Столбов Кирилл

**ЛАБОРАТОРНАЯ РАБОТА №1**

Перестановочные и подстановочные алгоритмы

шифрования

**ТЕКСТ ЗАДАНИЯ**

(Вариант №11)

1. Шифр Плейфейра с 4мя шифрующими таблицами, текст на английском языке;
2. Алгоритм Виженера, прямой ключ, текст на русском языке.

**ТЕСТИРОВАНИЕ ПРОГРАММЫ**

Шифр Плейфейра с 4мя шифрующими таблицами

***Дымовое тестирование.***

Тестовая фраза: CANDLйE-э

Ключевые слова:

1) JACK

2) BOOMER

3) CARDS

4) PROGRAMMER

Таблицы шифрования:

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| I/J | A | C | K | B |  | B | O | M | E | R |
| D | E | F | G | H |  | A | C | D | F | G |
| L | M | N | O | P |  | H | I/J | K | L | N |
| Q | R | S | T | U |  | P | Q | S | T | U |
| V | W | X | Y | Z |  | V | W | X | Y | Z |
|  |  |  |  |  |  |  |  |  |  |  |
| C | A | R | D | S |  | P | R | O | G | A |
| B | E | F | G | H |  | M | E | B | C | D |
| I/J | K | L | M | N |  | F | H | I/J | K | L |
| O | P | Q | T | U |  | N | Q | S | T | U |
| V | W | X | Y | Z |  | V | W | X | Y | Z |

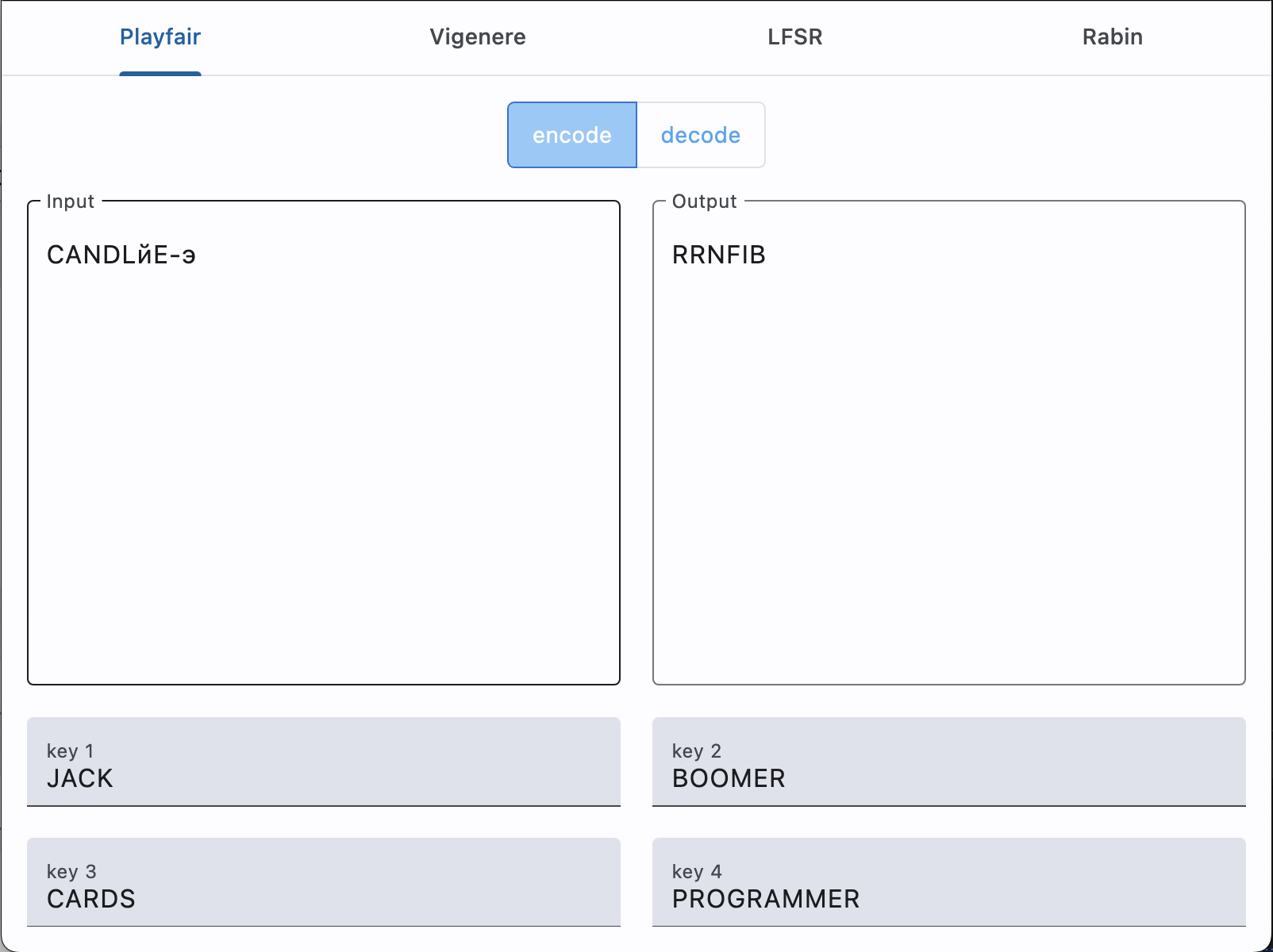
Преобразованная фраза: CANDLE

CA | ND | LE

RR | NF | IB

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| I/J | A | C | K | B |  | B | O | M | E | R |
| D | E | F | G | H |  | A | C | D | F | G |
| L | M | N | O | P |  | H | I/J | K | L | N |
| Q | R | S | T | U |  | P | Q | S | T | U |
| V | W | X | Y | Z |  | V | W | X | Y | Z |
|  |  |  |  |  |  |  |  |  |  |  |
| C | A | R | D | S |  | P | R | O | G | A |
| B | E | F | G | H |  | M | E | B | C | D |
| I/J | K | L | M | N |  | F | H | I/J | K | L |
| O | P | Q | T | U |  | N | Q | S | T | U |
| V | W | X | Y | Z |  | V | W | X | Y | Z |

Полученный шифротекст: RRNFIB

Результат работы программы: 

***Ломаем на валидных данных.***

Тестовая фраза: ЪHER»ЬE IS JON--NY

Ключевые слова:

1) MOON:)

2) TEXT

3) ASUS

4) PROCESS

Таблицы шифрования:

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| M | O | N | A | B |  | T | E | X | A | B |
| C | D | E | F | G |  | C | D | F | G | H |
| H | I/J | K | L | P |  | I/J | K | L | M | N |
| Q | R | S | T | U |  | O | P | Q | R | S |
| V | W | X | Y | Z |  | U | V | W | Y | Z |
|  |  |  |  |  |  |  |  |  |  |  |
| A | S | U | B | C |  | P | R | O | C | E |
| D | E | F | G | H |  | S | A | B | D | F |
| I/J | K | L | M | N |  | G | H | I/J | K | L |
| O | P | Q | R | T |  | M | N | Q | T | U |
| V | W | X | Y | Z |  | V | W | X | Y | Z |

