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

Тема работы: Простейшие шифры

Выполнил

студент: гр. 151003 Матошко И.В.

Проверил: Болтак С.В.

Минск, 2022

Вариант 7

Метод поворачивающейся решетки

Дымовое тестирование

Тестовая фраза на заданном языке: Hello@\*\*from^heaven

Исходная решетка:

|  |  |  |  |
| --- | --- | --- | --- |
| X |  |  |  |
|  |  |  | X |
|  |  | X |  |
|  | X |  |  |

Шифрование по шагам:

|  |  |  |  |
| --- | --- | --- | --- |
| H |  |  |  |
|  |  |  | E |
|  |  | L |  |
|  | L |  |  |

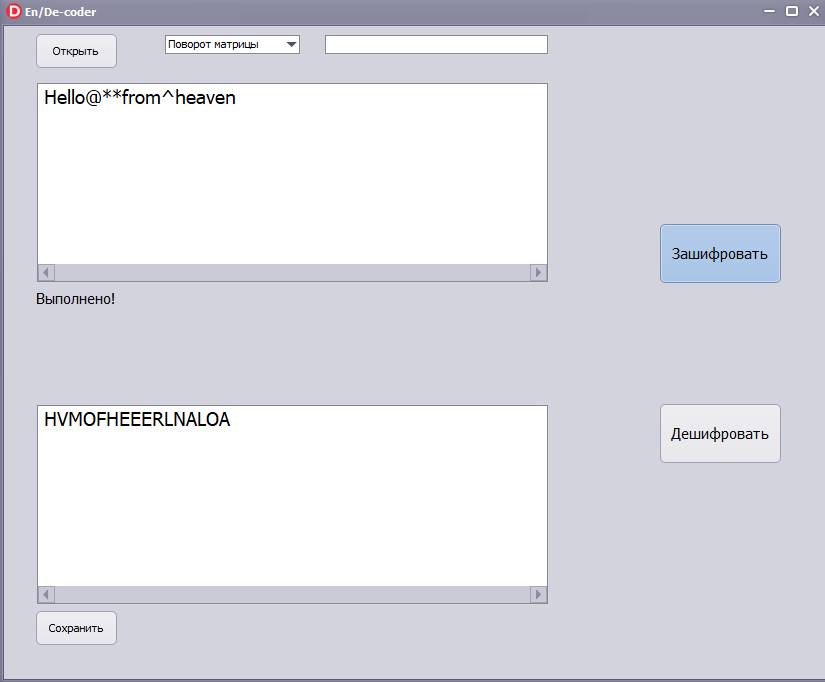
|  |  |  |  |
| --- | --- | --- | --- |
| H |  |  | O |
| F |  |  | E |
|  | R | L |  |
|  | L | O |  |

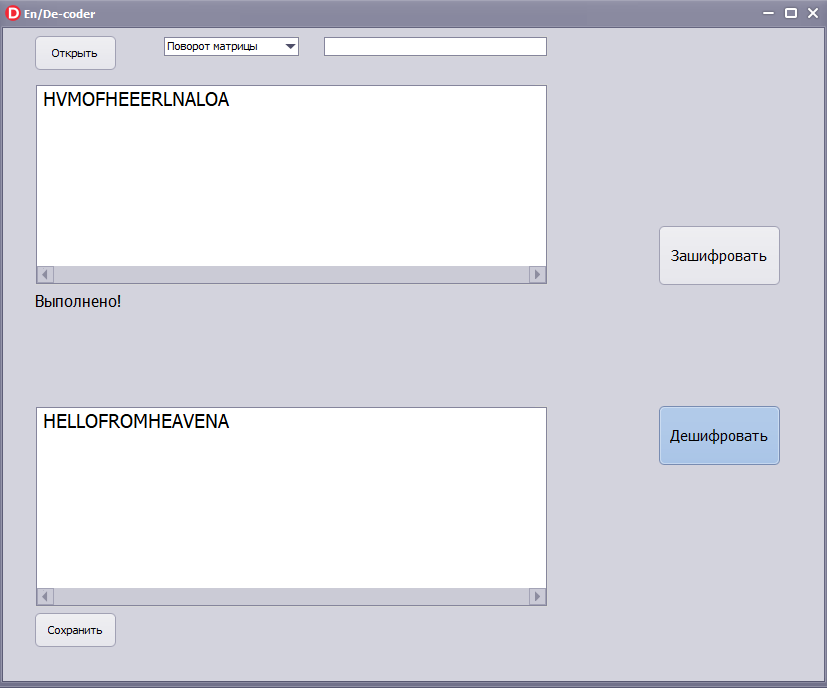
|  |  |  |  |
| --- | --- | --- | --- |
| H |  | M | O |
| F | H |  | E |
| E | R | L |  |
|  | L | O | A |

|  |  |  |  |
| --- | --- | --- | --- |
| H | V | M | O |
| F | H | E | E |
| E | R | L | N |
| A | L | O | A |

Шифротекст: HVMOFHEEERLNALOA

Результаты работы программы:





Тестирование на валидных данных

Тестовая фраза на заданном языке: hellofromheavenhello!

Исходная решетка:

|  |  |  |  |
| --- | --- | --- | --- |
| X |  |  |  |
|  |  |  | X |
|  |  | X |  |
|  | X |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| E |  |  |  |
|  |  |  | L |
|  |  | L |  |
|  | O |  |  |

Шифрование по шагам:

|  |  |  |  |
| --- | --- | --- | --- |
| H |  |  |  |
|  |  |  | E |
|  |  | L |  |
|  | L |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| H |  |  | O |
| F |  |  | E |
|  | R | L |  |
|  | L | O |  |

|  |  |  |  |
| --- | --- | --- | --- |
| E |  |  | A |
| B |  |  | L |
|  | C | L |  |
|  | O | D |  |

|  |  |  |  |
| --- | --- | --- | --- |
| H |  | M | O |
| F | H |  | E |
| E | R | L |  |
|  | L | O | A |

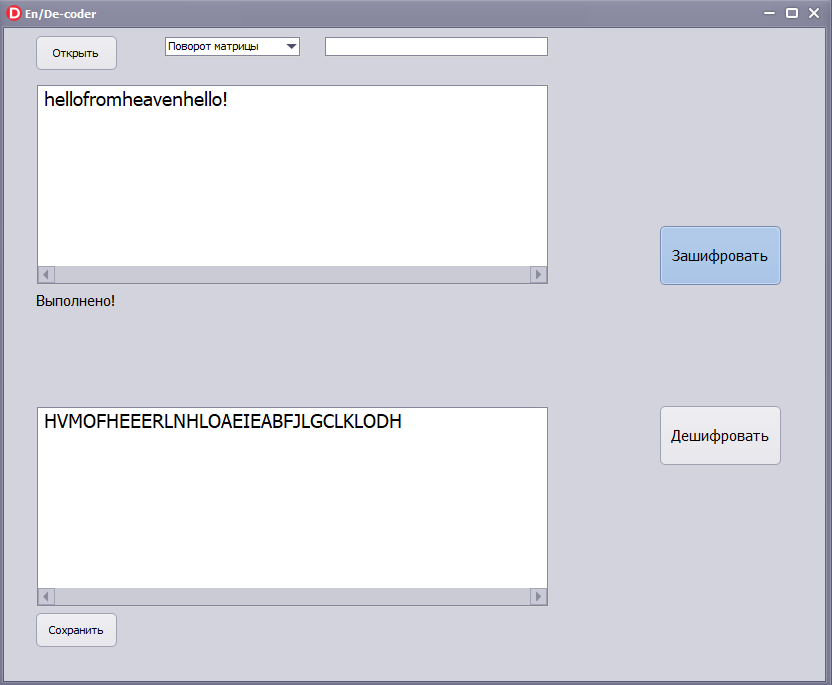
|  |  |  |  |
| --- | --- | --- | --- |
| E |  | E | A |
| B | F |  | L |
| G | C | L |  |
|  | O | D | H |

