Министерство образования Республики Беларусь

Учреждение образования

БелорусскиЙ государственный университет

информатики и радиоэлектроники

Факультет компьютерных систем и сетей

Кафедра программного обеспечения информационных технологий

Дисциплина: Теория информации (ТИ)

**оТЧЕТ**

ПО ЛАБОРАТОРНОЙ РАБОТЕ №1

Перестановочные и подстановочные алгоритмы шифрования

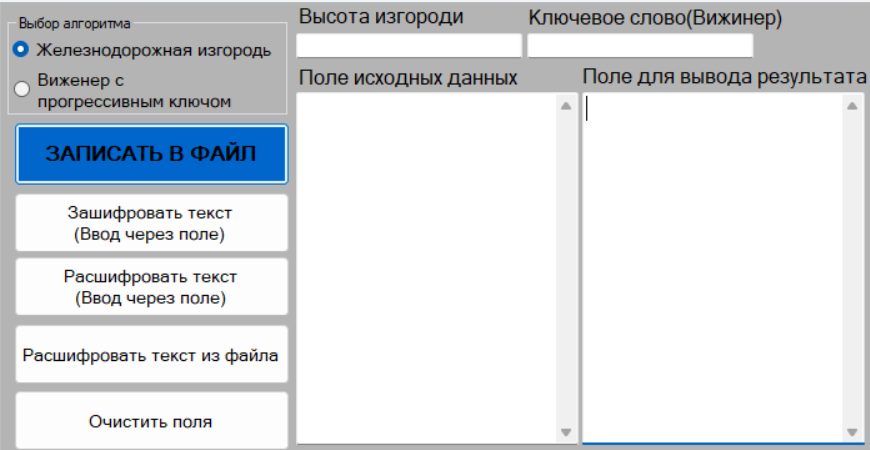
Выполнил

студент: гр. 351002 Яночкин И.Л.

Проверила: Болтак С.В.

Минск 2025

**Общий вид**

****

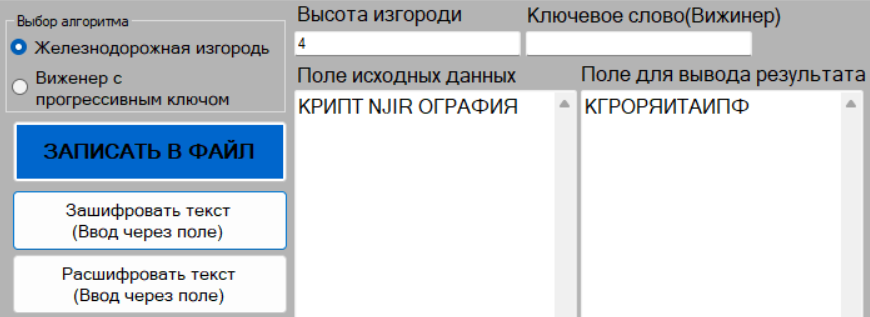
**Тестовые наборы для шифрования и дешифрования алгоритмом железнодорожная изгородь**

Тест 1

Тестовая ситуация: текст содержит английские буквы, **четный** ключ.

Исходный текст: КРИПТ NJIR ОГРАФИЯ

Ключ: 4



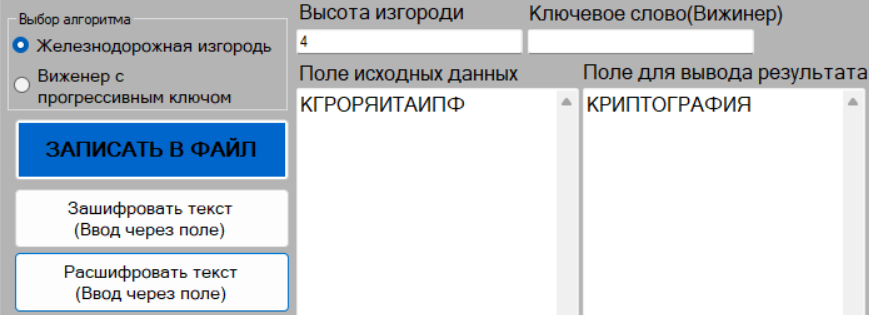


Рисунок 1 – Полученный результат. Тест 1

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| к |  |  |  |  |  | г |  |  |  |  |  |
|  | р |  |  |  | о |  | р |  |  |  | я |
|  |  | и |  | т |  |  |  | а |  | и |  |
|  |  |  | п |  |  |  |  |  | Ф |  |  |

*Шифротекст*: КГРОРЯИТАИПФ

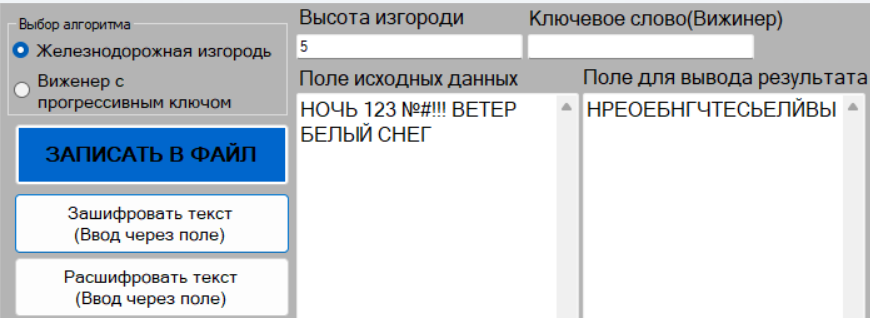
Ожидаемый и полученный результат: символы, не принадлежащие алфавиту, не были обработаны. Текст зашифрован и расшифрован.

Тест 2

Тестовая ситуация: текст содержит символы не принадлежащие алфавиту, **нечетный** ключ.

Исходный текст: НОЧЬ 123 №#!!! ВЕТЕР БЕЛЫЙ СНЕГ

Ключ: 5



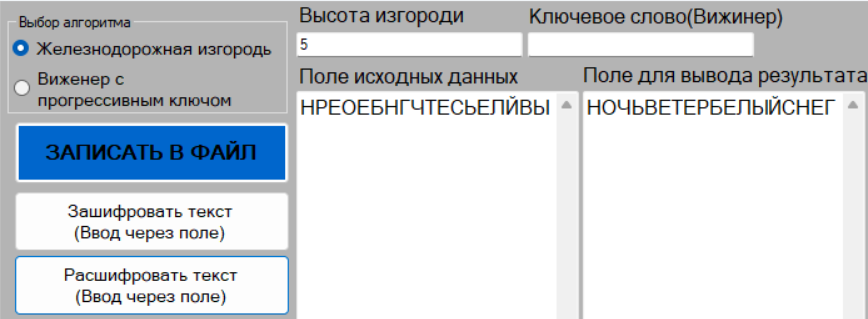


Рисунок 2 – Полученный результат. Тест 2

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Н |  |  |  |  |  |  |  | Р |  |  |  |  |  |  |  | Е |  |
|  | О |  |  |  |  |  | Е |  | Б |  |  |  |  |  | Н |  | Г |
|  |  | Ч |  |  |  | Т |  |  |  | Е |  |  |  | С |  |  |  |
|  |  |  | Ь |  | Е |  |  |  |  |  | Л |  | Й |  |  |  |  |
|  |  |  |  | В |  |  |  |  |  |  |  | Ы |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

*Шифротекст*: НРЕОЕБНГЧТЕСЬЕЛЙВЫ

Ожидаемый и полученный результат: Ожидаемый и полученный результат: символы, не принадлежащие алфавиту, не были обработаны. Текст зашифрован и расшифрован.

Тест 3

Тестовая ситуация: Корректный текст, ключ равен **нулю.**

Исходный текст: ПРИВЕТ МИР

Ключ: 0

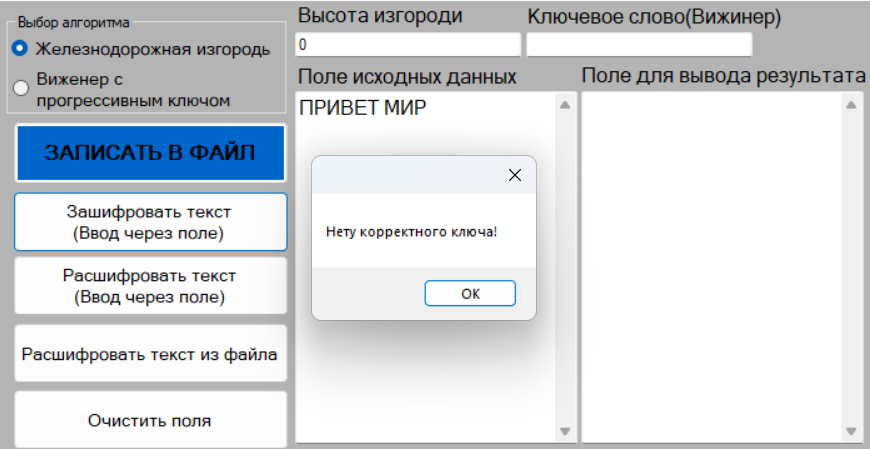


Рисунок 3 – Полученный результат. Тест 3

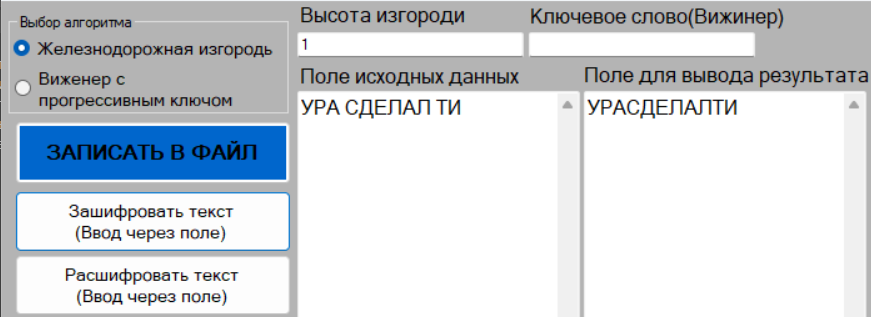
Ожидаемый и полученный результат: Выведено сообщение о некорректности ключа, текст не зашифрован.

Тест 4

Тестовая ситуация: Ввод корректного текста, ключ **равен 1**.

Исходный текст: УРА СДЕЛАЛ ТИ

Ключ: 1



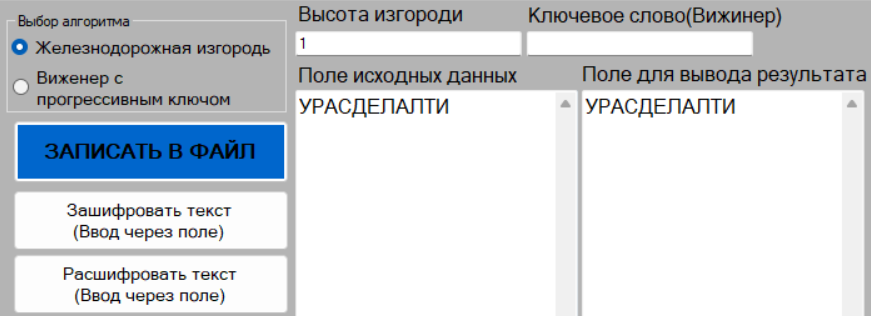


Рисунок 4 – Полученный результат. Тест 4

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| У | Р | А | С | Д | Е | Л | А | Л | Т | И |

*Шифротекст:*УРАСДЕЛАЛТИ

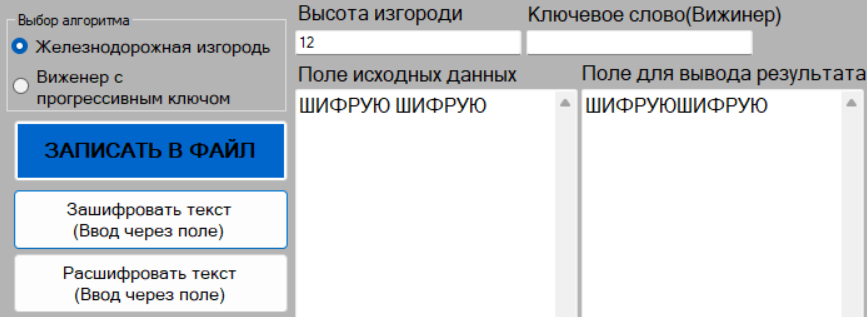
Ожидаемый и полученный результат: зашифрованный текст равен исходному тексту.

Тест 5

Тестовая ситуация: ключ равен количеству символов исходного текста.

Исходный текст: ШИФРУЮ ШИФРУЮ

Ключ: 12



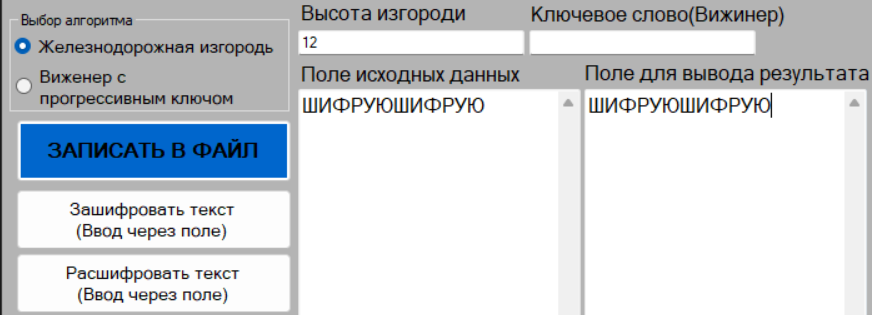


Рисунок 5 – Полученный результат. Тест 5

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Ш |  |  |  |  |  |  |  |  |  |  |  |
|  | И |  |  |  |  |  |  |  |  |  |  |
|  |  | Ф |  |  |  |  |  |  |  |  |  |
|  |  |  | Р |  |  |  |  |  |  |  |  |
|  |  |  |  | У |  |  |  |  |  |  |  |
|  |  |  |  |  | Ю |  |  |  |  |  |  |
|  |  |  |  |  |  | Ш |  |  |  |  |  |
|  |  |  |  |  |  |  | И |  |  |  |  |
|  |  |  |  |  |  |  |  | Ф |  |  |  |
|  |  |  |  |  |  |  |  |  | Р |  |  |
|  |  |  |  |  |  |  |  |  |  | У |  |
|  |  |  |  |  |  |  |  |  |  |  | Ю |

*Шифротекст:* ШИФРУЮШИФРУЮ

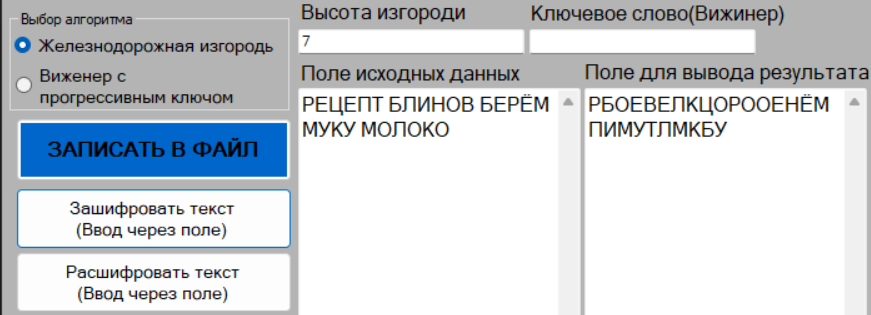
Ожидаемый и полученный результат: зашифрованный текст равен исходному тексту.

Тест 6

Тестовая ситуация: Ввод корректного текста и нечетного ключа.

Исходный текст: РЕЦЕПТ БЛИНОВ БЕРЁМ МУКУ МОЛОКО

Ключ: 7



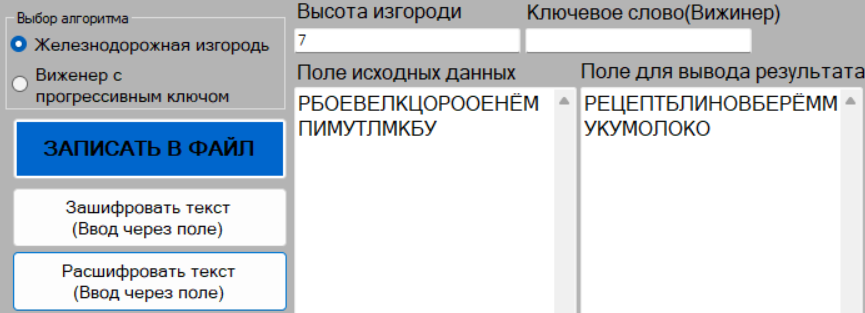


Рисунок 6 – Полученный результат. Тест 6

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Р |  |  |  |  |  |  |  |  |  |  |  | Б |  |  |  |  |  |  |  |  |  |  |  | О |  |  |
|  | Е |  |  |  |  |  |  |  |  |  | В |  | Е |  |  |  |  |  |  |  |  |  | Л |  | К |  |
|  |  | Ц |  |  |  |  |  |  |  | О |  |  |  | Р |  |  |  |  |  |  |  | О |  |  |  | О |
|  |  |  | Е |  |  |  |  |  | Н |  |  |  |  |  | Ё |  |  |  |  |  | М |  |  |  |  |  |
|  |  |  |  | П |  |  |  | И |  |  |  |  |  |  |  | М |  |  |  | У |  |  |  |  |  |  |
|  |  |  |  |  | Т |  | Л |  |  |  |  |  |  |  |  |  | М |  | К |  |  |  |  |  |  |  |
|  |  |  |  |  |  | Б |  |  |  |  |  |  |  |  |  |  |  | У |  |  |  |  |  |  |  |  |

*Шифротекст:* РБОЕВЕЛКЦОРООЕНЁМПИМУТЛМКБУ

Тест 7

Тестовая ситуация: Ввод одной буквы исходного текста, четный ключ.

Исходный текст: А

Ключ: 4

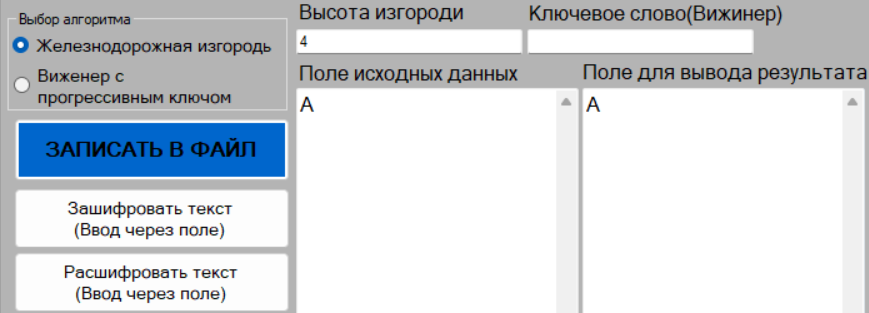


Рисунок 7 – Полученный результат. Тест 7

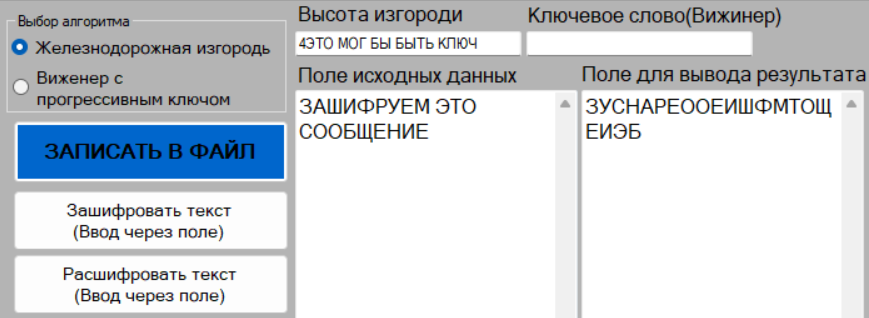
Ожидаемый и полученный результат: полученный результат - это исходный символ.