Преобразованная фраза: HEREISJONNYX

HE | RE | IS | JO | NN | YX

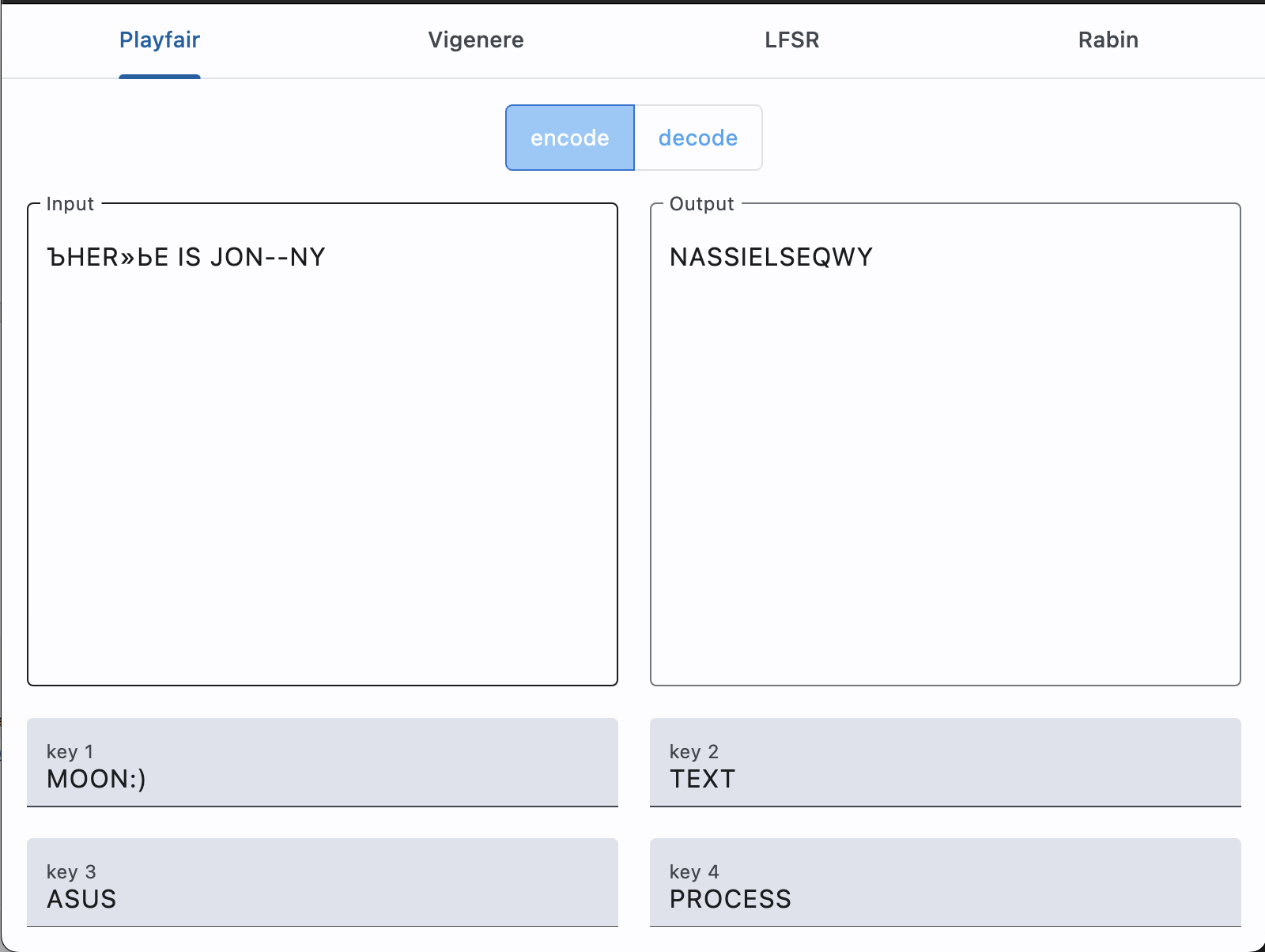
NA | SS | IE | LS | EQ | WY

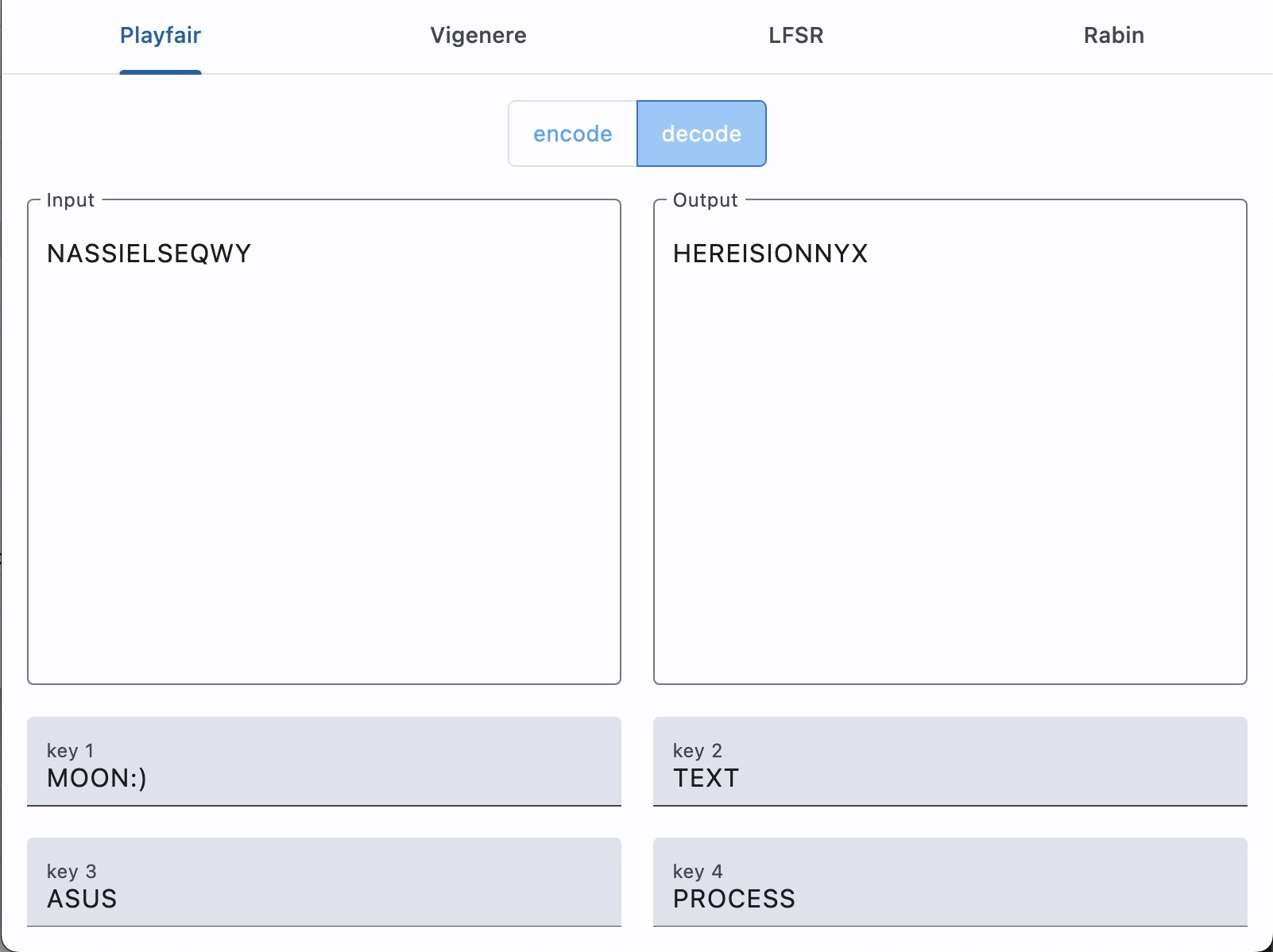
|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| M | O | N | A | B |  | T | E | X | A | B |
| C | D | E | F | G |  | C | D | F | G | H |
| H | I/J | K | L | P |  | I/J | K | L | M | N |
| Q | R | S | T | U |  | O | P | Q | R | S |
| V | W | X | Y | Z |  | U | V | W | Y | Z |
|  |  |  |  |  |  |  |  |  |  |  |
| A | S | U | B | C |  | P | R | O | C | E |
| D | E | F | G | H |  | S | A | B | D | F |
| I/J | K | L | M | N |  | G | H | I/J | K | L |
| O | P | Q | R | T |  | M | N | Q | T | U |
| V | W | X | Y | Z |  | V | W | X | Y | Z |

и т.д.

Полученный шифротекст: NASSIELSEQWY

Результат работы программы:





Тестовая фраза: IJIJJJX

Ключевые слова:

1) фыр-фыр

2) <пустая строка>

3) ASUS

4) JACK

Таблицы шифрования:

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| A | B | C | D | E |  | A | B | C | D | E |
| F | G | H | I/J | K |  | F | G | H | I/J | K |
| L | M | N | O | P |  | L | M | N | O | P |
| Q | R | S | T | U |  | Q | R | S | T | U |
| V | W | X | Y | Z |  | V | W | X | Y | Z |
|  |  |  |  |  |  |  |  |  |  |  |
| A | S | U | B | C |  | I/J | A | C | K | B |
| D | E | F | G | H |  | D | E | F | G | H |
| I/J | K | L | M | N |  | L | M | N | O | P |
| O | P | Q | R | T |  | Q | R | S | T | U |
| V | W | X | Y | Z |  | V | W | X | Y | Z |

Преобразованная фраза: IJIJJJXX

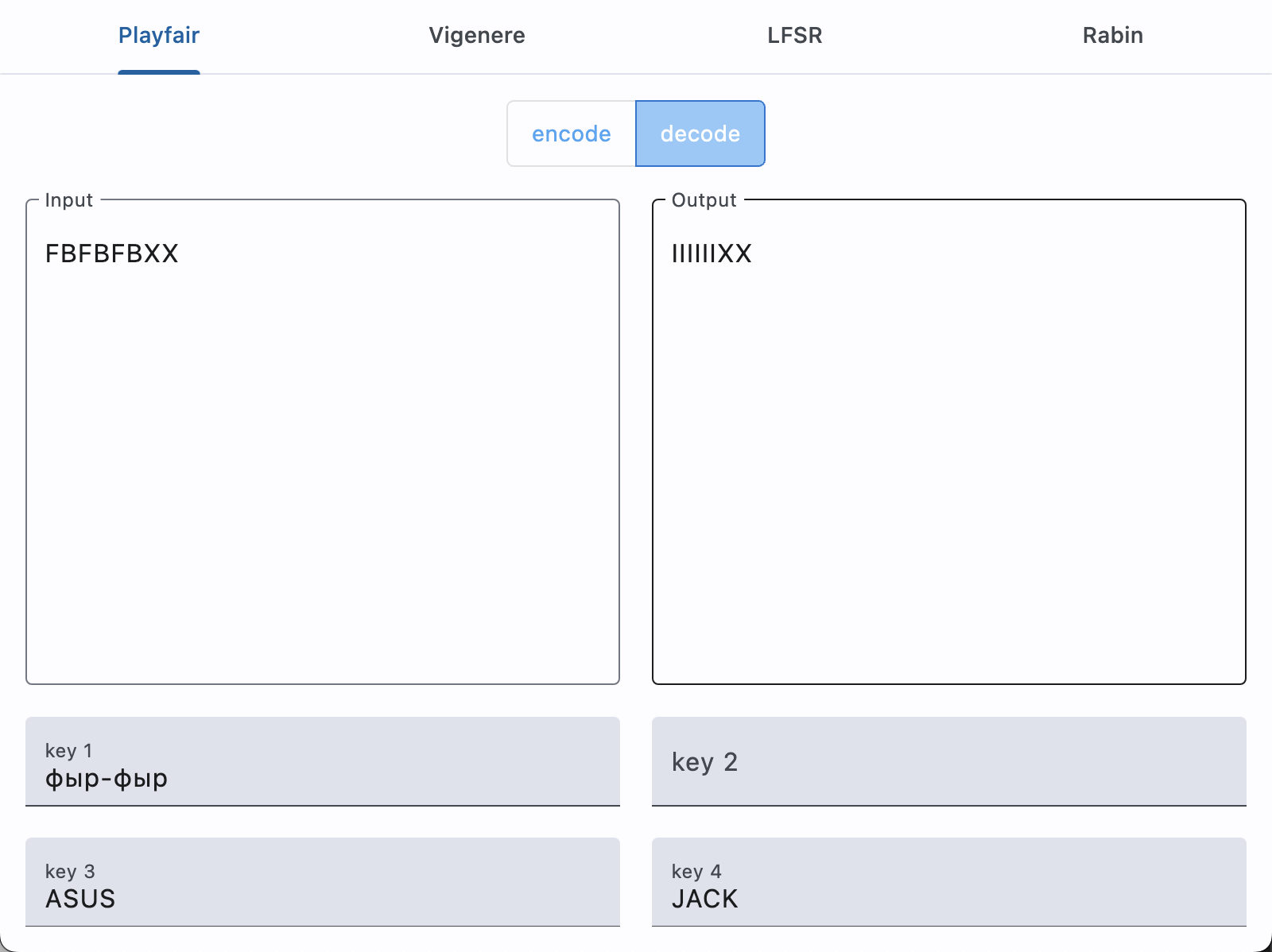
IJ | IJ | JJ | XX

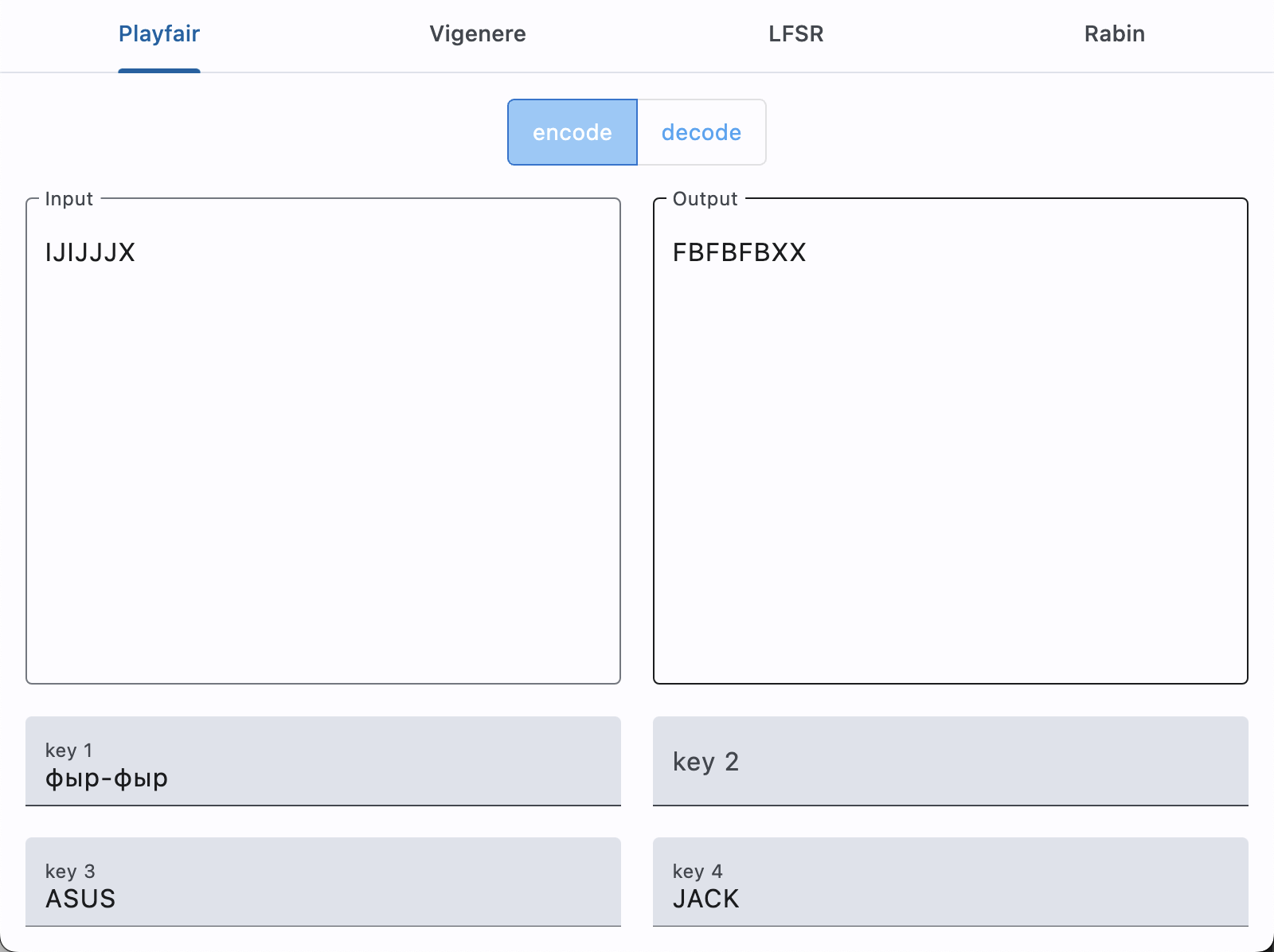
FB | FB | FB | XX

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| A | B | C | D | E |  | A | B | C | D | E |
| F | G | H | I/J | K |  | F | G | H | I/J | K |
| L | M | N | O | P |  | L | M | N | O | P |
| Q | R | S | T | U |  | Q | R | S | T | U |
| V | W | X | Y | Z |  | V | W | X | Y | Z |
|  |  |  |  |  |  |  |  |  |  |  |
| A | S | U | B | C |  | I/J | A | C | K | B |
| D | E | F | G | H |  | D | E | F | G | H |
| I/J | K | L | M | N |  | L | M | N | O | P |
| O | P | Q | R | T |  | Q | R | S | T | U |
| V | W | X | Y | Z |  | V | W | X | Y | Z |

Полученный шифротекст: FBFBFBXX

Результат работы программы:





***Ломаем на невалидных данных.***

Тестовая фраза: абвгдеё

Ключевые слова:

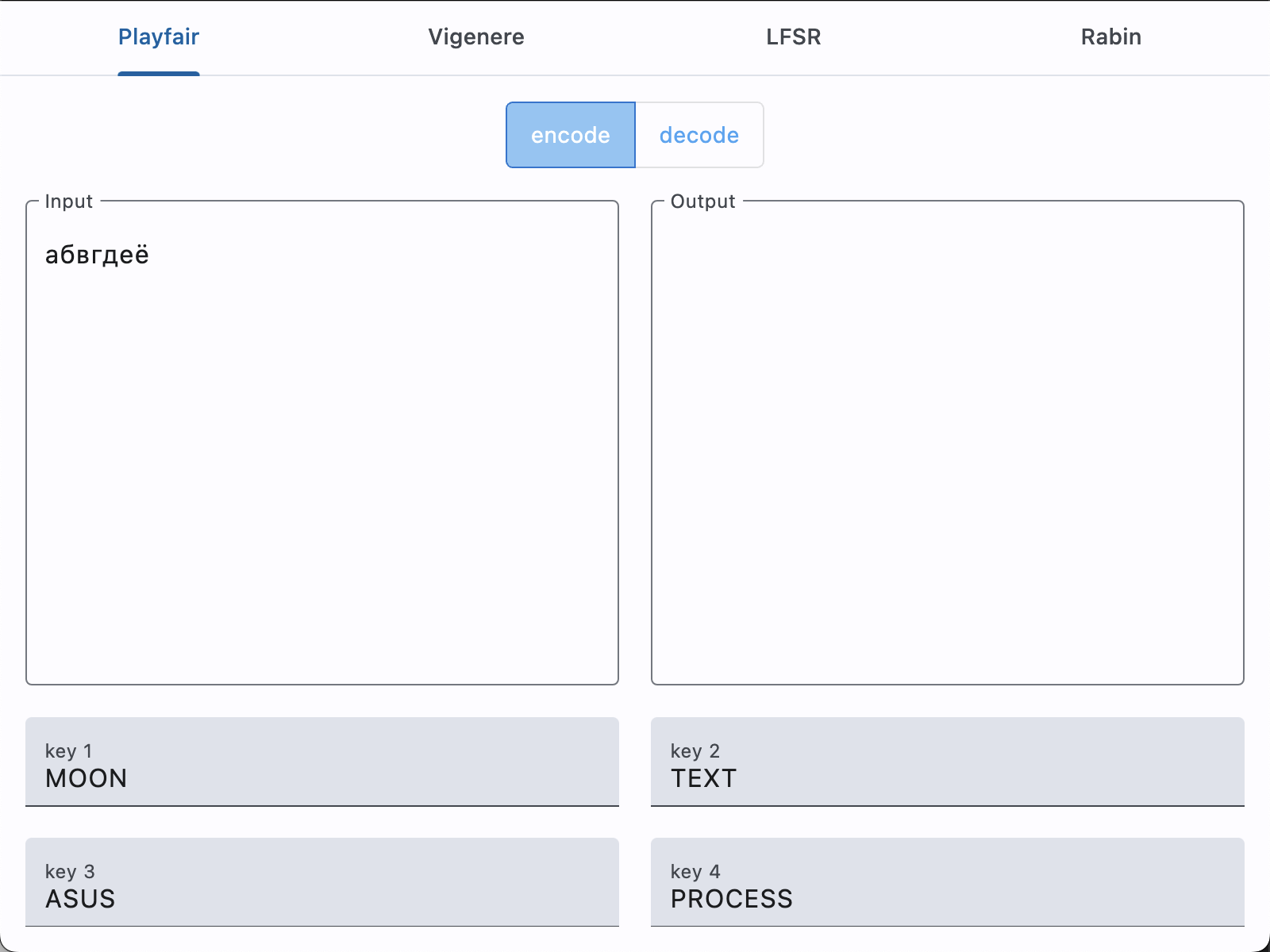
1) MOON

2) TEXT

3) ASUS

4) PROCESS

Результат работы программы:



Тестовая фраза: <пустая строка>

Ключевые слова:

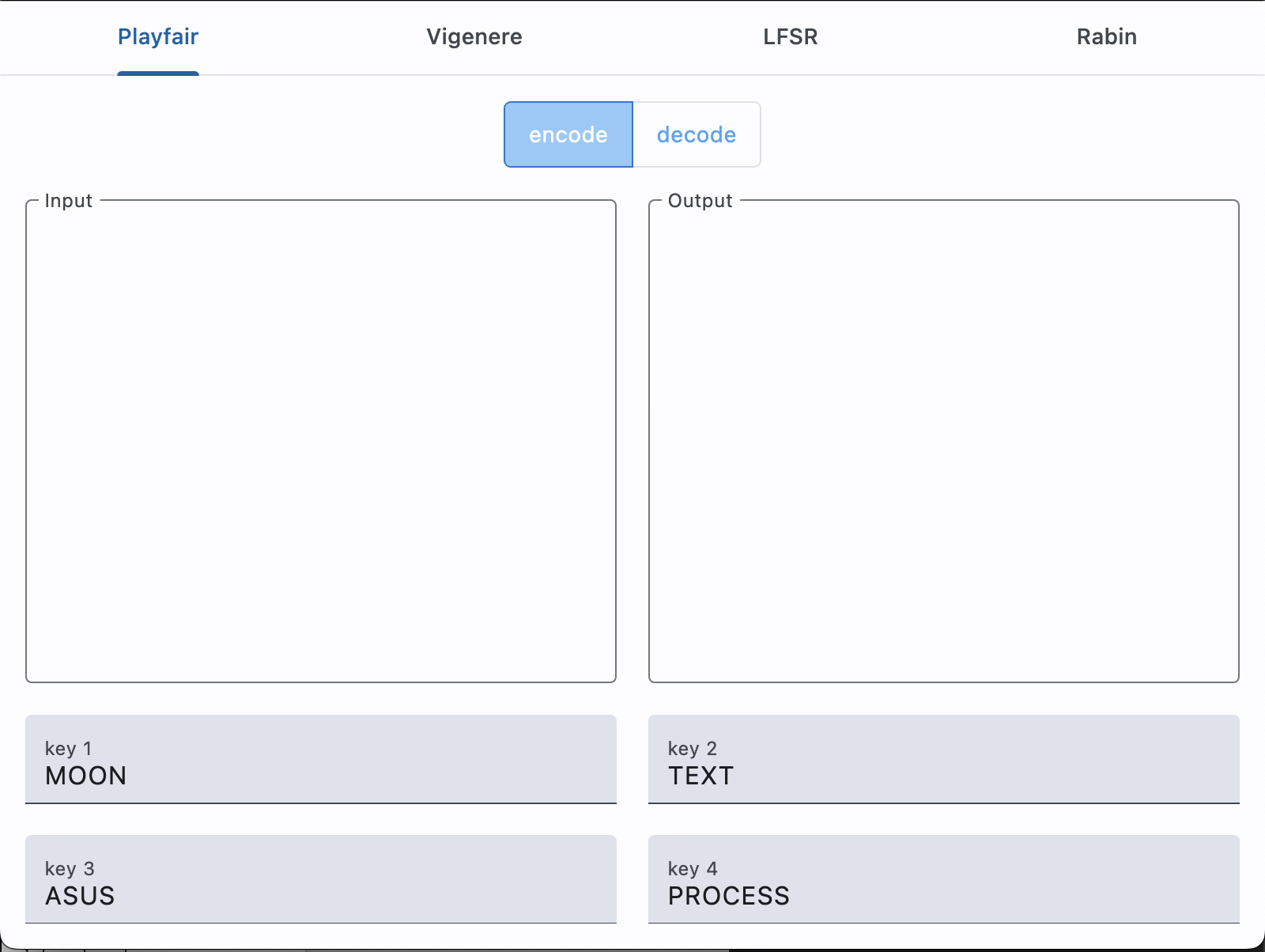
1) MOON

2) TEXT

3) ASUS

4) PROCESS

Результат работы программы:



Алгоритм Виженера, прямой ключ

***Дымовое тестирование.***

Тестовая фраза: jДАi БУДЕТ СВ-ЕТ

Ключевое слово: ЦИРК

Таблицы подстановки:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **А** | **Б** | **В** | **Г** | **Д** | **Е** | **Ё** | **Ж** | **З** | **И** | **Й** | **К** | **Л** | **М** | **Н** | **О** | **П** |
| Ц | Ч | Ш | Щ | Ъ | Ы | Ь | Э | Ю | Я | А | Б | В | Г | Д | Е | Ё |
| И | Й | К | Л | М | Н | О | П | Р | С | Т | У | Ф | Х | Ц | Ч | Ш |
| Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ъ | Ы | Ь | Э | Ю | Я | А |
| К | Л | М | Н | О | П | Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ъ |

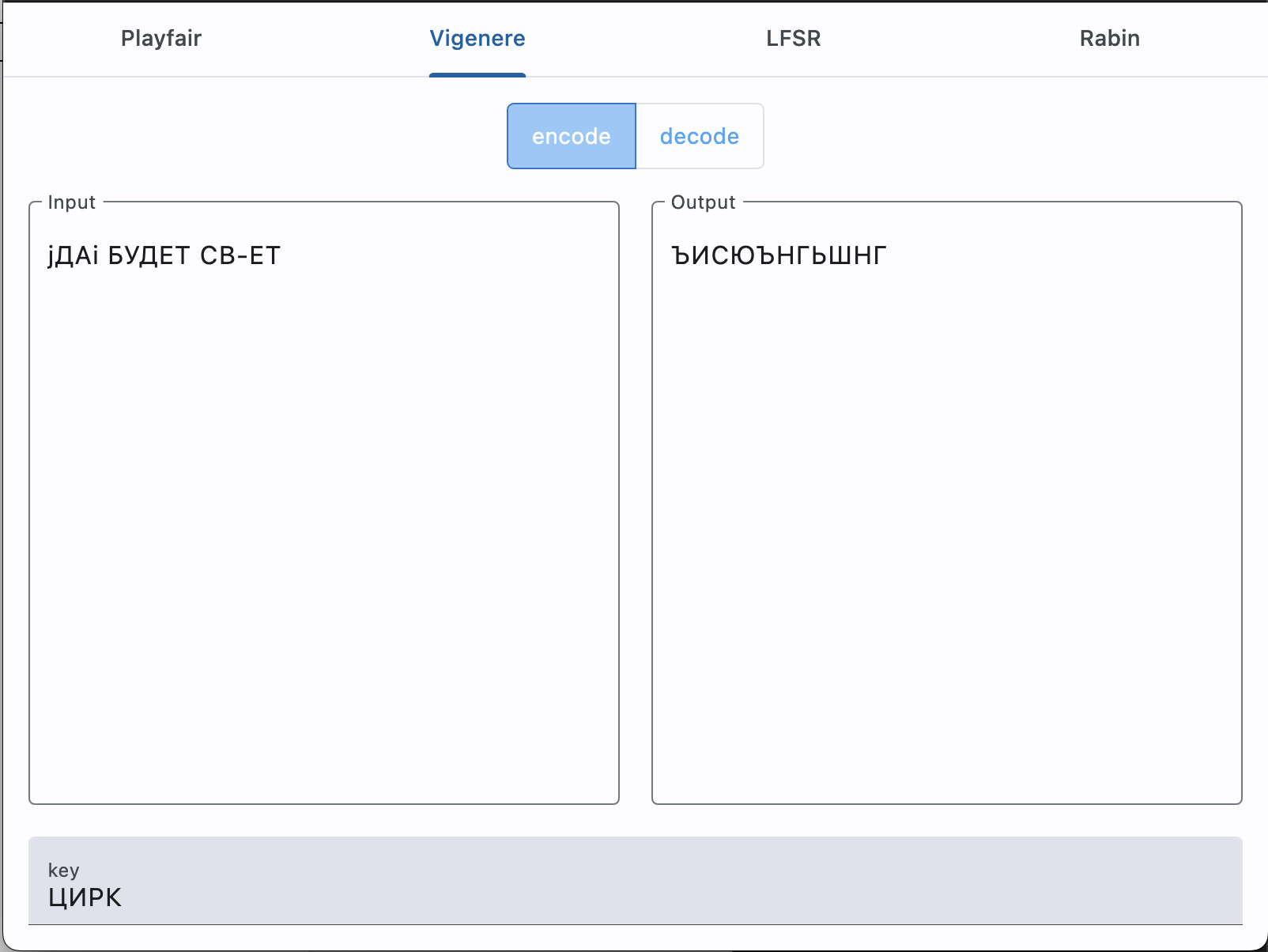
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Р** | **С** | **Т** | **У** | **Ф** | **Х** | **Ц** | **Ч** | **Ш** | **Щ** | **Ъ** | **Ы** | **Ь** | **Э** | **Ю** | **Я** |
| Ж | З | И | Й | К | Л | М | Н | О | П | Р | С | Т | У | Ф | Х |
| Щ | Ъ | Ы | Ь | Э | Ю | Я | А | Б | В | Г | Д | Е | Ё | Ж | З |
| Б | В | Г | Д | Е | Ё | Ж | З | И | Й | К | Л | М | Н | О | П |
| Ы | Ь | Э | Ю | Я | А | Б | В | Г | Д | Е | Ё | Ж | З | И | Й |

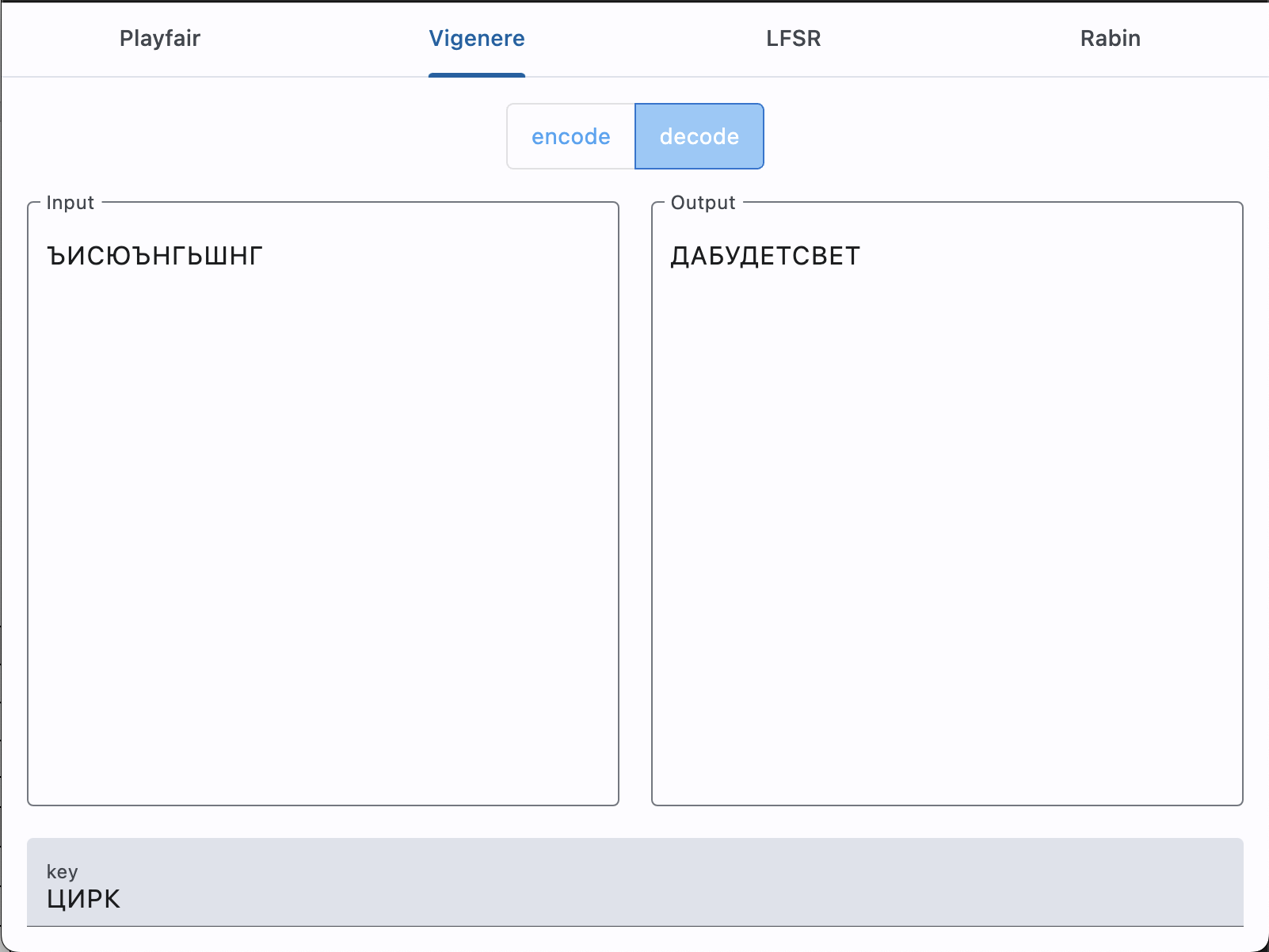
Преобразованная фраза: ДА БУДЕТ СВЕТ

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *М* ***=*** | **Д** | **А** | **Б** | **У** | **Д** | **Е** | **Т** | **С** | **В** | **Е** | **Т** |
| *К* ***=*** | **Ц** | **И** | **Р** | **К** | **Ц** | **И** | **Р** | **К** | **Ц** | **И** | **Р** |
| *С =* | Ъ | И | С | Ю | Ъ | Н | Г | Ь | Ш | Н | Г |

Полученный шифротекст: ЪИ СЮЪНГ ЬШНГ

Результат работы программы:





***Ломаем на валидных данных.***

Тестовая фраза: Ё-Ж]ИК В ТУМАНЕ

Ключевое слово: МЁД

Таблицы подстановки:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **А** | **Б** | **В** | **Г** | **Д** | **Е** | **Ё** | **Ж** | **З** | **И** | **Й** | **К** | **Л** | **М** | **Н** | **О** | **П** |
| М | Н | О | П | Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ъ | Ы | Ь |
| Ё | Ж | З | И | Й | К | Л | М | Н | О | П | Р | С | Т | У | Ф | Х |
| Д | Е | Ё | Ж | З | И | Й | К | Л | М | Н | О | П | Р | С | Т | У |

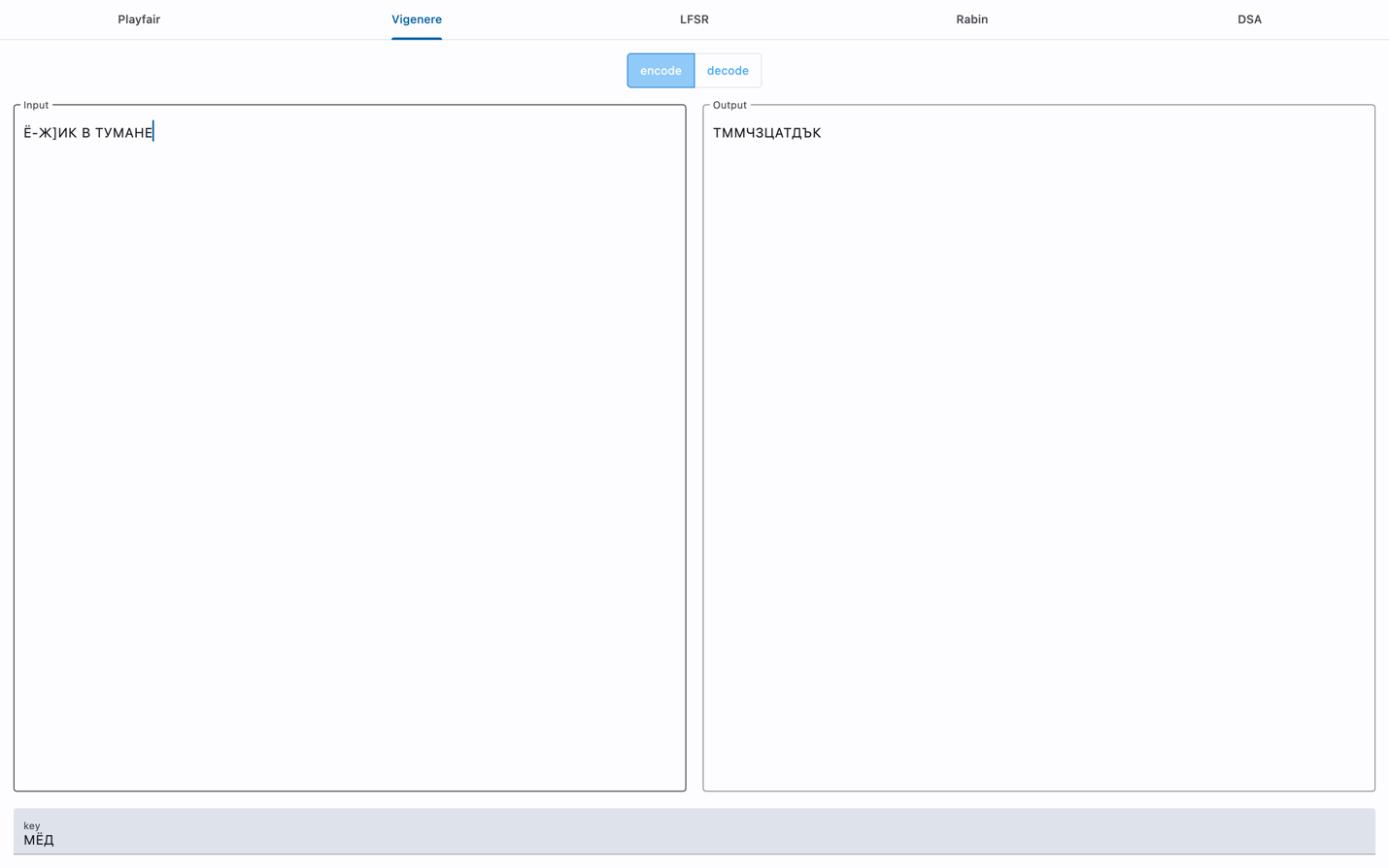
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Р** | **С** | **Т** | **У** | **Ф** | **Х** | **Ц** | **Ч** | **Ш** | **Щ** | **Ъ** | **Ы** | **Ь** | **Э** | **Ю** | **Я** |
| Э | Ю | Я | А | Б | В | Г | Д | Е | Ё | Ж | З | И | Й | К | Л |
| Ц | Ч | Ш | Щ | Ъ | Ы | Ь | Э | Ю | Я | А | Б | В | Г | Д | Е |
| Ф | Х | Ц | Ч | Ш | Щ | Ъ | Ы | Ь | Э | Ю | Я | А | Б | В | Г |

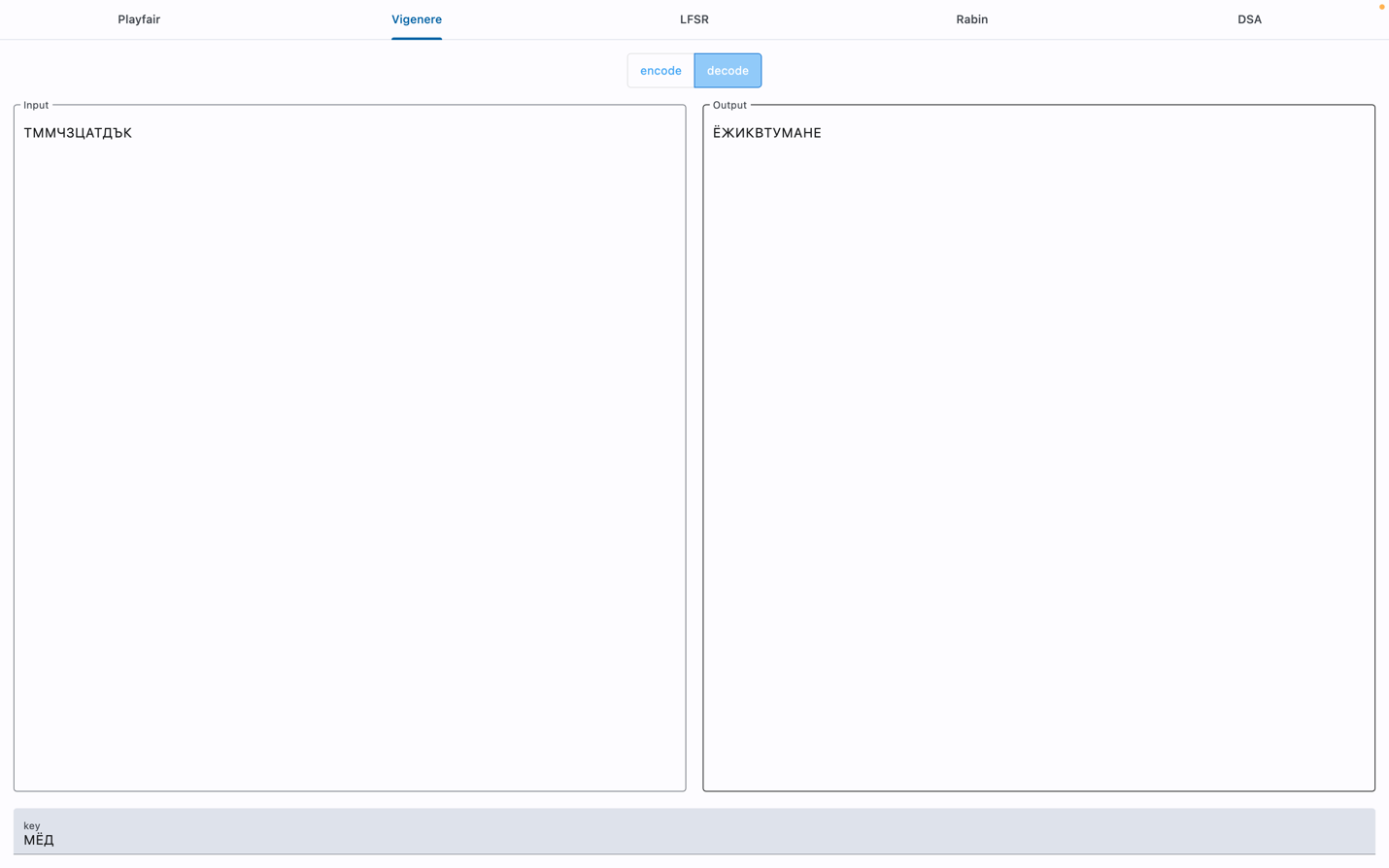
Преобразованная фраза: ЁЖИК В ТУМАНЕ

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *М* ***=*** | **Ё** | **Ж** | **И** | **К** | **В** | **Т** | **У** | **М** | **А** | **Н** | **Е** |
| *К* ***=*** | **М** | **Ё** | **Д** | **М** | **Ё** | **Д** | **М** | **Ё** | **Д** | **М** | **Ё** |
| *С =* | Т | М | М | Ч | З | Ц | А | Т | Д | Ъ | К |

Полученный шифротекст: ТММЧ З ЦАТДЪК

Результат работы программы:





Тестовая фраза: Ё-ЛКА

Ключевое слово: ПЧЁЛКА

Таблицы подстановки:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **А** | **Б** | **В** | **Г** | **Д** | **Е** | **Ё** | **Ж** | **З** | **И** | **Й** | **К** | **Л** | **М** | **Н** | **О** | **П** |
| П | Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ъ | Ы | Ь | Э | Ю | Я |
| Ч | Ш | Щ | Ъ | Ы | Ь | Э | Ю | Я | А | Б | В | Г | Д | Е | Ё | Ж |
| Ё | Ж | З | И | Й | К | Л | М | Н | О | П | Р | С | Т | У | Ф | Х |
| Л | М | Н | О | П | Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ъ | Ы |
| К | Л | М | Н | О | П | Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ъ |
| А | Б | В | Г | Д | Е | Ё | Ж | З | И | Й | К | Л | М | Н | О | П |

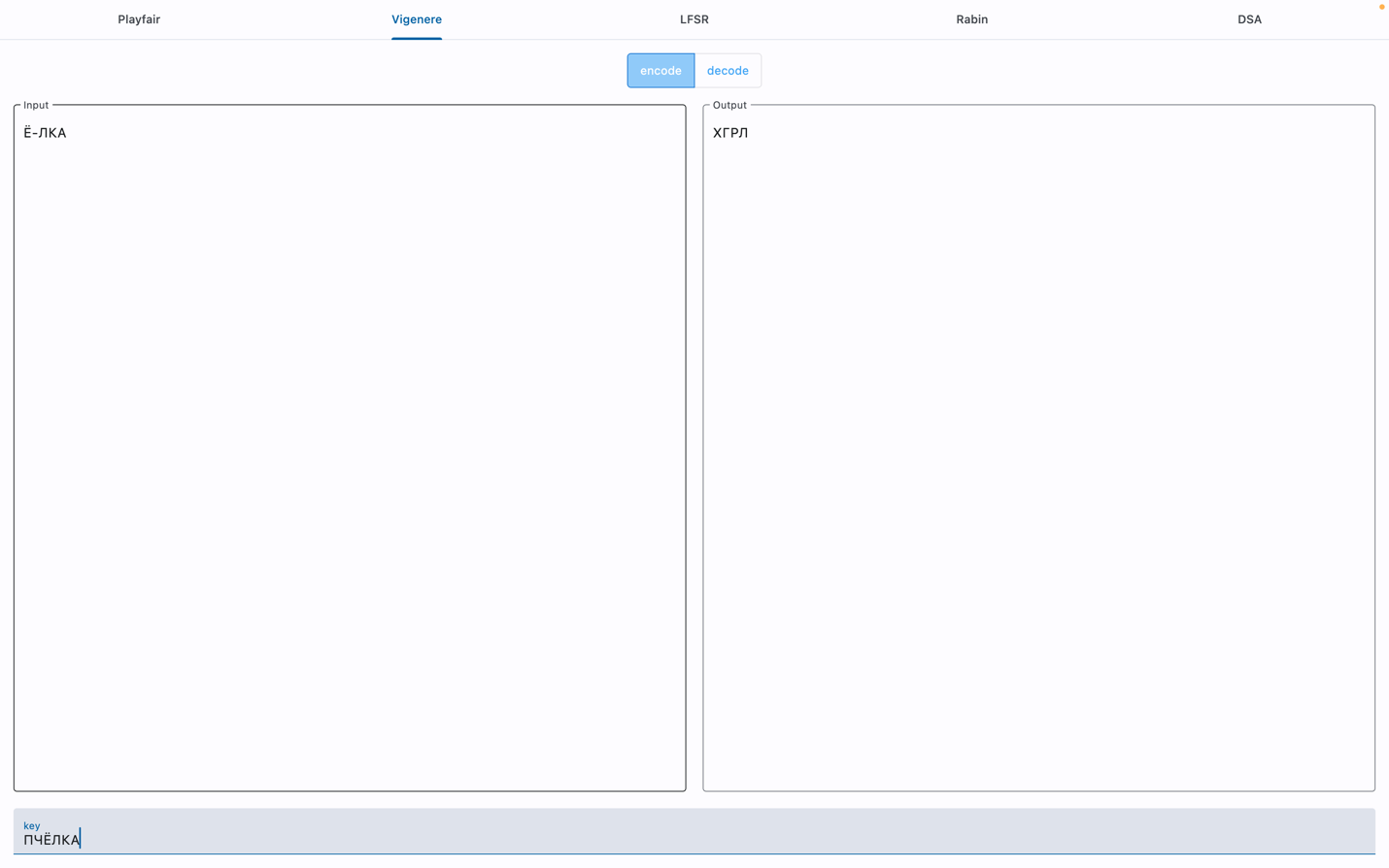
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Р** | **С** | **Т** | **У** | **Ф** | **Х** | **Ц** | **Ч** | **Ш** | **Щ** | **Ъ** | **Ы** | **Ь** | **Э** | **Ю** | **Я** |
| А | Б | В | Г | Д | Е | Ё | Ж | З | И | Й | К | Л | М | Н | О |
| З | И | Й | К | Л | М | Н | О | П | Р | С | Т | У | Ф | Х | Ц |
| Ц | Ч | Ш | Щ | Ъ | Ы | Ь | Э | Ю | Я | А | Б | В | Г | Д | Е |
| Ь | Э | Ю | Я | А | Б | В | Г | Д | Е | Ё | Ж | З | И | Й | К |
| Ы | Ь | Э | Ю | Я | А | Б | В | Г | Д | Е | Ё | Ж | З | И | Й |
| Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ъ | Ы | Ь | Э | Ю | Я |

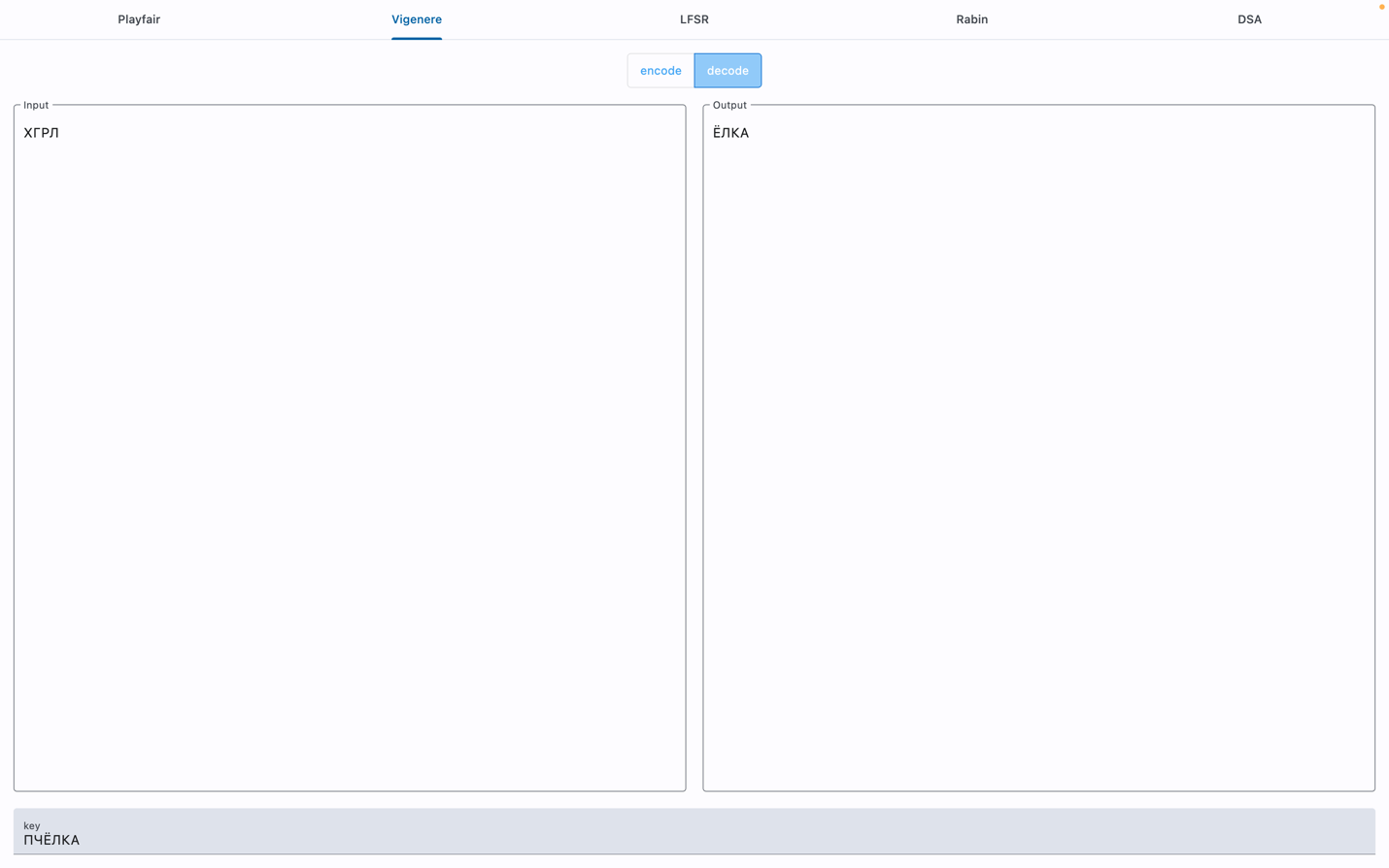
Преобразованная фраза: ЁЛКА

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| *М* ***=*** | **Ё** | **Л** | **К** | **А** |
| *К* ***=*** | **П** | **Ч** | **Ё** | **Л** |
| *С =* | Х | Г | Р | Л |

Полученный шифротекст: ХГРЛ

Результат работы программы:





***Ломаем на невалидных данных.***

Тестовая фраза: ИСХОДНЫЙ ТЕКСТ

Ключевое слово: abcde

Результат работы программы:

