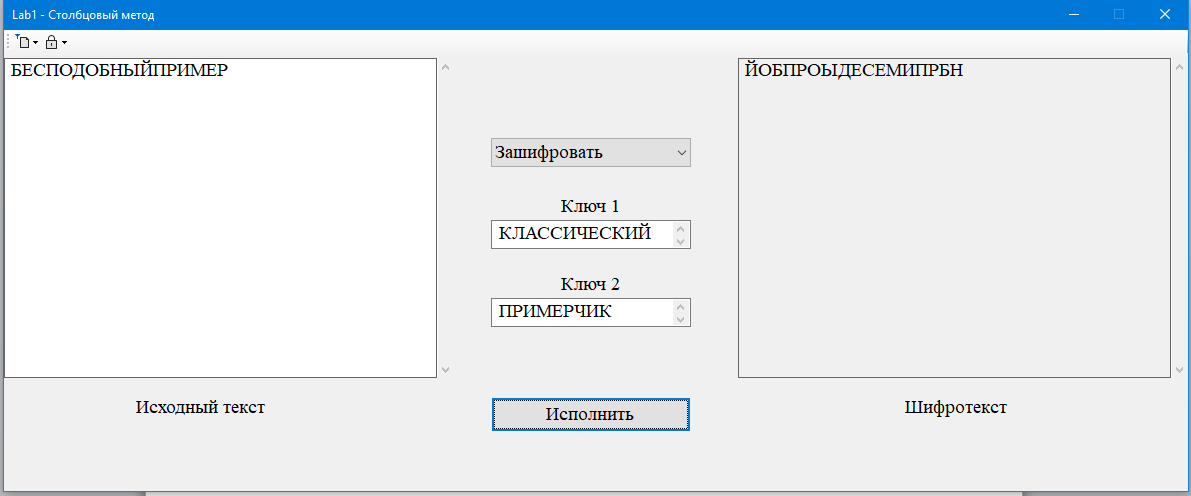


Рис. 10 – Шифрование (после выполнения)

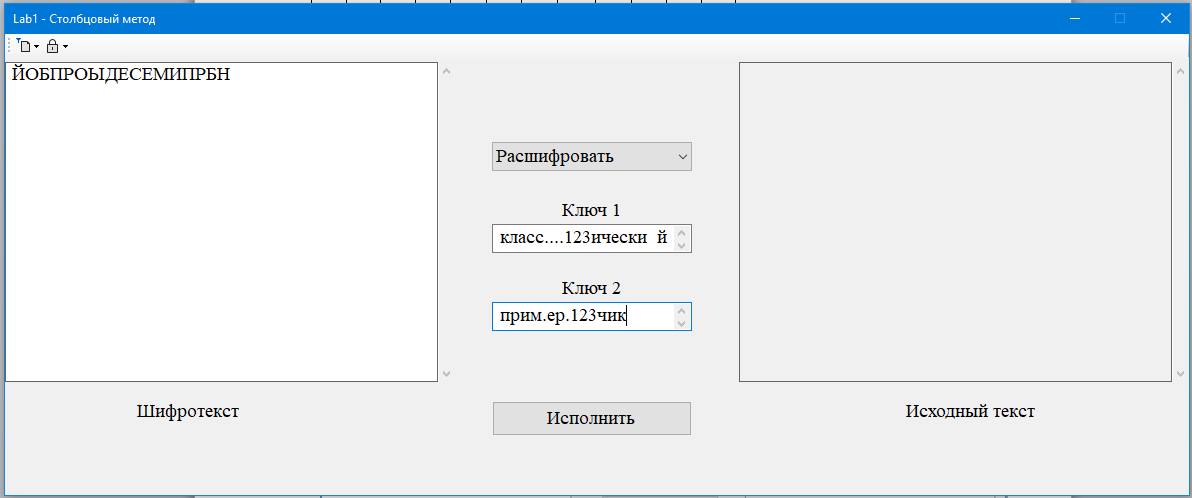


Рис. 11 – Дешифрование (до выполнения)

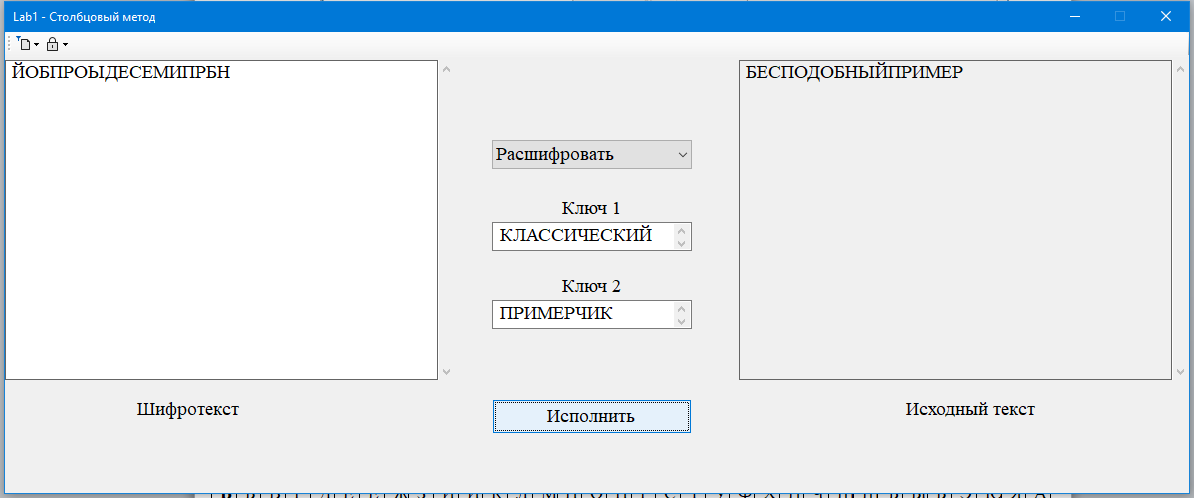


Рис. 11 – Дешифрование (после выполнения)

Шифр Виженера (самогенерирующийся ключ)

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **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 |

1. Дымовое тестирование

Тест 1

**Исходный текст:** три3333 градус..а сеGGGGверной широ т ы

**Полученный шифрующий текст:** ТРИ ГРАДУСА СЕВЕРНОЙ ШИРОТЫ

**Ключ:** география

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Т | Р | И | Г | Р | А | Д | У | С | А | С | Е | В | Е | Р | Н | О | Й | Ш | И | Р | О | Т | Ы |
| Г | Е | О | Г | Р | А | Ф | И | Я | Т | Р | И | Г | Р | А | Д | У | С | А | С | Е | В | Е | Р |

**Шифротекст:** ХХХЧЁБАШЬРТВНЕХРСВЫШЪХРЧЛ

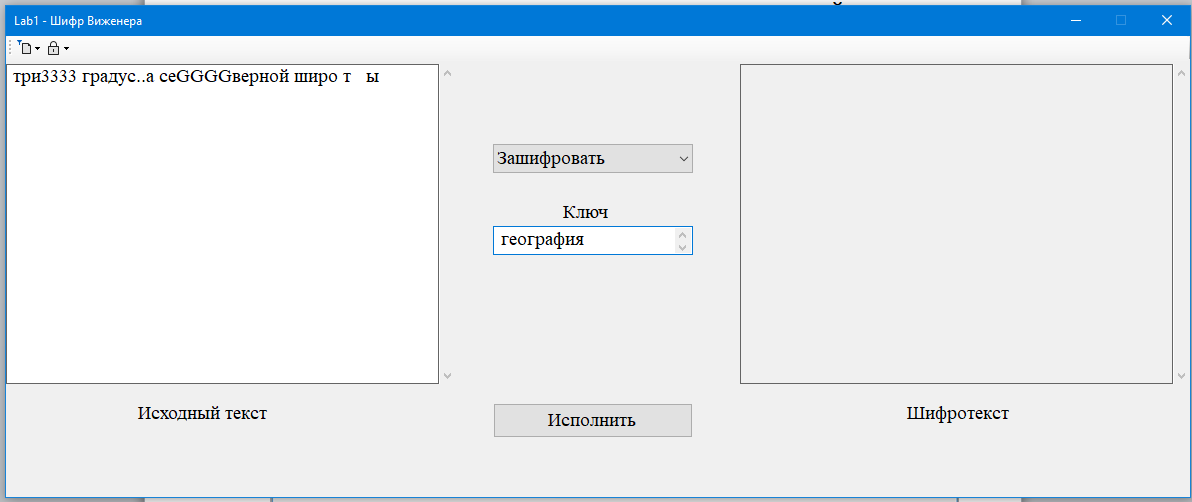
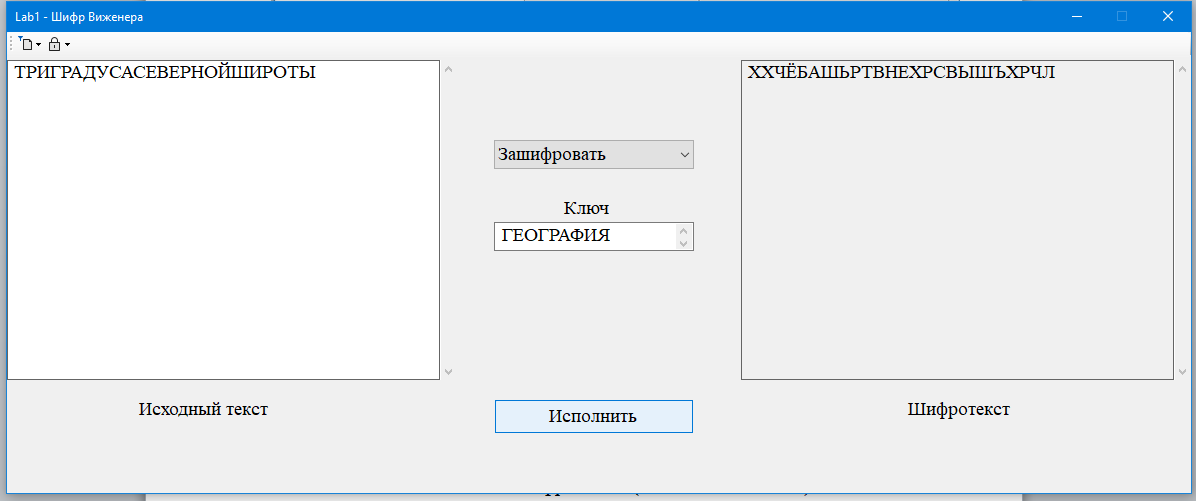


Рис. 12 – Шифрование (до выполениня)

 Рис. 13 – Шифрование (после выполениня)

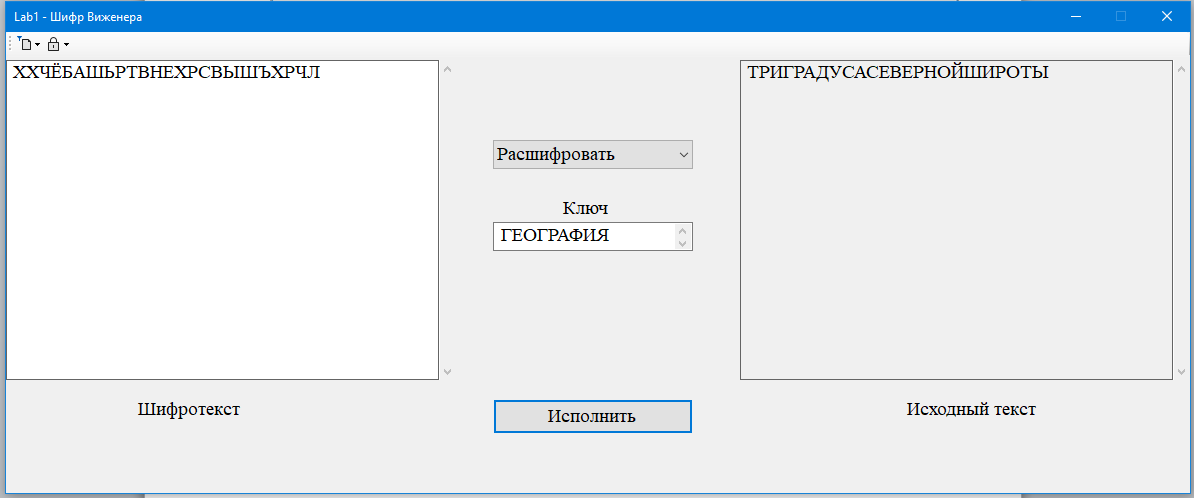


Рис. 14 – Дешифрование

2. Наличие буквы Ё

Тест 2

**Исходный текст:** очень грязная ёмкость

**Полученный шифрующий текст:** ОЧЕНЬ ГРЯЗНАЯ ЁМКОСТЬ

**Ключ:** ещё ключ

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| О | Ч | Е | Н | Ь | Г | Р | Я | З | Н | А | Я | Ё | М | К | О | С | Т | Ь |
| Е | Щ | Ё | К | Л | Ю | Ч | О | Ч | Е | Н | Ь | Г | Р | Я | З | Н | А | Я |

**Шифротекст:** УРКШЗБЗНЯТНЫИЭЙЦЯТЫ

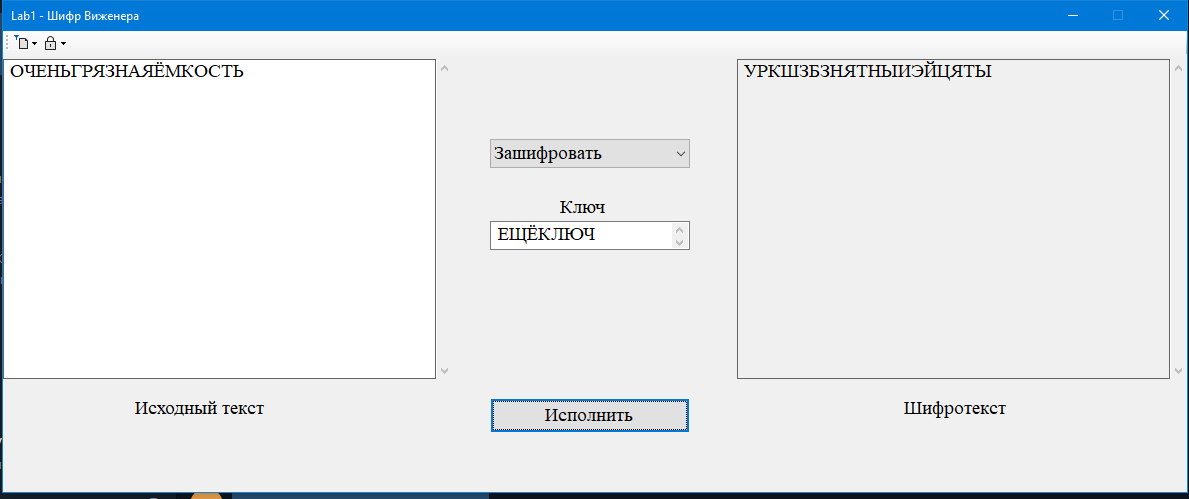


Рис. 15 – Шифрование

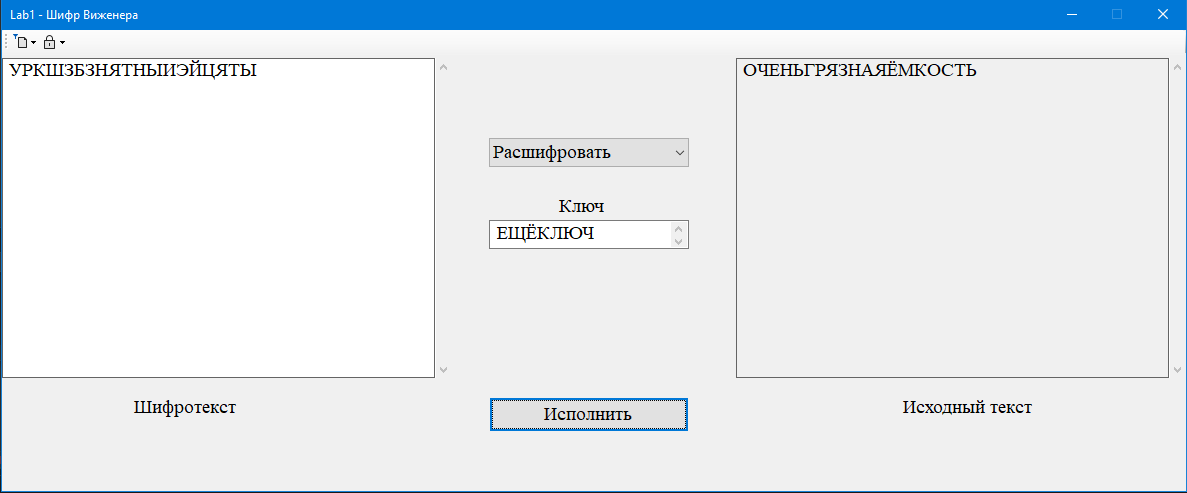


Рис. 16 – Дешифрование

3. Недопустимые значения для ключа

Тест 3

**Исходный текст:** текст для теста

**Полученный шифрующий текст:** ТЕКСТ ДЛЯ ТЕСТА

**Ключ:** 1

**Шифротекст:** –

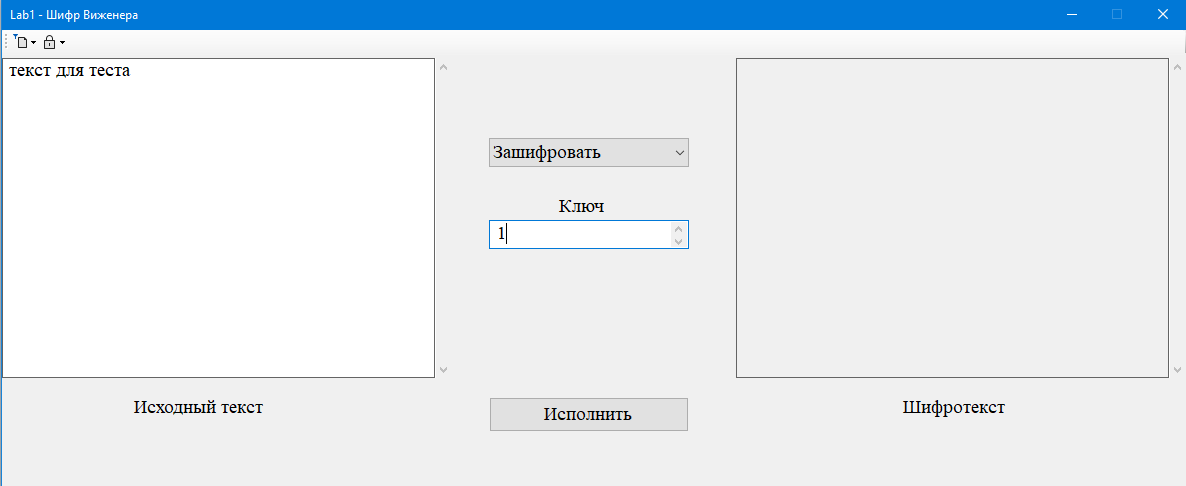


Рис. 17 – Попытка шифрования (до выполнения)

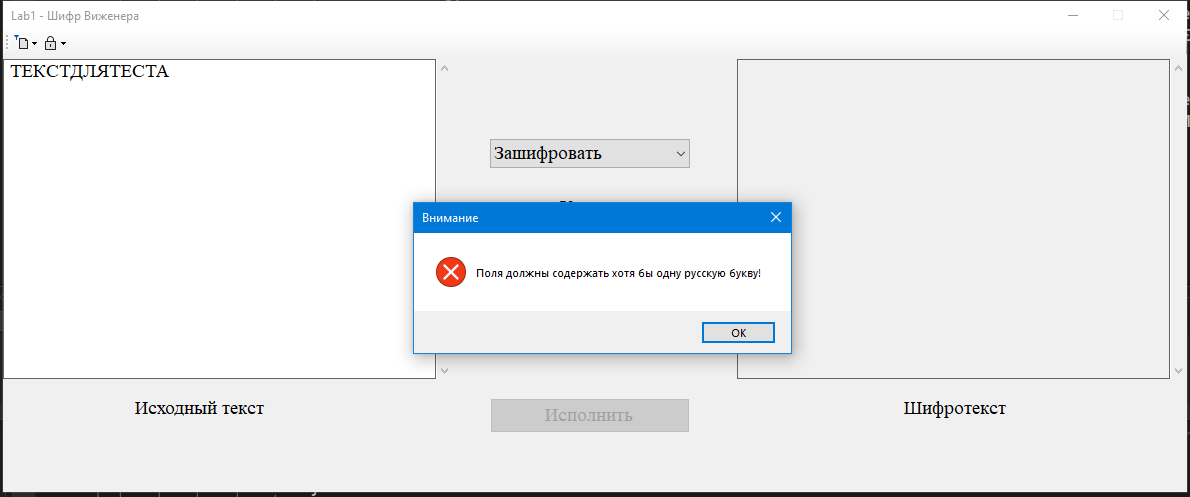


Рис. 18 – Попытка шифрования (после выполнения)

Тест 4

**Исходный текст:** проверка ключа

**Полученный шифрующий текст:** ПРОВЕРКА КЛЮЧА

**Ключ:** FLболь.шой...ключ 123на этот22 раз

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| П | Р | О | В | Е | Р | К | А | К | Л | Ю | Ч | А |  |  |  |  |  |  |  |
| Б | О | Л | Ь | Ш | О | Й | К | Л | Ю | Ч | Н | А | Э | Т | О | Т | Р | А | З |

**Шифротекст:** РЯЪЮЭЯФКЦЙХЕА

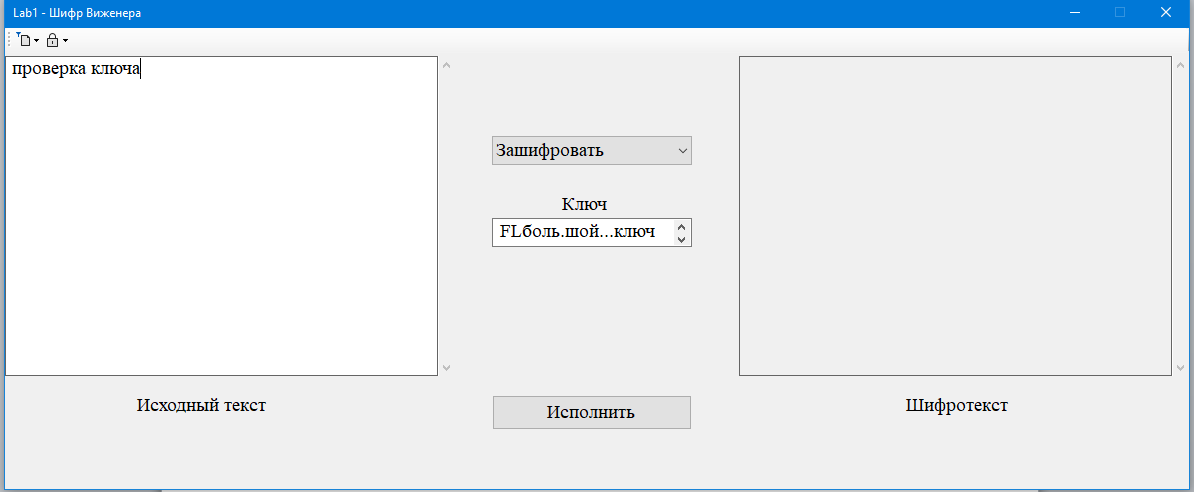


Рис. 19 – Шифрование (до выполнения)

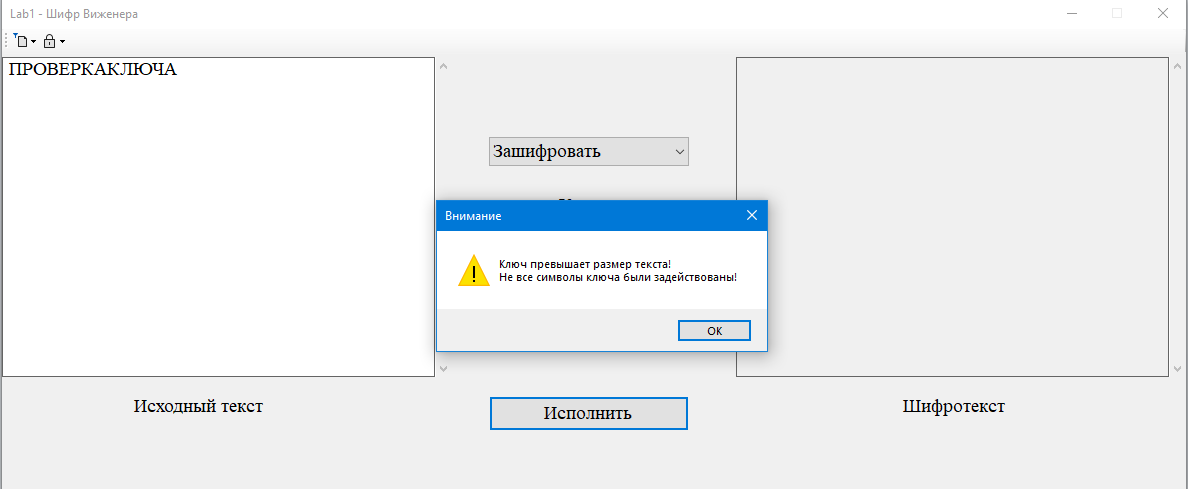


Рис. 20 – Шифрование (во время выполнения)

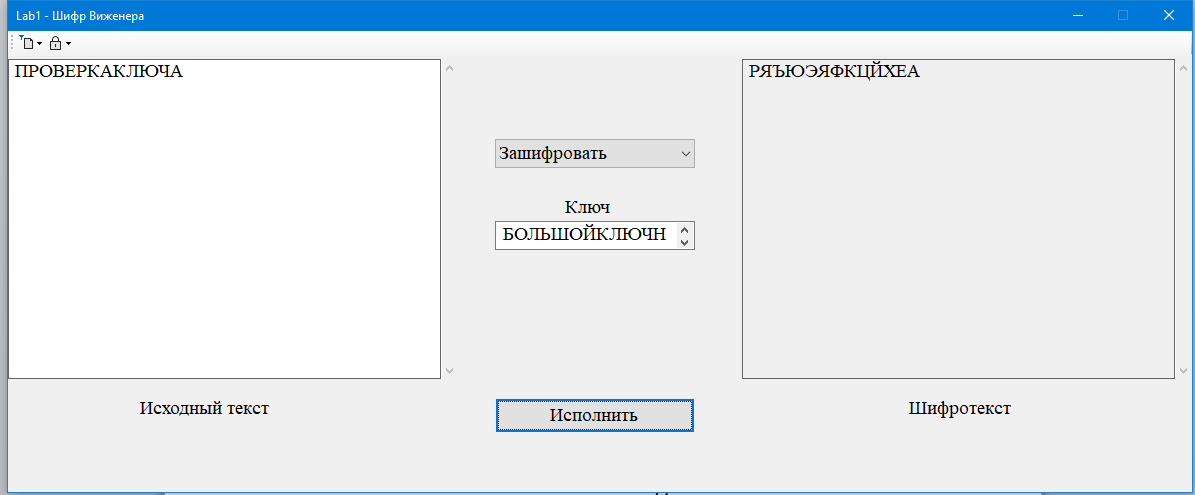


Рис. 19 – Шифрование (после выполнения)

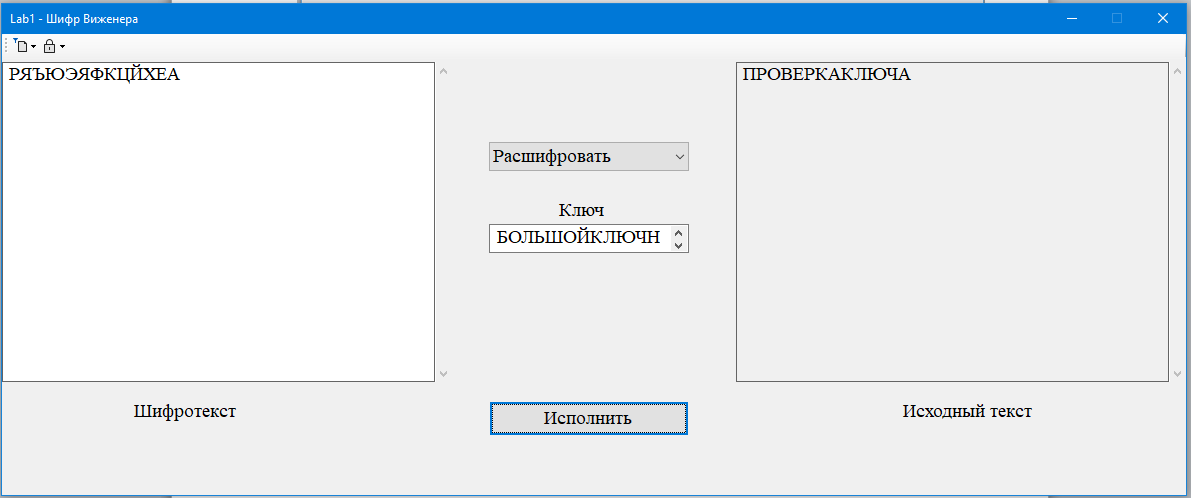


Рис. 20 – Дешифрование