Тест 8

Тестовая ситуация: Ввод корректного исходного текста и ключа содержащего буквы.

Исходный текст: ЗАШИФРУЕМ ЭТО СООБЩЕНИЕ

Ключ: 4ЭТО МОГ БЫ БЫТЬ КЛЮЧ



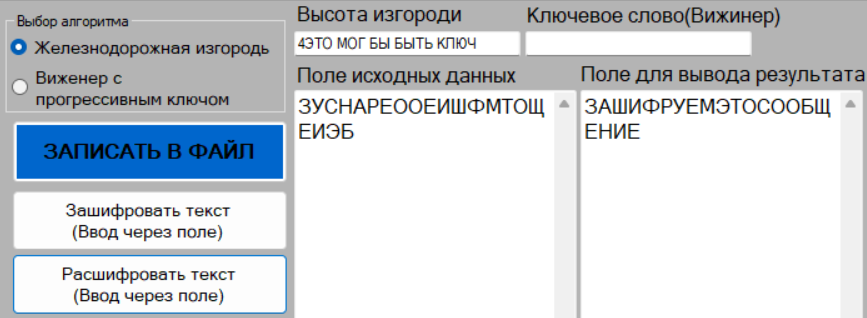


Рисунок 8 – Полученный результат. Тест 8

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| З |  |  |  |  |  | У |  |  |  |  |  | С |  |  |  |  |  | Н |  |  |
|  | А |  |  |  | Р |  | Е |  |  |  | О |  | О |  |  |  | Е |  | И |  |
|  |  | Ш |  | Ф |  |  |  | М |  | Т |  |  |  | О |  | Щ |  |  |  | Е |
|  |  |  | И |  |  |  |  |  | Э |  |  |  |  |  | Б |  |  |  |  |  |

*Шифротекст:* ЗУСНАРЕООЕИШФМТОЩЕИЭБ

**Тестовые наборы для шифрования и дешифрования Виженера(прогрессивный ключ)**

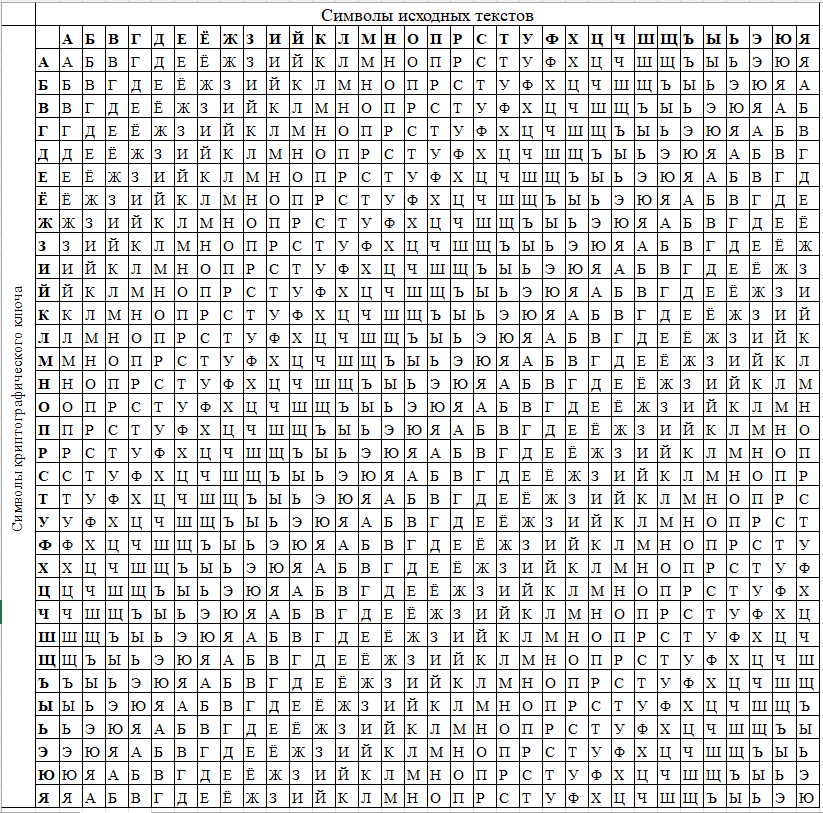


Рисунок 1 – Таблица Виженера.

Считаем по формулам каждый символ:

Для шифрования: C = (P + K) mod N

Для дешифрования: P = (C - K + N) mod N

C — буква зашифрованного текста; P — буква исходного текста; K — буква ключа; N — длина алфавита

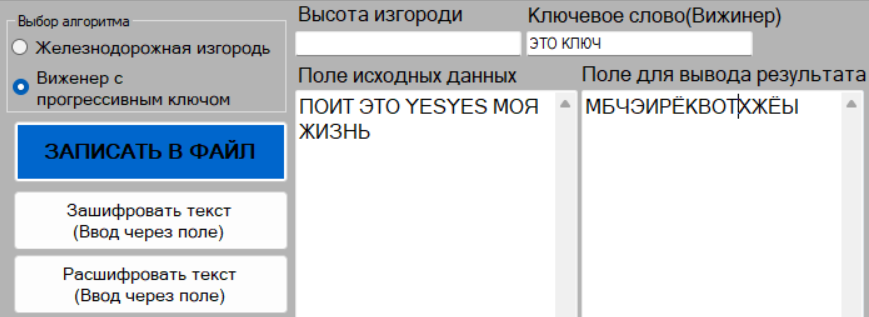
Тест 9

Тестовая ситуация: текст с недопустимыми символами, корректный ключ.

Исходный текст: ПОИТ ЭТО YESYES МОЯ ЖИЗНЬ

Ключ: ЭТО КЛЮЧ

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| M | = | П | О | И | Т | Э | Т | О | М | О | Я | Ж | И | З | Н | Ь |
| K | = | Э | Т | О | К | Л | Ю | Ч | Ю | У | П | Л | М | Я | Ш | Я |
| C | = | М | Б | Ч | Э | И | Р | Ё | К | В | О | Т | Х | Ж | Ё | Ы |



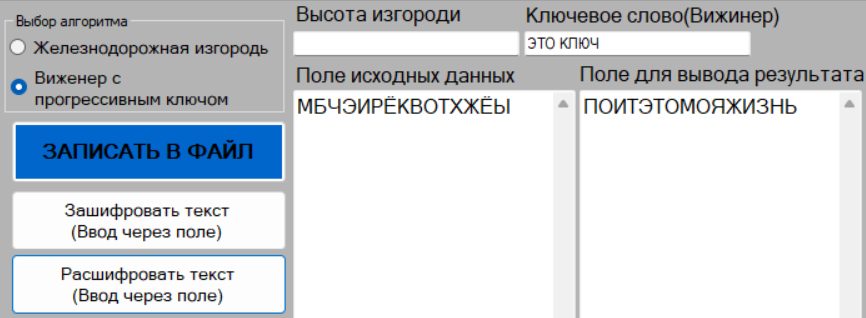


Рисунок 9 – Полученный результат. Тест 9

*Шифротекст*: МБЧЭИРЁКВОТХЖЁЫ.

Тест 10

Тестовая ситуация: текст, содержащий букву Ё, корректный ключ.

Исходный текст: ЧЁ КОГО БРО ЭТО Я МАРИО

Ключ: ТОЖЕ КЛЮЧ

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| M | = | Ч | Ё | К | О | Г | О | Б | Р | О | Э | Т | О | Я | М | А | Р | И | О |
| K | = | Т | О | Ж | Е | К | Л | Ю | Ч | У | П | З | Ё | Л | М | Я | Ш | Ф | Р |
| C | = | Й | Ф | С | У | Н | Ъ | Я | З | В | М | Ъ | Ф | К | Щ | Я | И | Э | Я |

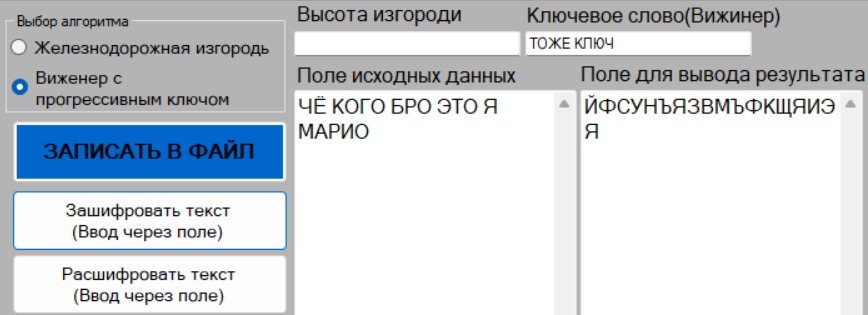
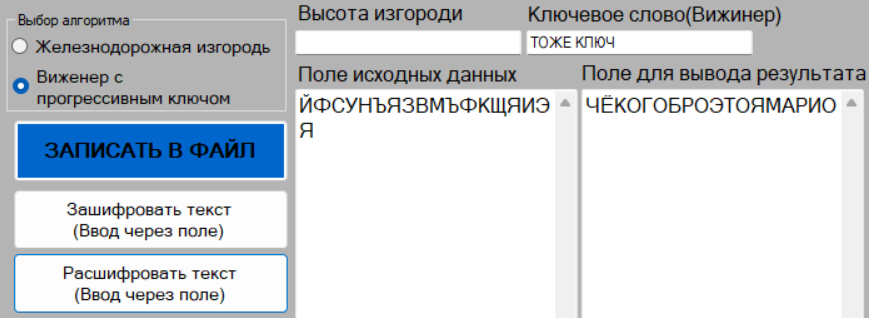
 

Рисунок 10 – Полученный результат. Тест 10

*Шифротекст*: ЙФСУНЪЯЗВМЪФКЩЯИЭЯ

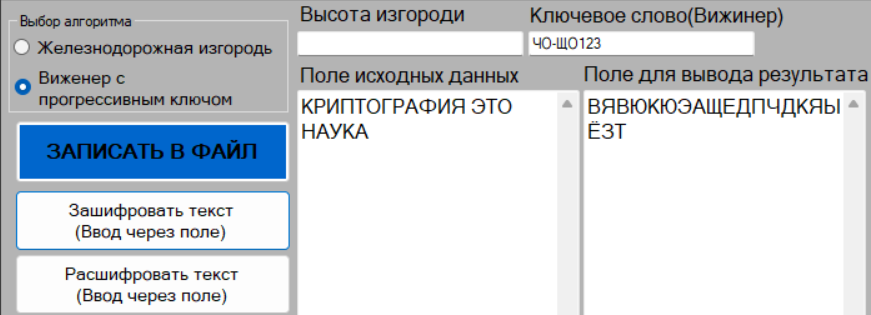
Тест 11

Тестовая ситуация: ключ, содержащий недопустимые значения.

Исходный текст: КРИПТОГРАФИЯ ЭТО НАУКА

Ключ: ЧО-ЩО123

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| M | = | К | Р | И | П | Т | О | Г | Р | А | Ф | И | Я | Э | Т | О | Н | А | У | К | А |
| K | = | Ч | О | Щ | О | Ш | П | Ъ | П | Щ | Р | Ы | Р | Ъ | С | Ь | С | Ы | Т | Э | Т |
| C | = | В | Я | В | Ю | К | Ю | Э | А | Щ | Е | Д | П | Ч | Д | К | Я | Ы | Ё | З | Т |



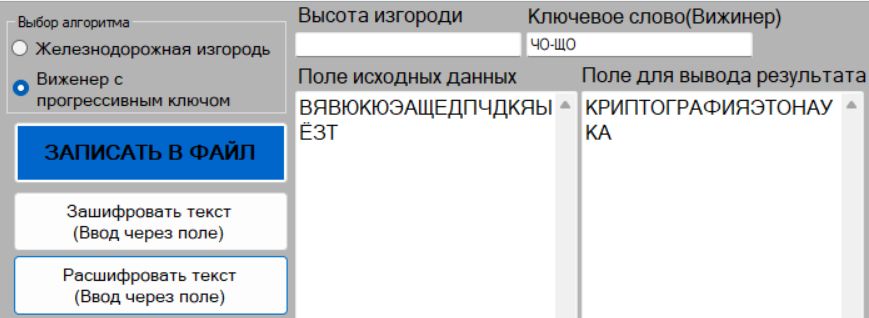


Рисунок 11 – Полученный результат. Тест 11

*Шифротекст*: ВЯВЮКЮЭАЩЕДПЧДКЯЫЁЗТ

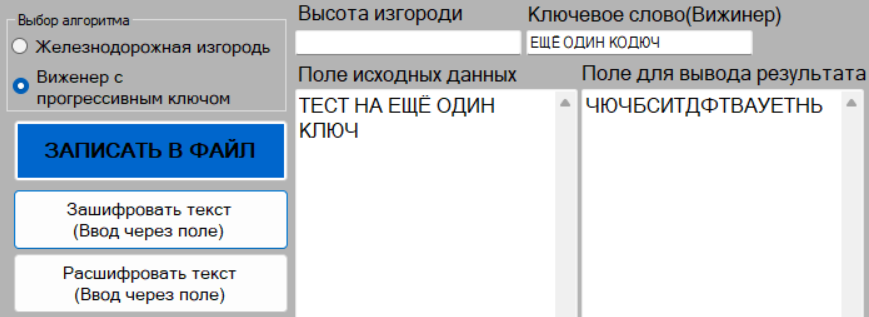
Тест 12

Тестовая ситуация: ключ, содержащий букву ё.

Исходный текст: ТЕСТ НА ЕЩЁ ОДИН КЛЮЧ

Ключ: ЕЩЁ ОДИН КОДЮЧ

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| M | = | Т | Е | С | Т | Н | А | Е | Щ | Ё | О | Д | И | Н | К | Л | Ю | Ч |
| K | = | Е | Щ | Ё | О | Д | И | Н | К | Л | Ю | Ч | Ё | Ъ | Ж | П | Е | Й |
| C | = | Ч | Ю | Ч | Б | С | И | Т | Д | С | М | Ы | О | З | С | Ы | Г | Б |



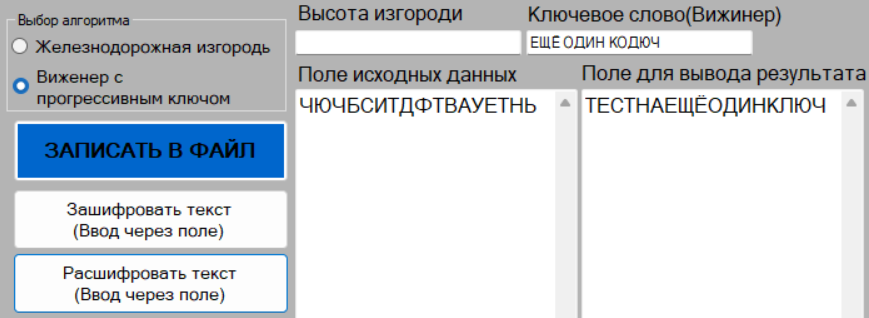


Рисунок 12 – Полученный результат. Тест 12

*Шифротекст*: ТЕСТНАЕЩЁОДИНКЛЮЧ

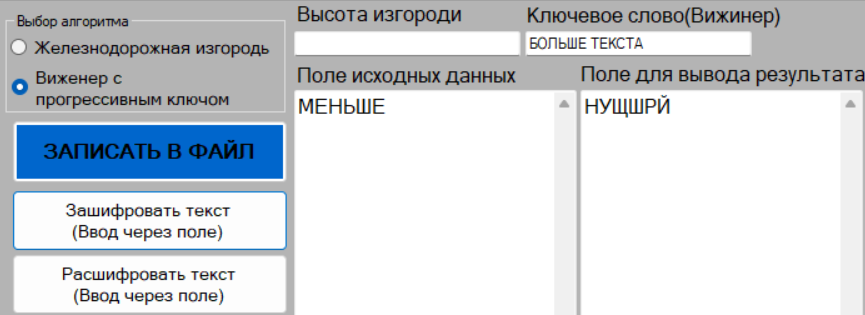
Тест 13

Тестовая ситуация: ключ больше исходного текста.

Исходный текст: МЕНЬШЕ

Ключ: БОЛЬШЕ ТЕКСТА

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| M | = | М | Е | Н | Ь | Ш | Е |  |  |  |  |  |  |
| K | = | Б | О | Л | Ь | Ш | Е | Т | Е | К | С | Т | А |
| C | = | Н | У | Щ | Ш | Р | Й |  |  |  |  |  |  |



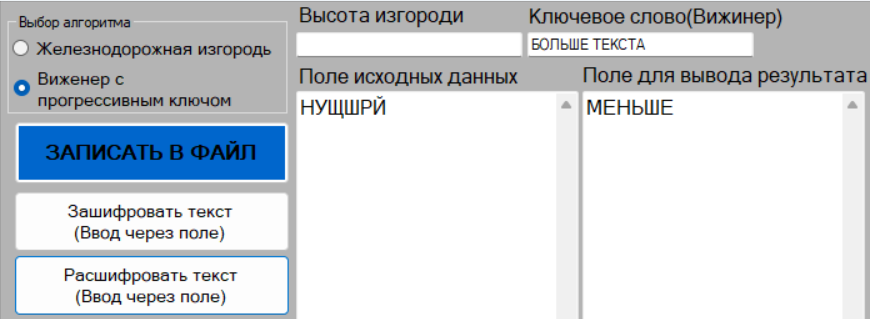


Рисунок 13 – Полученный результат. Тест 13

*Шифротекст*: НУЩШРЙ

Тест 14

Тестовая ситуация: Ввод некорректного ключа.

Исходный текст: ТЕКСТ

Ключ: INCORRECT

Ожидаемый и полученный результат: Сообщение о некорректности ключа, текст не зашифрован.

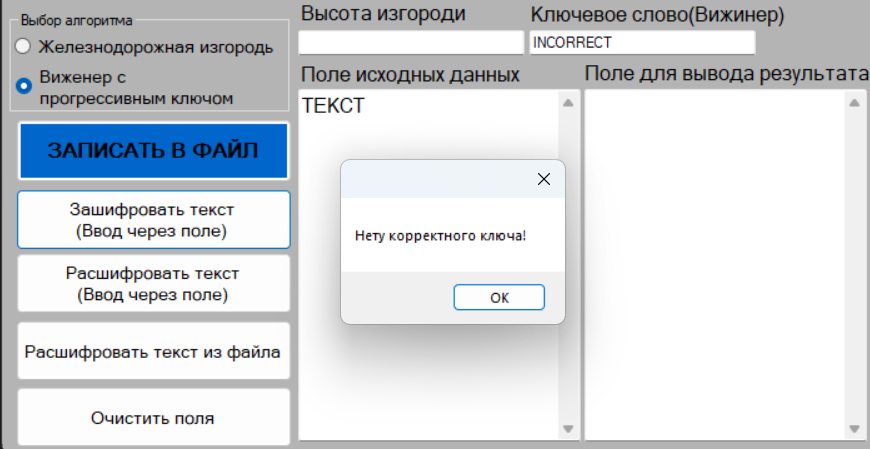


Рисунок 14 – Полученный результат. Тест 14