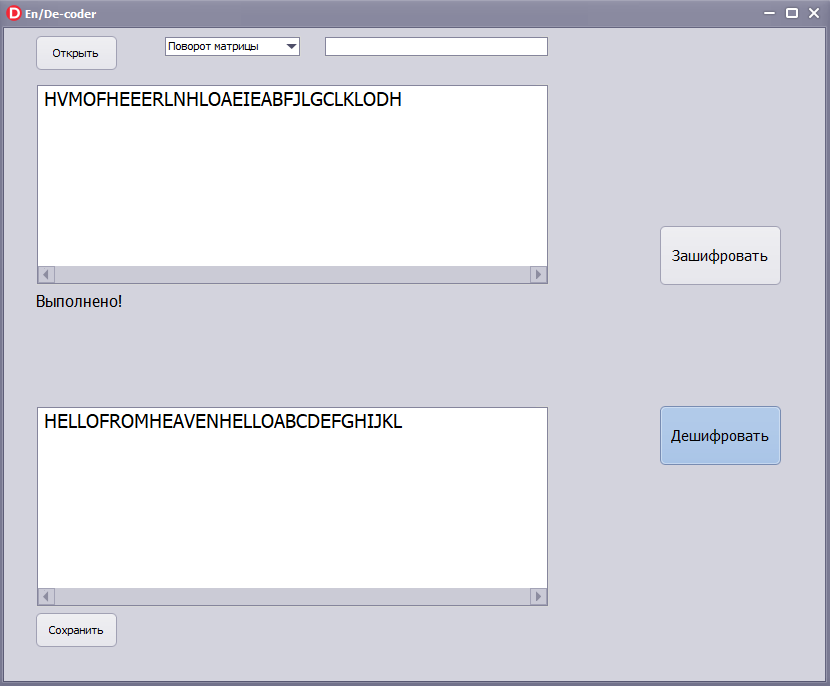
|  |  |  |  |
| --- | --- | --- | --- |
| H | V | M | O |
| F | H | E | E |
| E | R | L | N |
| H | L | O | A |

|  |  |  |  |
| --- | --- | --- | --- |
| E | I | E | A |
| B | F | J | L |
| G | C | L | K |
| L | O | D | H |

Шифротекст: HVMOFHEEERLNHLOAEIEABFJLGCLKLODH

Результаты работы программы:





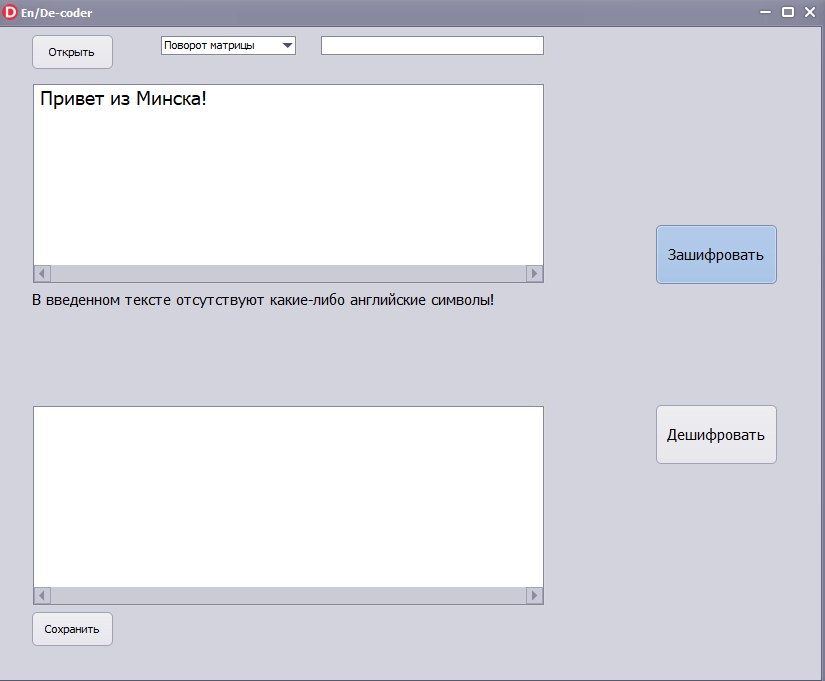
Тестирование на не валидных данных

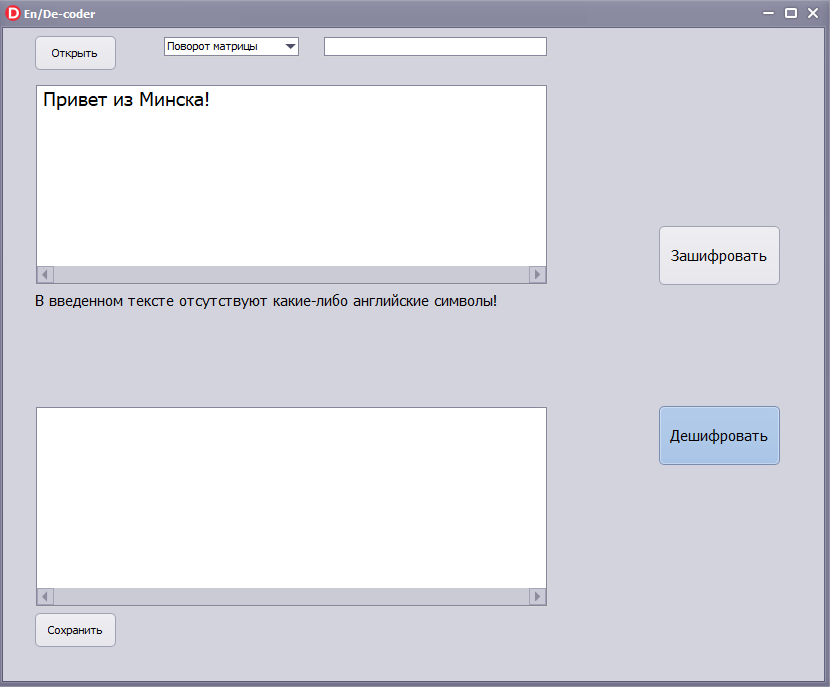
Тестовая фраза на заданном языке: Привет из Минска!

Исходная решетка:

|  |  |  |  |
| --- | --- | --- | --- |
| X |  |  |  |
|  |  |  | X |
|  |  | X |  |
|  | X |  |  |

Результаты работы программы:



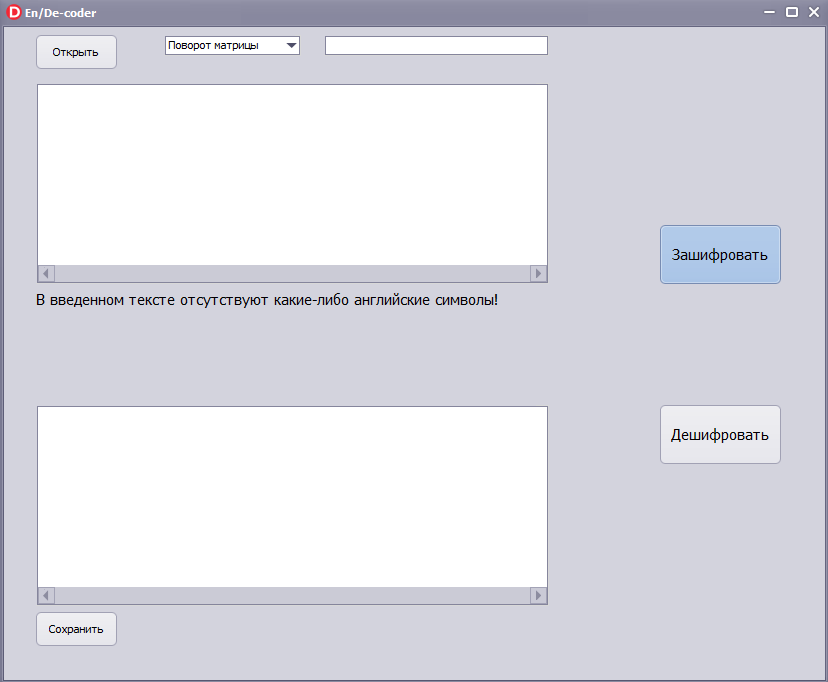


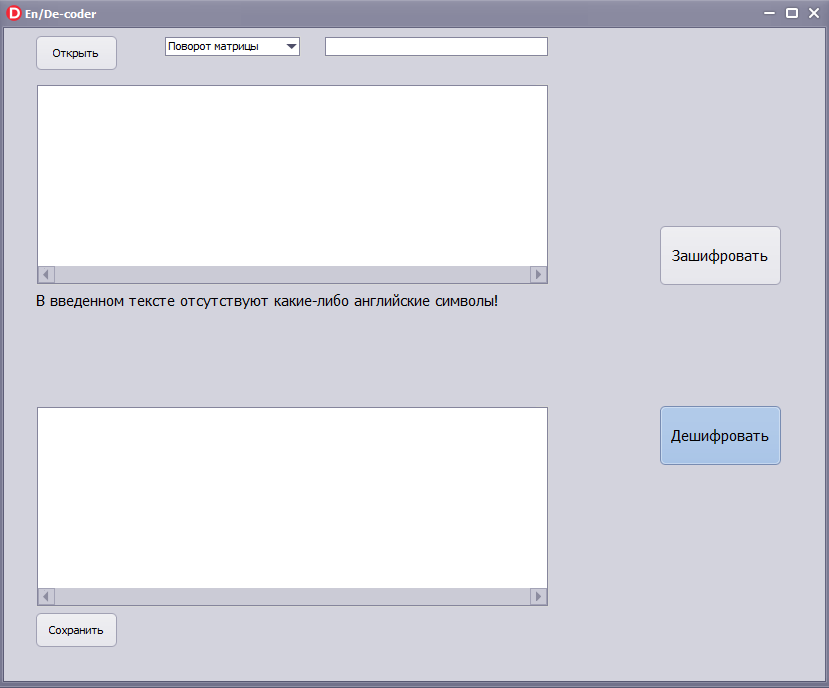
Тестовая фраза на заданном языке: \*пустая строка\*

Исходная решетка:

|  |  |  |  |
| --- | --- | --- | --- |
| X |  |  |  |
|  |  |  | X |
|  |  | X |  |
|  | X |  |  |

Результаты работы программы:





Алгоритм Виженера

Дымовое тестирование

Тестовая фраза на заданном языке: При»»вет из Минска!

Ключ: мир

Преобразованная фраза: ПРИВЕТИЗМИНСКА

Таблица подстановки:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 16 | 17 | 9 | 2 | 5 | 19 | 9 | 8 | 13 | 9 | 14 | 18 | 11 | 0 |
| П | Р | И | В | Е | Т | И | З | М | И | Н | С | К | А |
| 13 | 9 | 17 | 14 | 10 | 18 | 15 | 11 | 19 | 16 | 12 | 20 | 17 | 13 |
| М | И | Р | Н | Й | С | О | К | Т | П | Л | У | Р | М |

П и М = 16 + 13 mod 33 = 29 = Ь

Р и И = 17 + 9 mod 33 = 26 = Щ

И и Р = 17 + 9 mod 33 = 26 = Щ

В и Н = 2 + 14 mod 33 = 16 = П

Е и Й = 5 + 10 mod 33 = 15 = О

Т и С = 19 + 18 mod 33 = 4 = Д

И и о = 9 + 15 mod 33 = 24 = Ч

З и К = 8 + 11 mod 33 = 19 = Т

М и Т = 13 + 19 mod 33 = 32 = Я

И и П = 9 + 16 mod 33 = 25 = Ш

Н и Л = 14 + 12 mod 33 = 26 = Щ

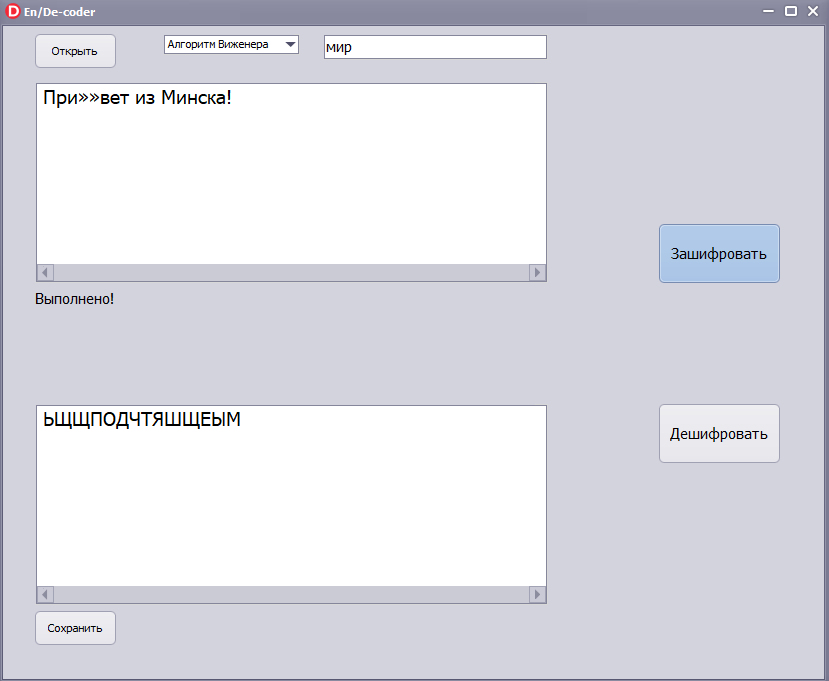
С и У = 18 + 20 mod 33 = 5 = Е

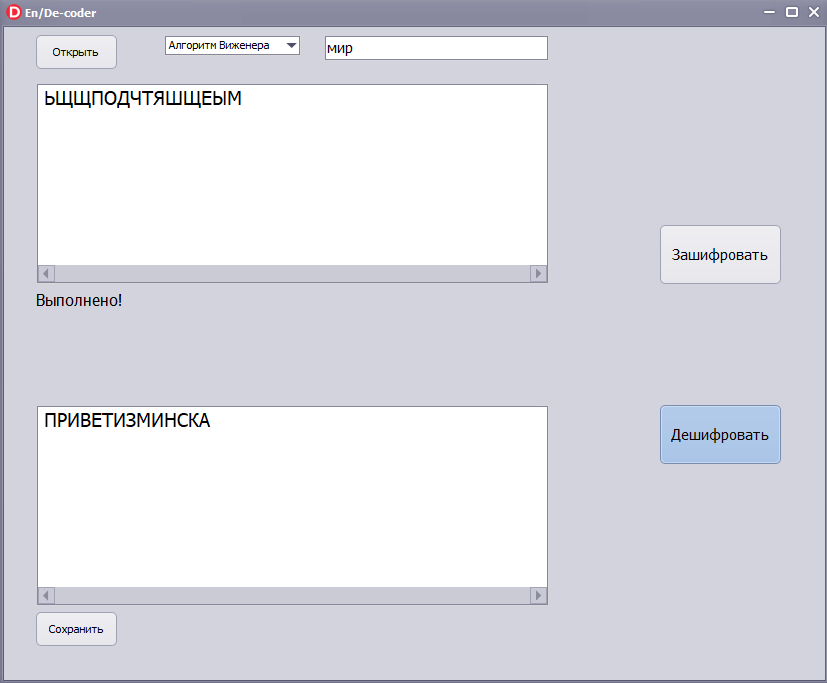
К и Р =11 + 17 mod 33 = 28 = Ы

А и М = 0 + 13 mod 33 = 13 = М

Шифротекст: ЬЩЩПОДЧТЯШЩЕЫМ

Результаты работы программы:





Тестирование на валидных данных

Тестовая фраза на заданном языке: ЁЛКА

Ключ: м

Преобразованная фраза: ЁЛКА

Таблица подстановки:

|  |  |  |  |
| --- | --- | --- | --- |
| 6 | 12 | 11 | 0 |
| Ё | Л | К | А |
| 13 | 14 | 15 | 16 |
| М | Н | О | П |

Ё и М = 6 + 13 mod 33 = 19 = Т

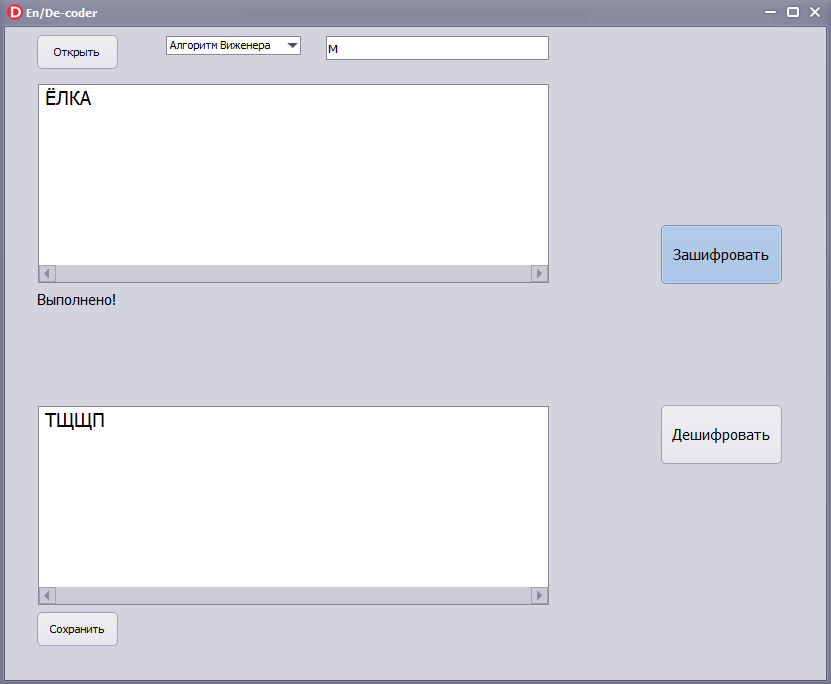
Л и Н = 12 + 14 mod 33 = 26 = Щ

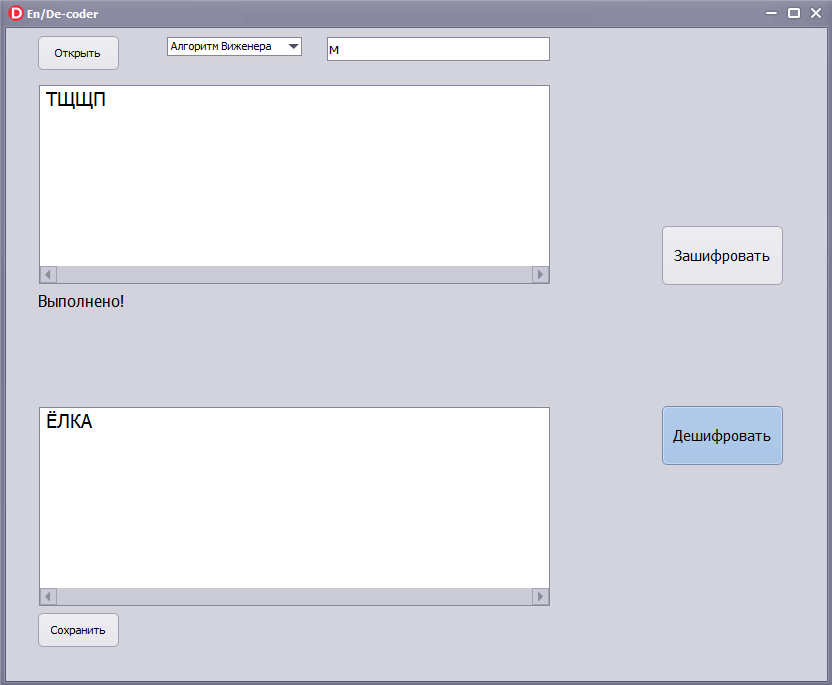
К и О = 11 + 15 mod 33 = 26 = Щ

А и П = 0 + 16 mod 33 = 16 = П

Шифротекст: ТЩЩП

Результаты работы программы:





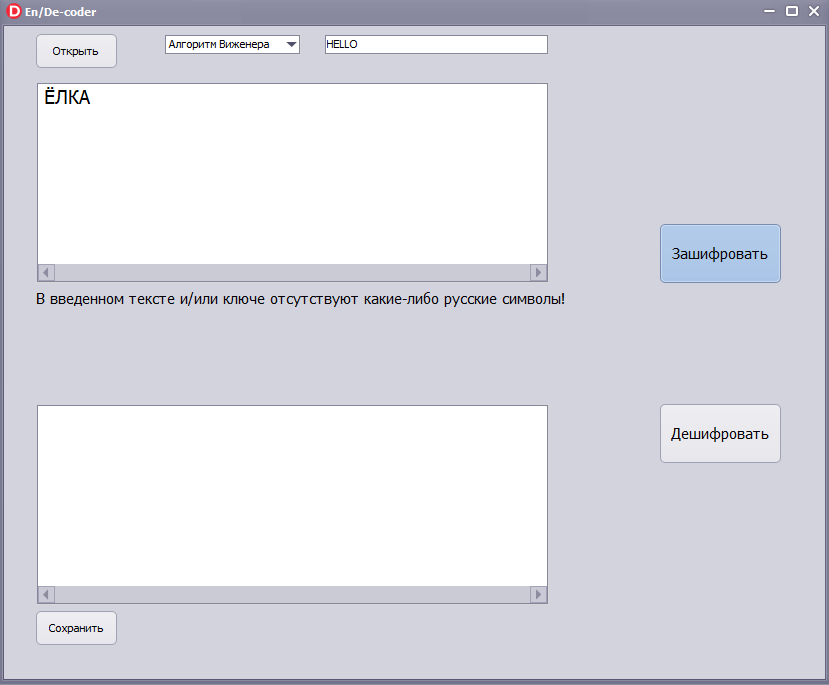
Тестирование на не валидных данных

Тестовая фраза на заданном языке: ЁЛКА

Ключ: HELLO

Преобразованная фраза: ЁЛКА

Результаты работы программы:

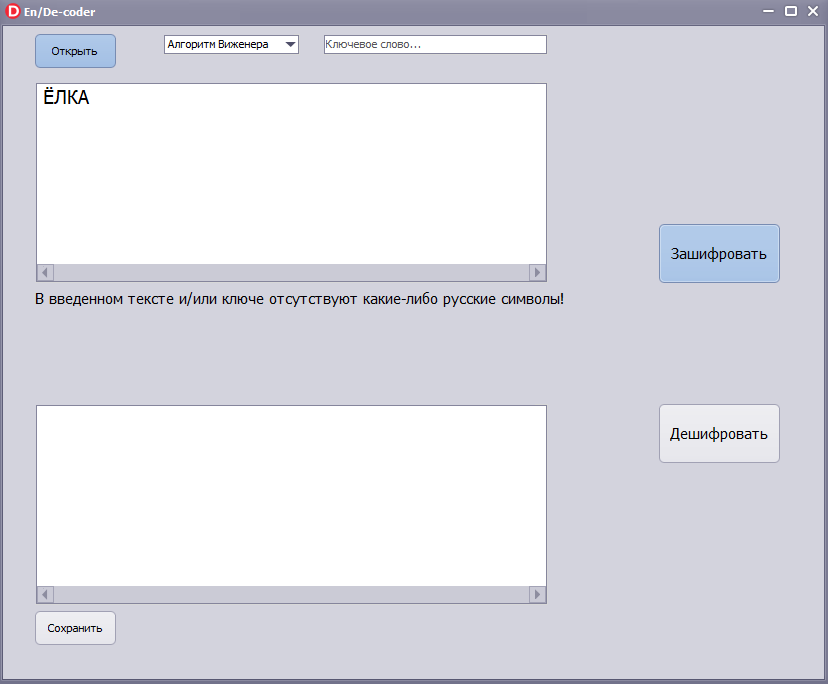


Тестовая фраза на заданном языке: ЁЛКА

Ключ: \*пустая строка\*

Преобразованная фраза: ЁЛКА

Результаты работы программы:



Тестовая фраза на заданном языке: ЁЛКА

Ключ: @м”””””

Использованный ключ (после исключения недопустимых символов): м

Преобразованная фраза: ЁЛКА

Таблица подстановки:

|  |  |  |  |
| --- | --- | --- | --- |
| 6 | 12 | 11 | 0 |
| Ё | Л | К | А |
| 13 | 14 | 15 | 16 |
| М | Н | О | П |

Ё и М = 6 + 13 mod 33 = 19 = Т

Л и Н = 12 + 14 mod 33 = 26 = Щ

К и О = 11 + 15 mod 33 = 26 = Щ

А и П = 0 + 16 mod 33 = 16 = П

Шифротекст: ТЩЩП

Результаты работы программы:

