УО «Белорусский государственный университет информатики и радиоэлектроники»

Кафедра ПОИТ

Отчет по лабораторной работе №1

по предмету «Теория информации»

Вариант 4

Выполнил:

Шевченко А.Д.

Проверил:

Болтак С.В.

Группа 351001

Минск, 2025

**Шифр Виженера(прогрессивный ключ)**

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 |

Тестовый набор 1(проверка корректной работы на валидных данных)

Тест 1

Тестовая ситуация: проверка корректности шифрования случайной фразы

Исходный текст: КРИПТО

Ключ: АБВ

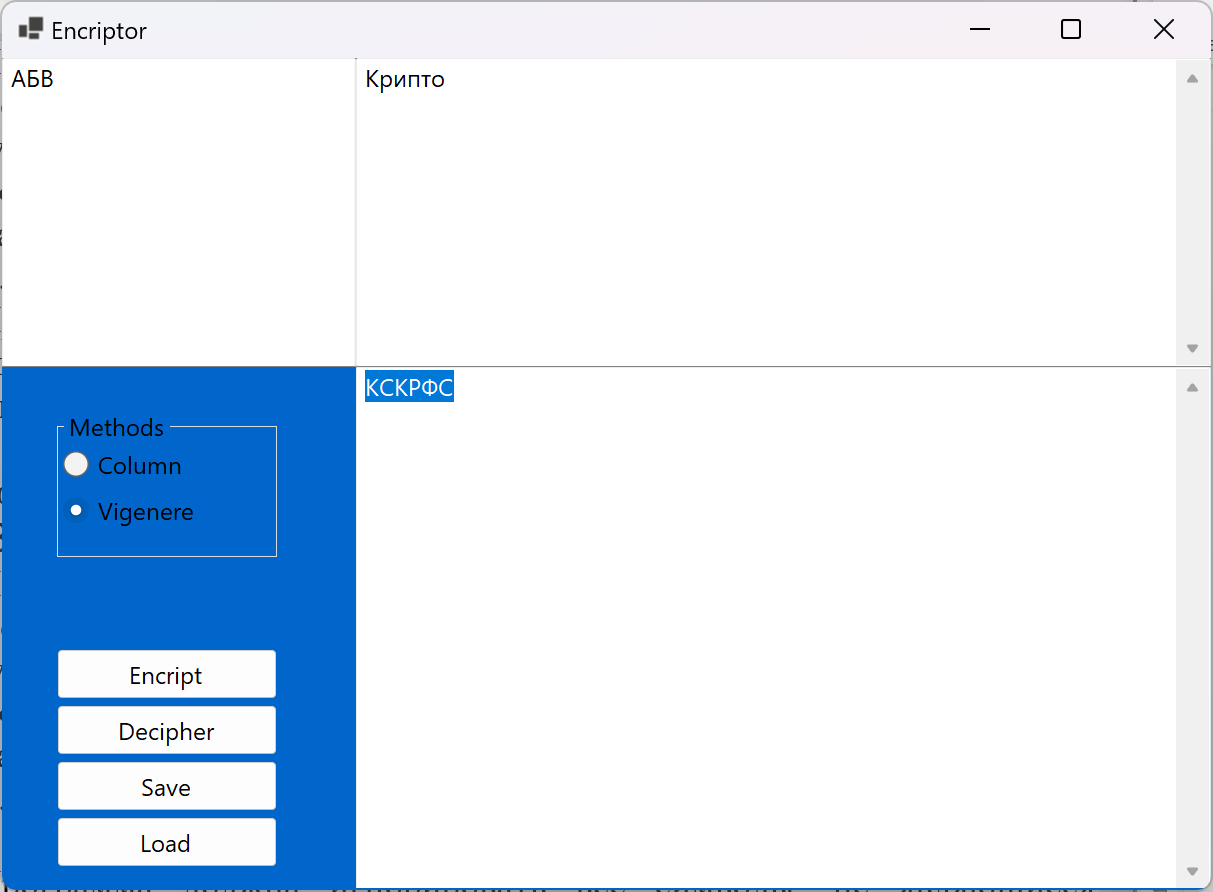
Операция: шифрование

Таблица:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| К | Р | И | П | Т | О |
| А | Б | В | Б | В | Г |
| К | С | К | Р | Ф | С |

Шифротекст: КСКРФС

Скриншот:



Тест 2

Тестовая ситуация: проверка коректности прогрессивного ключа

Исходный текст: Павлюченко

Ключ: асик

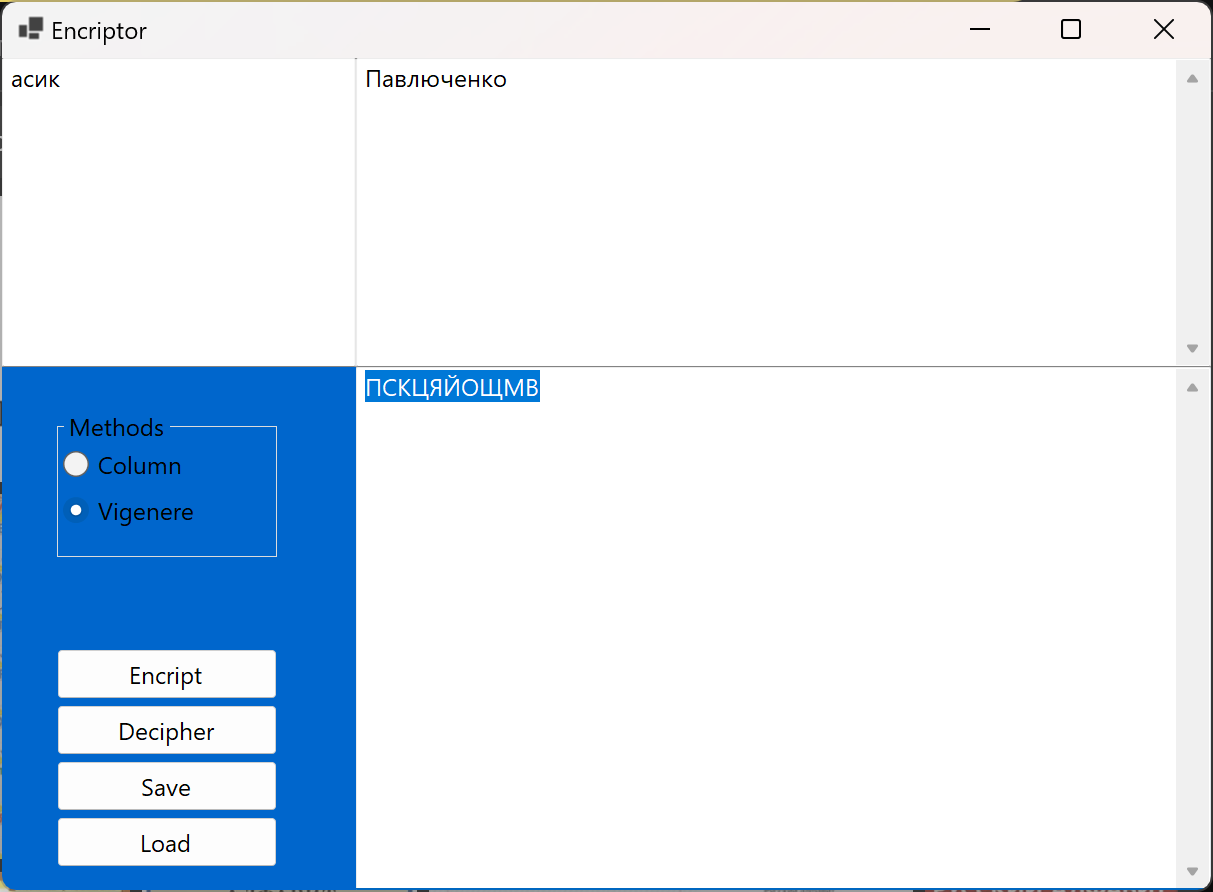
Операция: шифрование

Таблица:

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| П | а | в | л | ю | ч | е | н | к | о |
| а | с | и | к | б | т | й | л | в | у |
| П | С | К | Ц | Я | Й | О | Щ | М | В |

Шифротекст: ПСКЦЯЙОЩМВ

Скриншот:



Тест 3

Тестовая ситуация: проверка корректности шифрования при ключе больше текста

Исходный текст: Отец

Ключ: Родитель

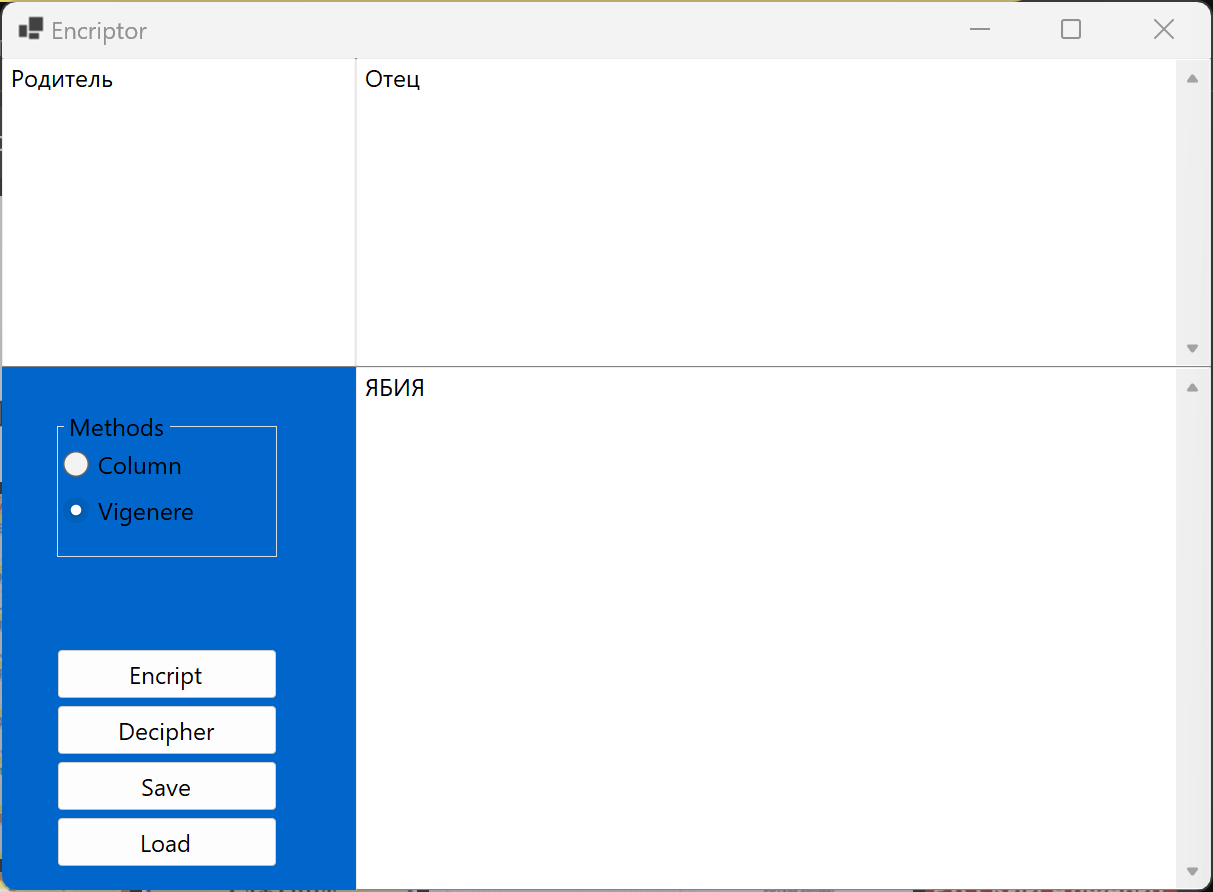
Операция: шифрование

Таблица:

|  |  |  |  |
| --- | --- | --- | --- |
| О | т | е | ц |
| Р | о | д | и |
| Я | Б | И | Я |

Шифротекст: ЯБИЯ

Скриншот:



Тест 4

Тестовая ситуация: проверка корректности дешифрирования

Исходный текст: ПСКЦЯЙОЩМВ

Ключ: асик

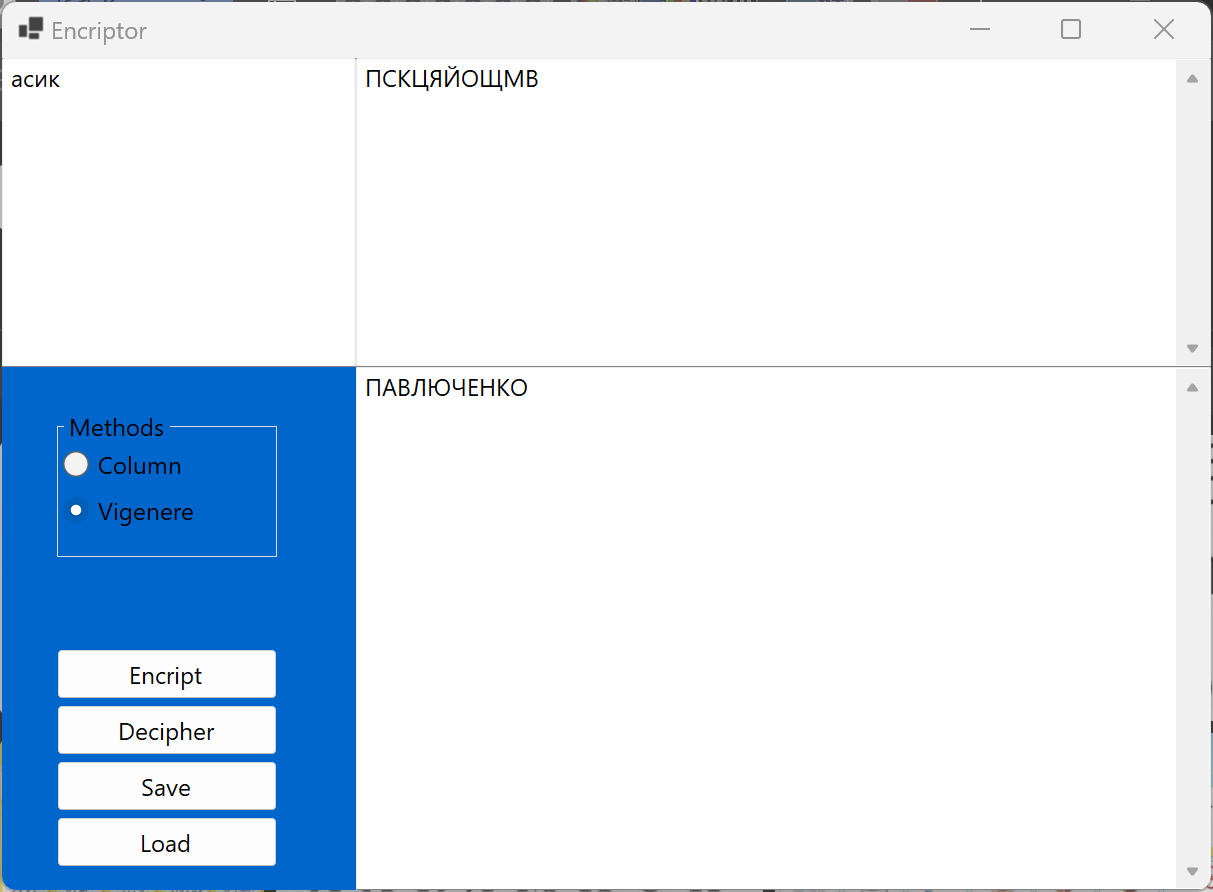
Операция: дешифрование

Таблица:

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| П | С | К | Ц | Я | Й | О | Щ | М | В |
| а | с | и | к | б | т | й | л | в | у |
| П | А | В | Л | Ю | Ч | Е | Н | К | О |

Шифротекст: ПАВЛЮЧЕНКО

Скриншот:



Тестовый набор 2(проверка корректной работы на невалидных данных)

Тест 1

Тестовая ситуация: проверка корректности результата при пустом ключе.

Исходный текст: Самолёт

Ключ:

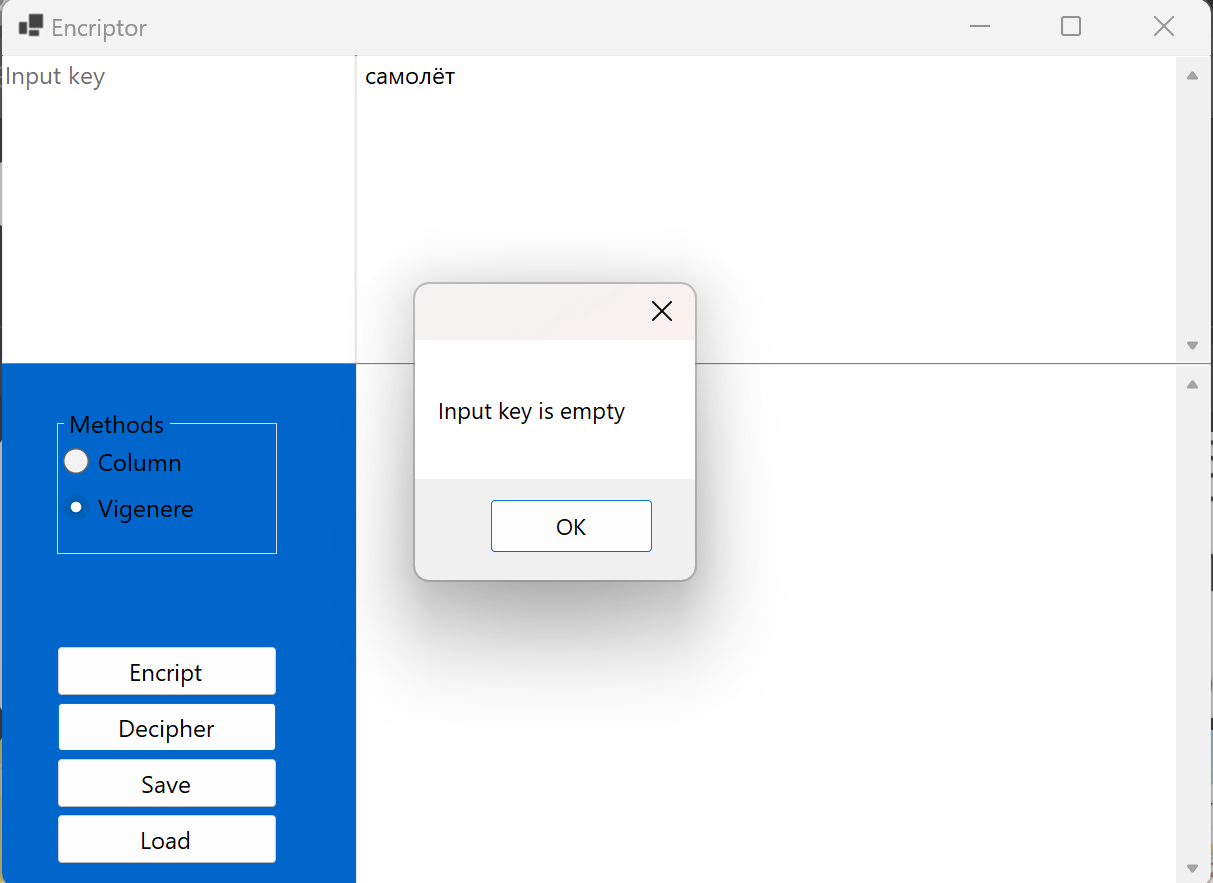
Операция: шифрование

Таблица:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| С | а | м | о | л | ё | т |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

Результат: вывод о невалидности данных

Скриншот:



Тест 2

Тестовая ситуация: наличие невалидных символов.

Исходный текст: Заме21123чател2133ьный

Ключ: окнGASJDhfsо

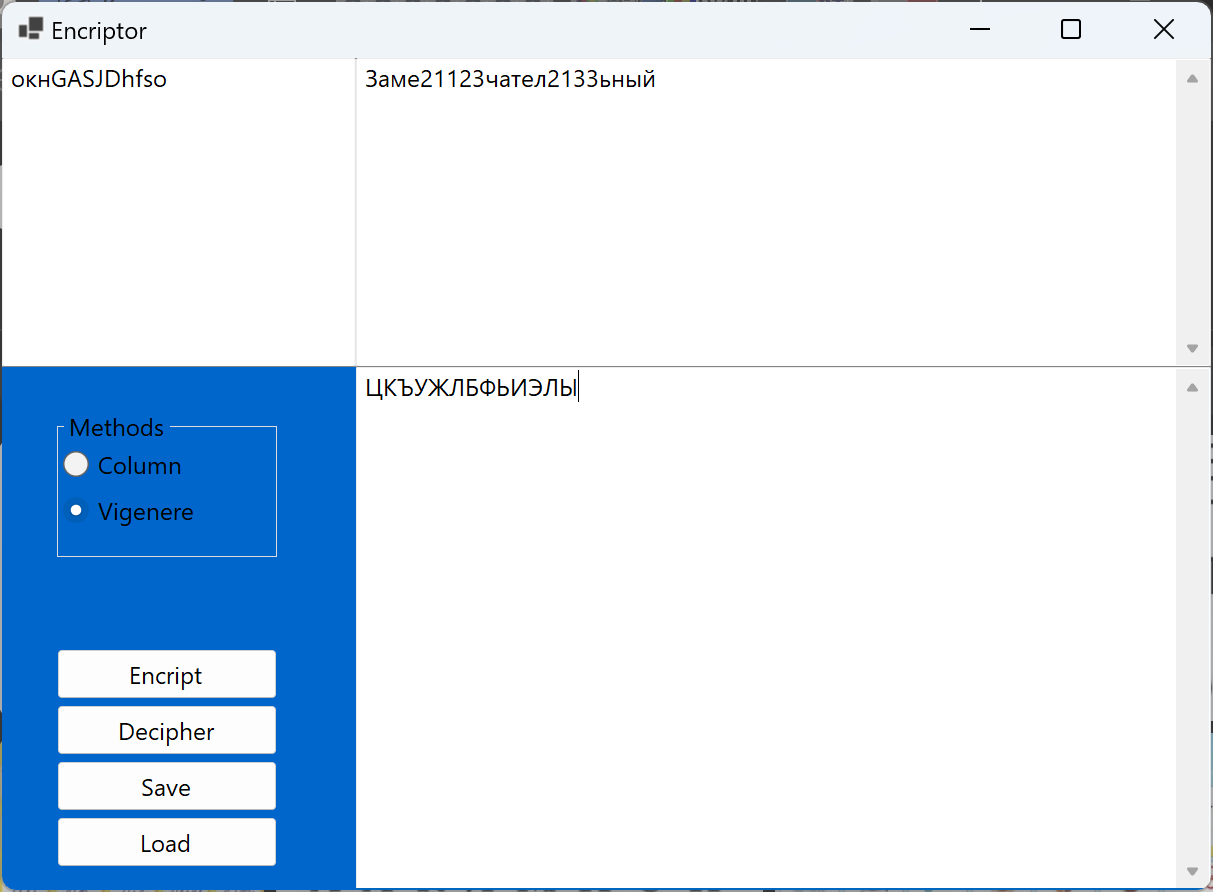
Операция: шифрование

Таблица:

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| З | а | м | е | ч | а | т | е | л | ь | н | ы | й |
| о | к | н | о | п | л | о | п | р | м | п | р | с |
| Ц | к | ъ | у | ж | л | б | ф | ь | и | э | л | ы |

Шифротекст: ЦКЪУЖЛБФЬИЭЛЫ

Скриншот:



Тест 3

Тестовая ситуация: проверка корректности шифрования с буквой ё

Исходный текст: Ёжик

Ключ: АЁЕЁ

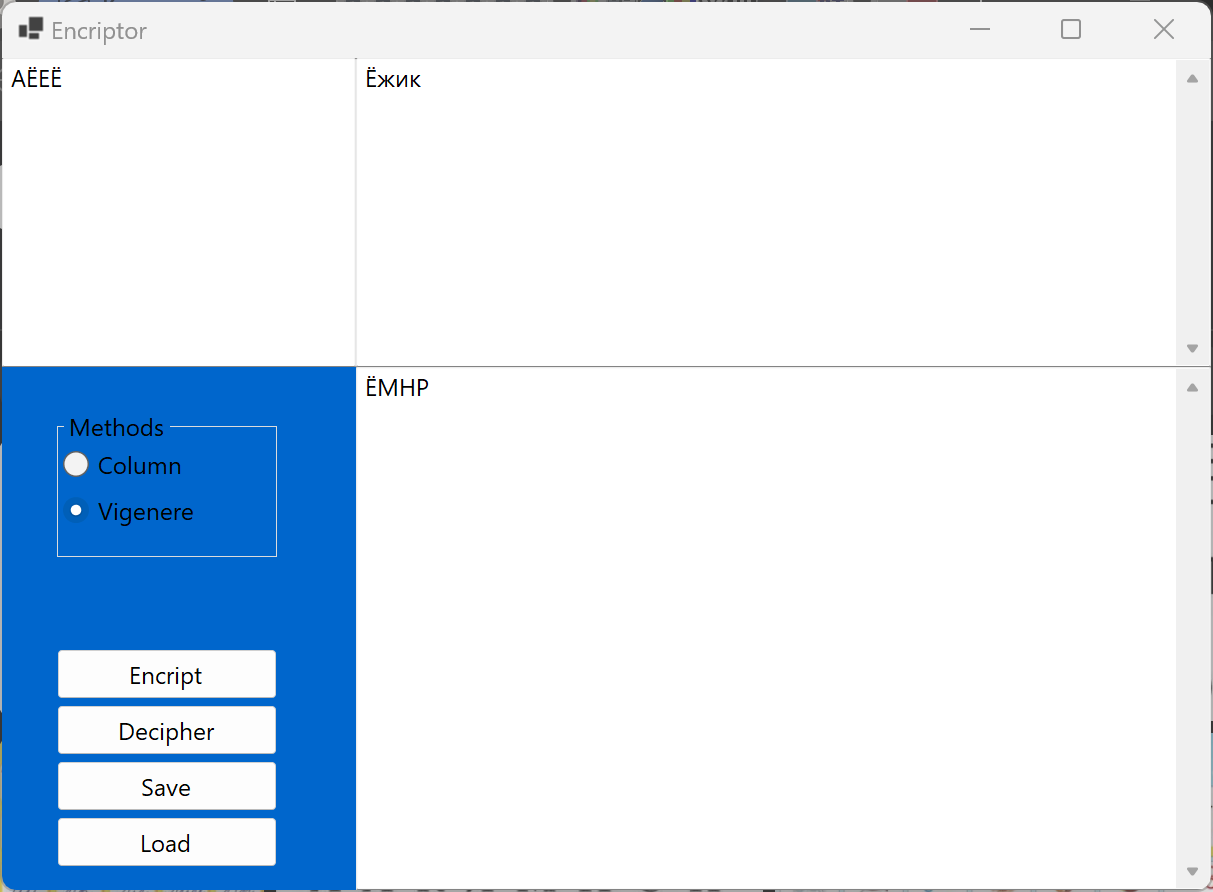
Операция: шифрование

Таблица:

|  |  |  |  |
| --- | --- | --- | --- |
| Ё | ж | и | к |
| А | Ё | Е | Ё |
| Ё | М | Н | Р |

Шифротекст: ЁМНР

Скрин:



**Шифр Столбцы**

Тестовый набор 1(проверка корректной работы на валидных данных)

Тест 1

Тестовая ситуация: проверка корректности шифрования случайной фразы, неполное заполнение.

Тестовая фраза: Windows

Ключ: OS

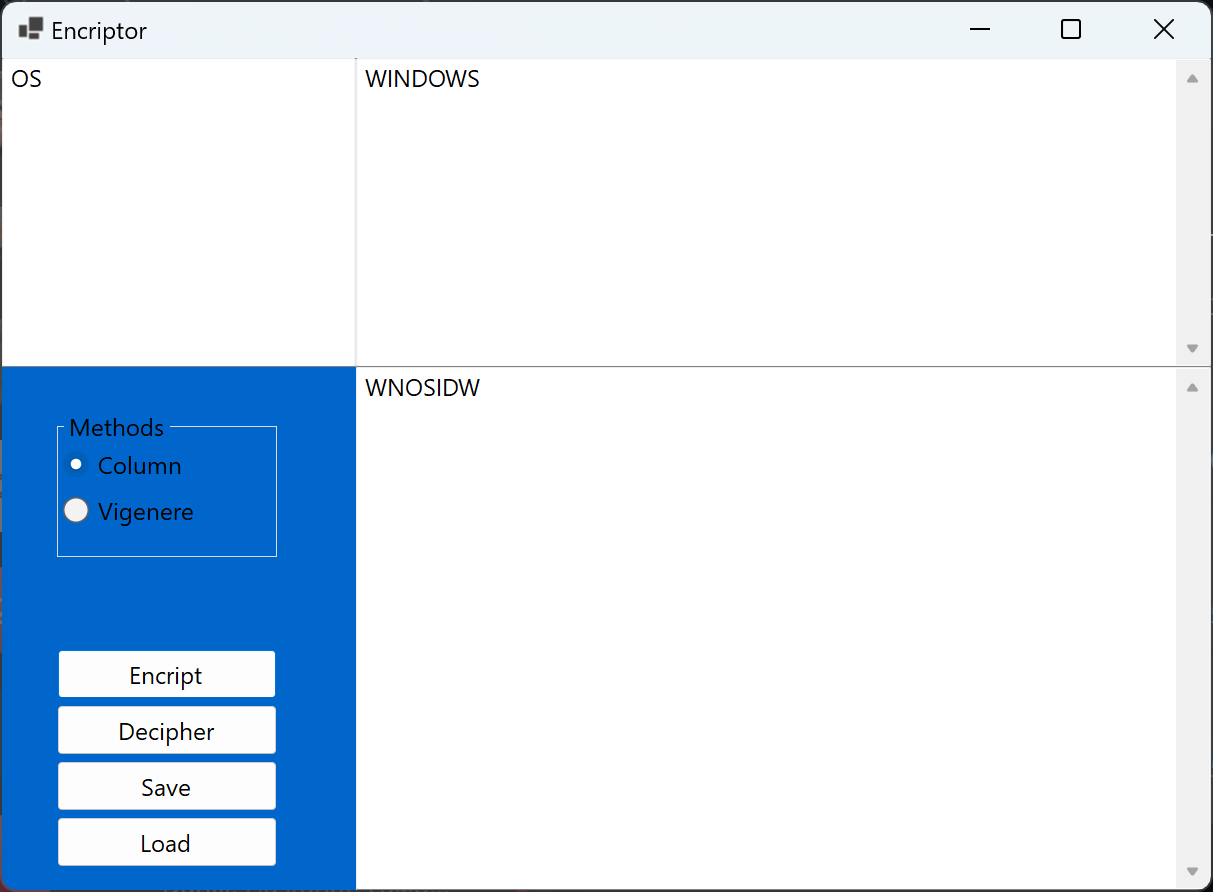
Операция: шифрование

Таблица:

|  |  |
| --- | --- |
| O | S |
| 1 | 2 |
| W | I |
| N | D |
| O | W |
| S |  |

Шифротекст: WNOSIDW

Скриншот:



Тест 2

Тестовая ситуация: проверка корректности шифрования случайной фразы, полное заполнение.

Исходный текст: Crazy night

Ключ: da

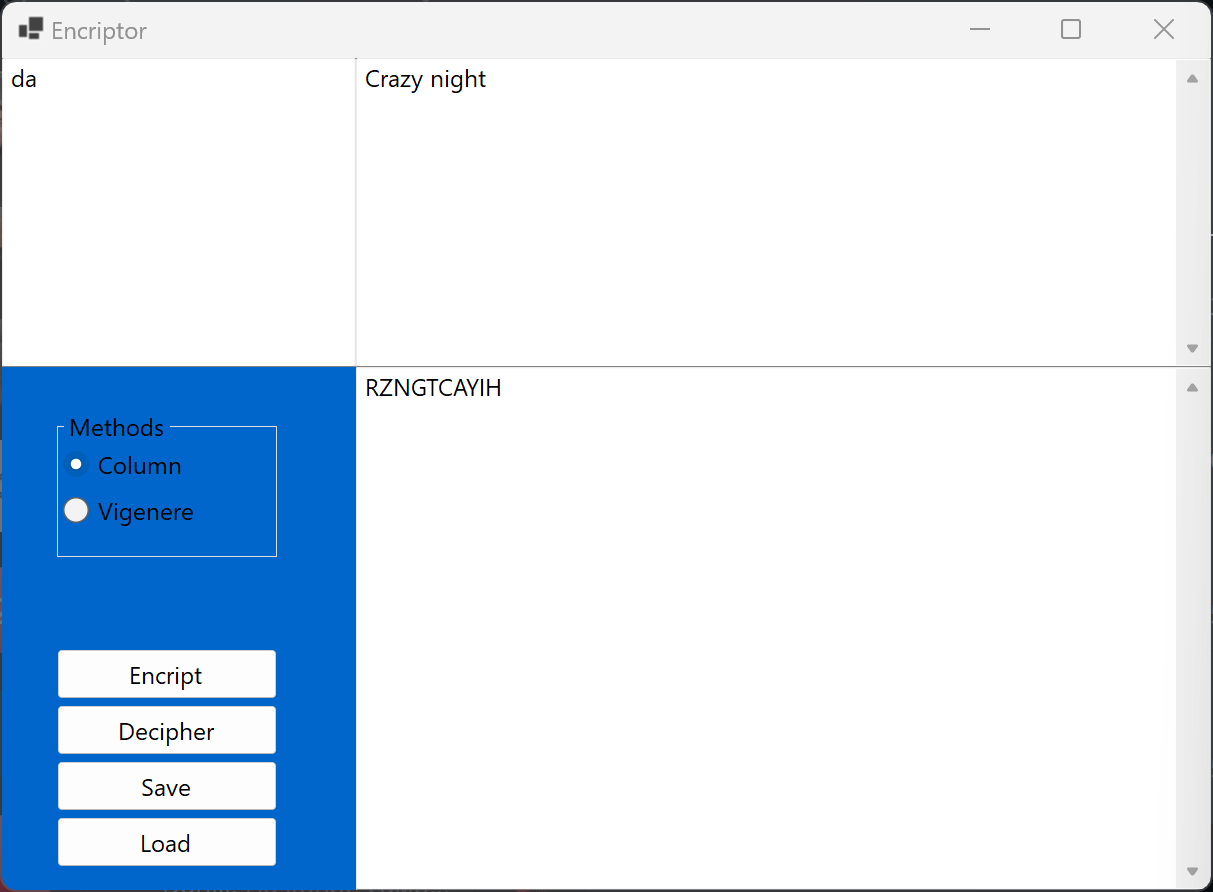
Операция: шифрование

Таблица:

|  |  |
| --- | --- |
| d | a |
| 2 | 1 |
| c | R |
| a | z |
| y | n |
| i | g |
| h | t |

Шифротекст: RZNGTCAYIH

Скриншот:



Тест 3

Тестовая ситуация: проверка корректности дешифрования случайной фразы, неполное заполнение

Исходный текст: WNOSIDW

Ключ: OS

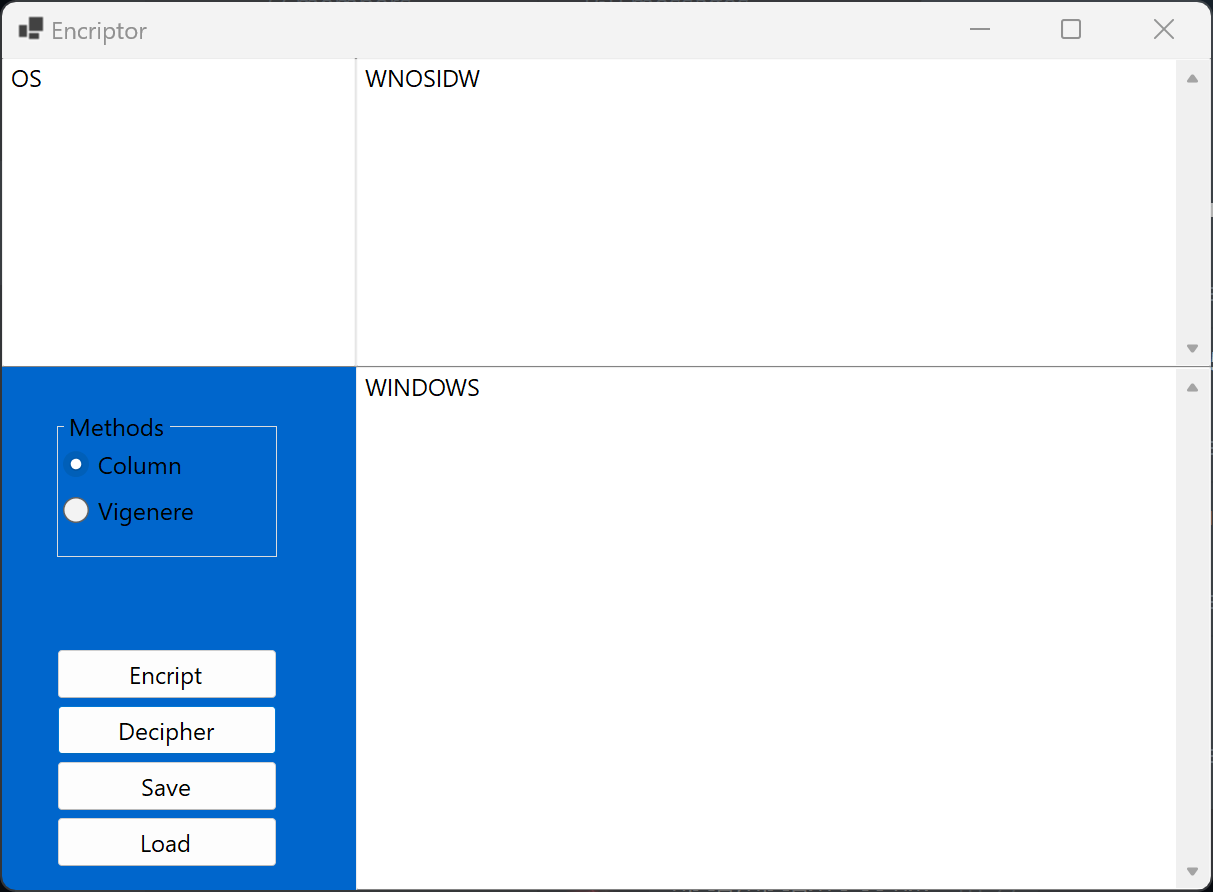
Операция: дешифрование

Таблица:

|  |  |
| --- | --- |
| O | S |
| 1 | 2 |
| W | I |
| N | D |
| O | W |
| S |  |

Полученная фраза: WINDOWS

Скриншот:



Тест 4

Тестовая ситуация: проверка корректности дешифрования случайной фразы, полное заполнение

Исходный текст: RZNGTCAYIH

Ключ: da

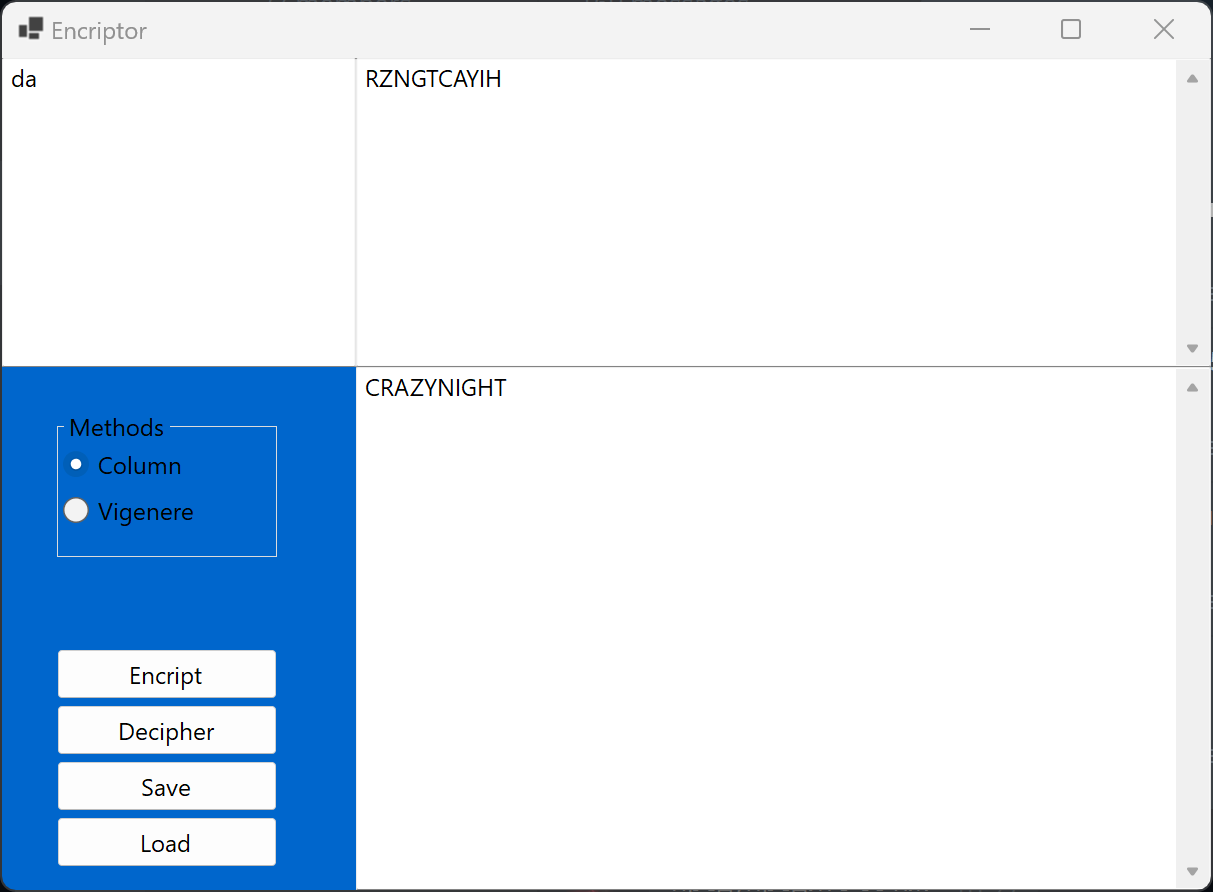
Операция: дешифрование

Таблица:

|  |  |
| --- | --- |
| d | a |
| 2 | 1 |
| c | R |
| a | z |
| y | n |
| i | g |

Полученная фраза: CRAZYNIGHT

Скриншот:



Тестовый набор 2(проверка корректной работы на невалидных данных)

Тест 1

Тестовая ситуация: проверка корректности результата при пустом ключе.

Исходный текст: RANDOMTEXT

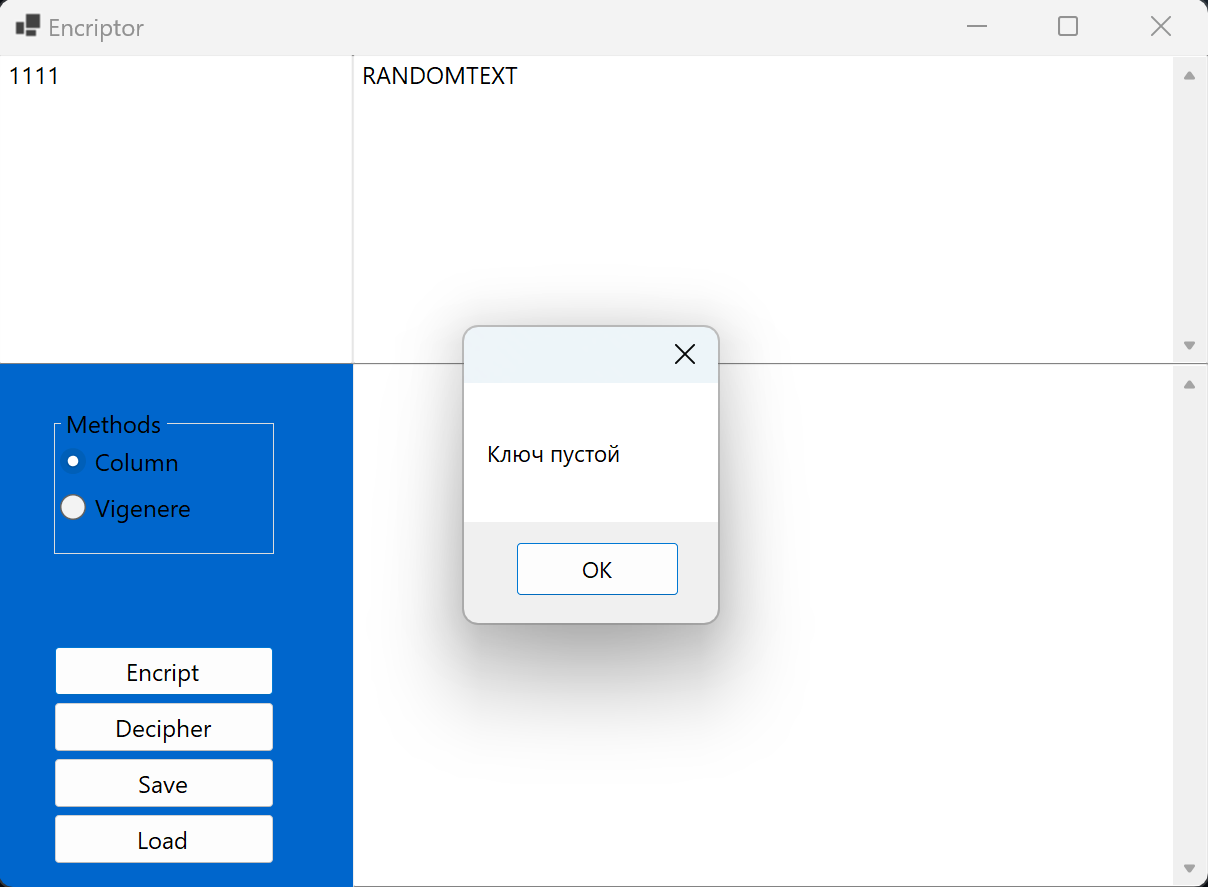
Ключ: 1111

Операция: дешифрование

Таблица: отсутствует

Результат: вывод о невалидности ключа.

Скриншот:



Тест 2

Тестовая ситуация: наличие невалидных символов.

Тестовая фраза: TO231HAVEырвA6644CURSE

Ключ: Z\_\_E\_\_L\_\_D\_\_A

Операция: шифрование

Таблица:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| z | e | l | d | a |
| 5 | 4 | 3 | 2 | 1 |
| t | o | h | a | v |
| e | a | c | u | r |
| s | e |  |  |  |

Шифротекст: VRAUOAEHCTES

Скриншот:

