**ЛАБОРАТОРНАЯ РАБОТА №1**

**Вариант 2**

*Выполнил староста гр. 351001*

*Ушаков Александр*

*Дата 28.02.2025*

# 1 Задание

Написать программу, которая выполняет шифрование и дешифрование текстового файла любого размера, содержащего текст на заданном языке, используя следующие алгоритмы шифрования:

* метод «железнодорожной изгороди», текст на русском языке;
* алгоритм Виженера, прогрессивный ключ, текст на русском языке.

Для всех алгоритмов ключ задается с клавиатуры пользователем.

Программа должна игнорировать все символы, не являющиеся буквами заданного алфавита, и шифровать только текст на заданном языке. Все алгоритмы должны быть реализованы в одной программе. Программа не должна быть написана в консольном режиме. Результат работы программы – зашифрованный/расшифрованный файл(ы).

# 2 Метод «Железнодорожной изгороди»

## 2.1 Дымовое тестирование для чётного ключа

**2.1.1** Запись тестовой фразы «Криптография» с недопустимыми символами и запись ключа «4».На рисунке 2.1.1 показан введённый текст.

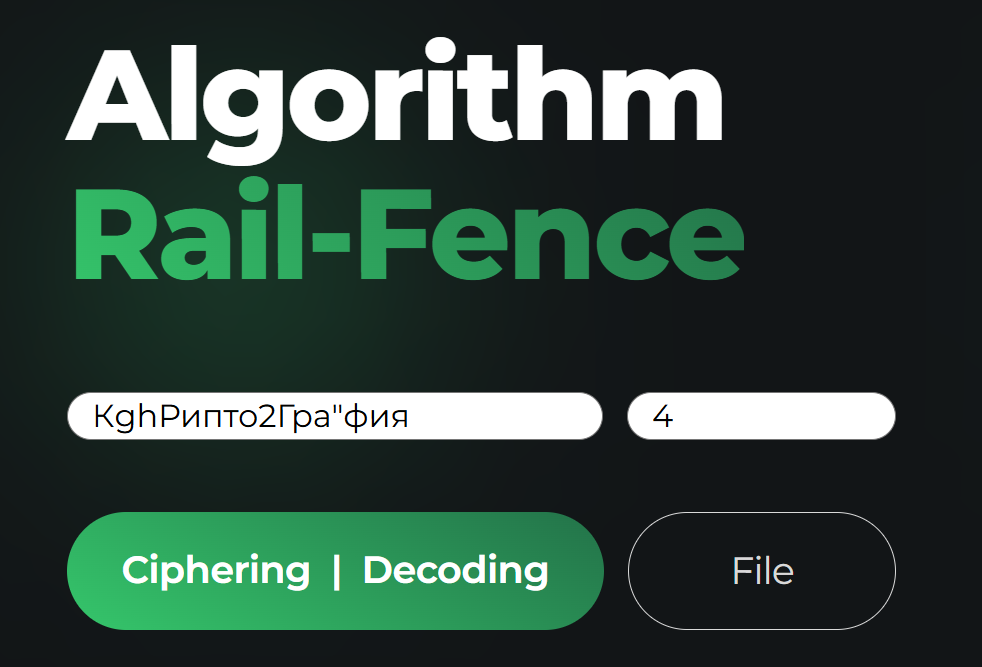


Рисунок 2.1.1 – Запись данных

**2.1.2** Отображение тестовой фразы в виде изгороди (см. таблицу 2.1.1).

Таблица 2.1.1 – Железнодорожная изгородь

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

**2.1.3** Полученный из изгороди шифротекст: **кгроряитаипф**.

**2.1.4** Результат шифрования представлен на рисунке 2.1.2. На изображении не отображается ключ, так при нажатии кнопки «Ciphering (Шифровать)» он сразу исчезает: все данные о ключе стираются моментально.

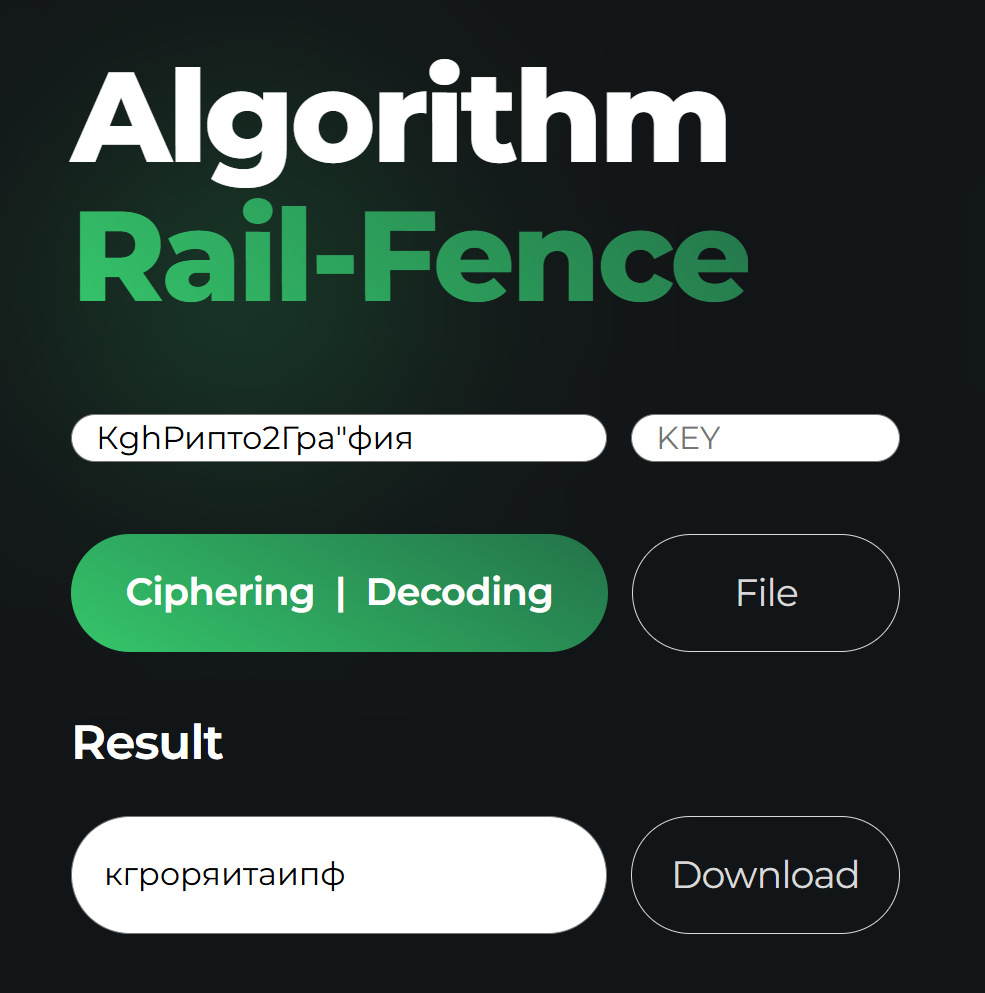


Рисунок 2.1.2 – Результат шифрования

**2.1.5** Дешифрирование. Теперь фразу «кгроряитаипф» необходимо ввести в качестве исходного текста, задать ключ «4» и нажать на кнопку «Decoding (Дешифрировать)» (см. рисунок 2.1.3 – след. стр.).

Аналогичным образом для более качественного тестирования можно добавить **недопустимые** символы, например цифры 1, 2, 5, 7, 8.

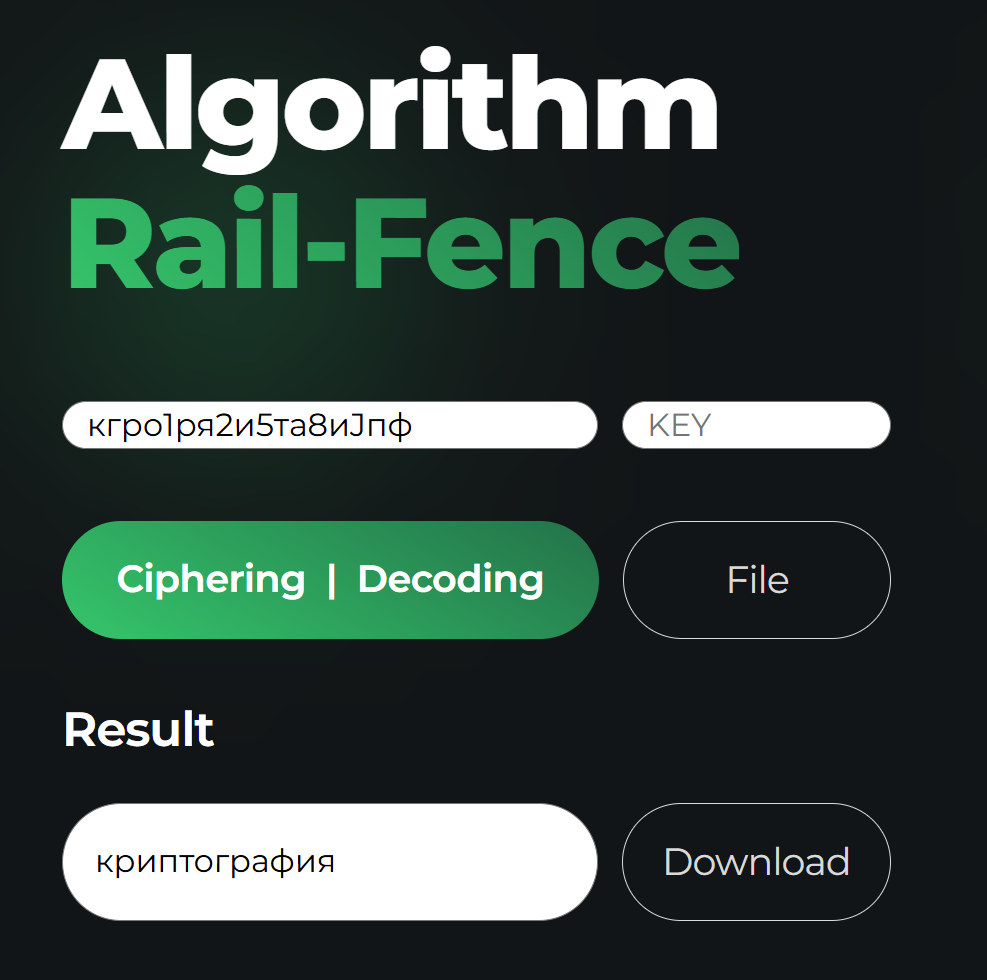


Рисунок 2.1.3 – Результат дешифрирования

Результатом дешифрирования стало слово «криптография», которое изначально и вводилось в качестве исходного текста. Тест пройден успешно.

## 2.2 Дымовое тестирование для нечётного ключа

**2.2.1** Запись тестовой фразы «До свидания Донателла Версаче» с недопустимыми символами и запись ключа «5».На рисунке 2.2.1 показан введённый текст.



Рисунок 2.2.1 – Запись данных

**2.2.2** Отображение тестовой фразы в виде изгороди (см. таблицу 2.2.1).

Таблица 2.2.1 – Железнодорожная изгородь

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| д |  |  |  |  |  |  |  | и |  |  |  |  |  |  |  | л |  |  |  |  |  |  |  | ч |  |
|  | о |  |  |  |  |  | н |  | я |  |  |  |  |  | е |  | л |  |  |  |  |  | а |  | е |
|  |  | с |  |  |  | а |  |  |  | д |  |  |  | т |  |  |  | а |  |  |  | с |  |  |  |
|  |  |  | в |  | д |  |  |  |  |  | о |  | а |  |  |  |  |  | в |  | р |  |  |  |  |
|  |  |  |  | и |  |  |  |  |  |  |  | н |  |  |  |  |  |  |  | е |  |  |  |  |  |

**2.2.3** Полученный из изгороди шифротекст:

**дилчоняелаесадтасвдоаврине**.

**2.2.4** Результат шифрования представлен на рисунке 2.2.2. На изображении не отображается ключ, так при нажатии кнопки «Ciphering (Шифровать)» он сразу исчезает: все данные о ключе стираются моментально.

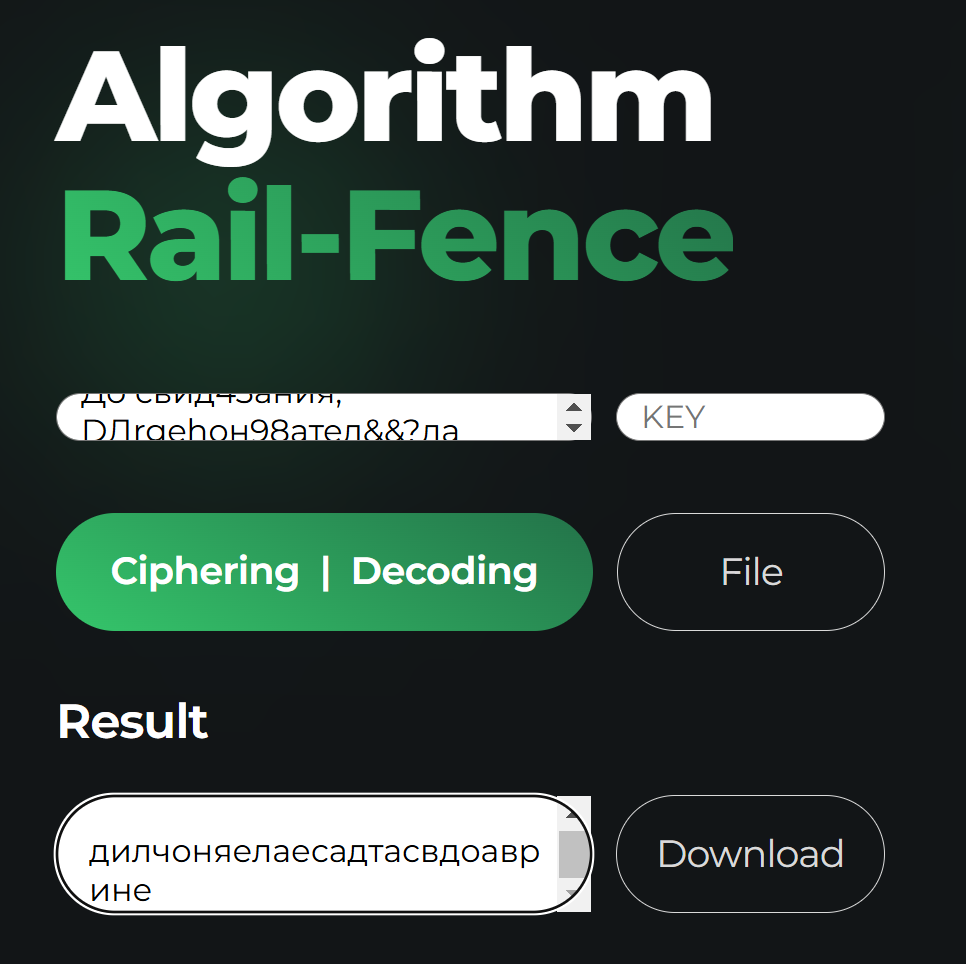


Рисунок 2.2.2 – Результат шифрования

**2.2.5** Дешифрирование. Теперь фразу «дилчоняелаесадтасвдоаврине» необходимо ввести в качестве исходного текста, задать ключ «5» и нажать на кнопку «Decoding (Дешифрировать)» (см. рисунок 2.2.3 – след. стр.).

Аналогичным образом для более качественного тестирования можно добавить **недопустимые** символы, например цифры 4, 6, 7.

Результатом дешифрирования стала фраза «досвиданиядона-теллаверсаче», которая изначально (до форматирования) и вводилось в качестве исходного текста. Тест пройден успешно.

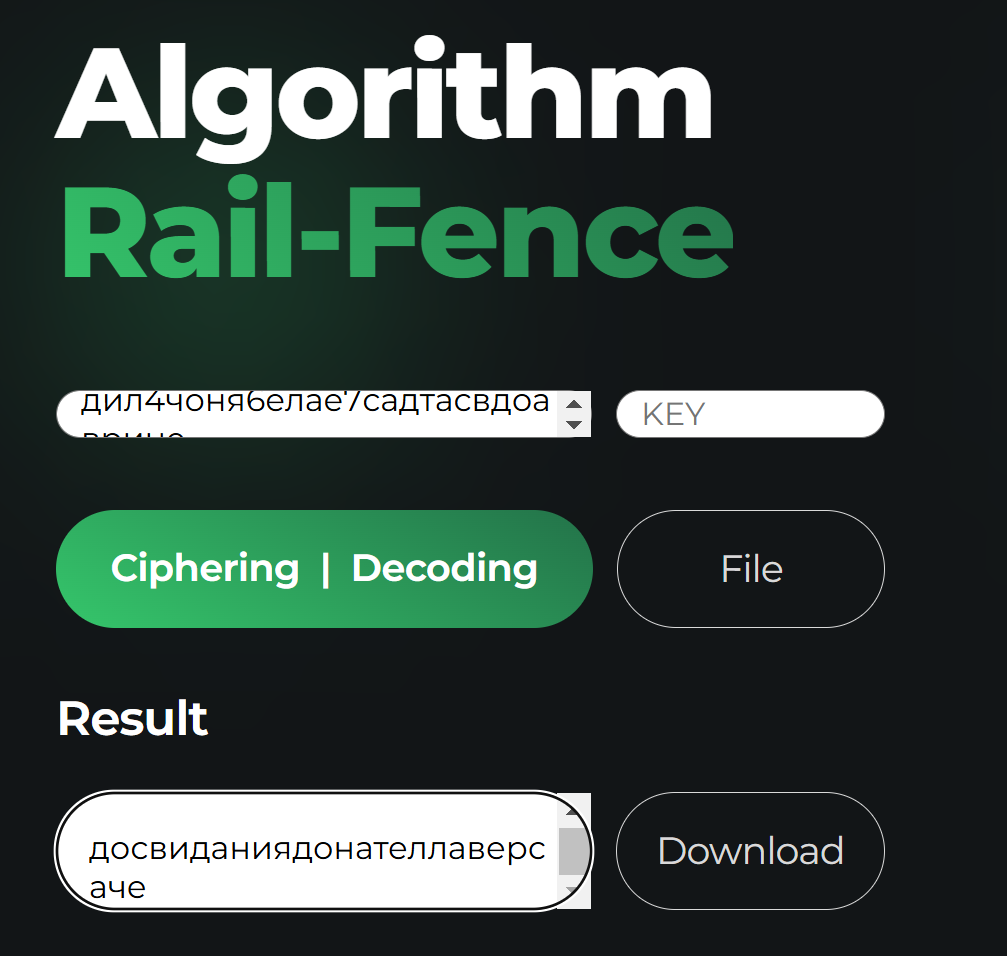


Рисунок 2.2.3 – Результат дешифрирования

## 2.3 Тестирование на валидных значениях ключа

К валидным крайним значениям ключа будут относиться:

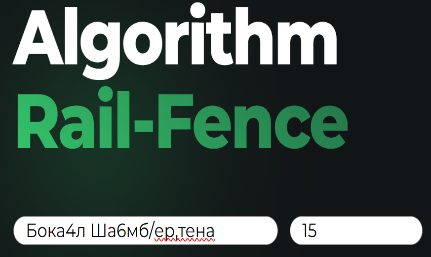
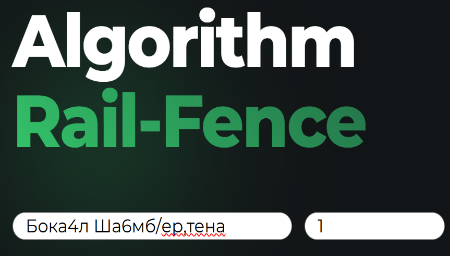
* 0: изгородь не будет сформирована;
* 1: так как исходный текст выстроиться в один ряд, результат

шифрования не будет от него отличаться;

* n ≥ plain\_text.length: если значение ключа будет равно длине

исходного текста или больше его, то сам текст выстроиться в одни ступени, а значит, шифротекст будет таким же.

**2.3.1** Ввод значений: тестирование будет реализовано на примере фразы «бокал Шамбертена», которая содержит 15 допустимых символов (n = 15).



**2.3.2** Как уже было сказано в пункте, не имеет смысла изображать изгородь для крайних случаев, так как для «0» это невозможно, а для «1» и «15» получится банально одна строка.

**2.3.3** Результатом должна стать исходная фраза для каждого из ключей:

«**бокалшамбертена**», только уже прошедшая стадию форматирования.

**2.3.4** Результат шифрования совпадает для всех ключей и представлен на рисунке 2.3.1.

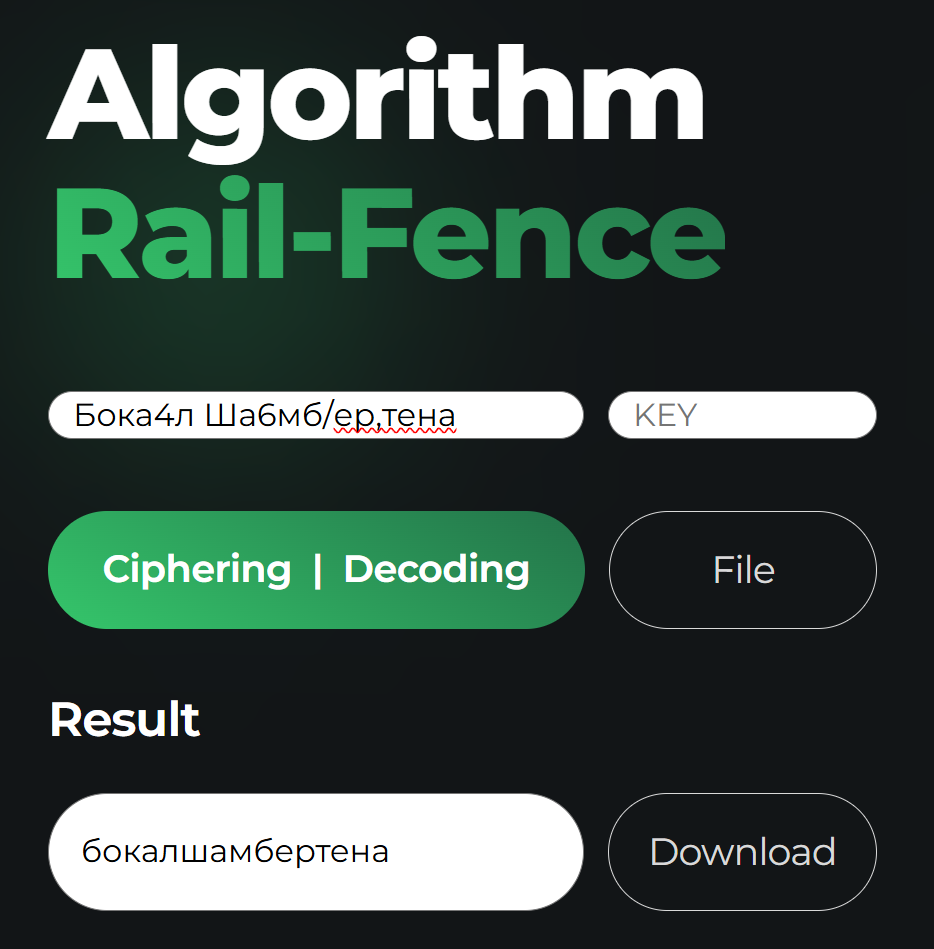


Рисунок 2.3.1 – Результат шифрования для крайних значений ключа

**2.3.5** Дешифрирование. Результатом дешифрирования для ключе 0, 1, 15 должен стать исходный текст (отформатированный), то есть «бокалшамбертена»: смотреть рисунок 2.3.2.

Для того, чтобы продемонстрировать надёжность работы алгоритма, добавим к шифротексту недопустимых символов и нажмём на кнопку «Decoding (Дешифрировать)».

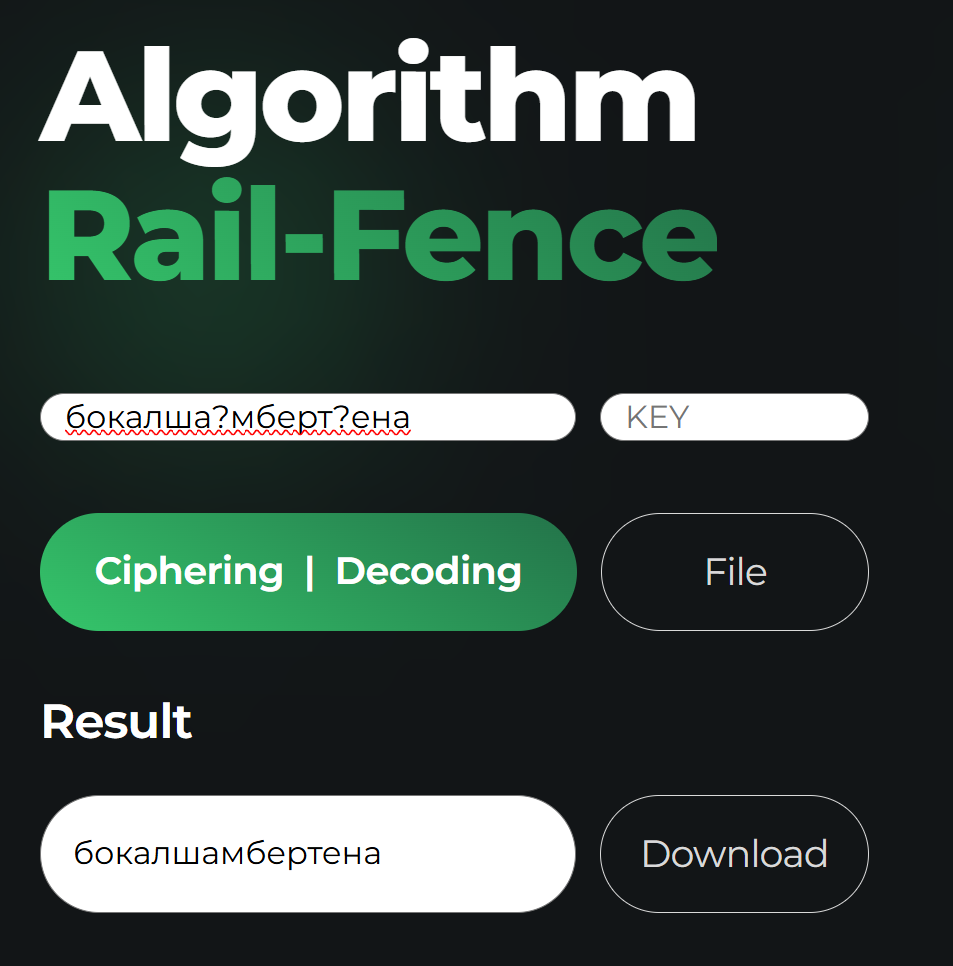


Рисунок 2.3.2 – Результат дешифрирования

Как и ожидалось, на выходе для каждого из ключей мы получили исходный текст. Тест пройден успешно.

## 2.4 Тестирование на невалидных значениях ключа

Под невалидными значениями ключа подразумеваются все нечисловые данные. В этом случае возможны 3 варианта:

* поле ключа оказалось пустым: на странице появиться сообщение о том, что ключ невозможно распознать;
* поле ключа содержит только нечисловые символы: на странице появиться сообщение о том, что ключ невозможно распознать;
* поле ключа содержит символы, среди которых есть числа: в этом случае ключ будет обработан и его валидная часть будет использована.

**2.4.1** Ввод данных: в качестве исходного текста будет слово «Аббревиатура», а ключ введём «?4фn» (см. рисунок 2.4.1).



Рисунок 2.4.1 – Исходные данные

**2.4.2** Построение изгороди по введённой фразе с учётом того, что ожидается ключ «4» (см. таблицу 2.4.1).

Таблица 2.4.1 – Железнодорожная изгородь

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| а |  |  |  |  |  | и |  |  |  |  |  |
|  | б |  |  |  | в |  | а |  |  |  | а |
|  |  | б |  | е |  |  |  | т |  | р |  |
|  |  |  | р |  |  |  |  |  | у |  |  |

**2.4.3** Полученный из изгороди шифротекст: **аибваабетрру.**

**2.4.4** Результат шифрования представлен на рисунке 2.4.2.

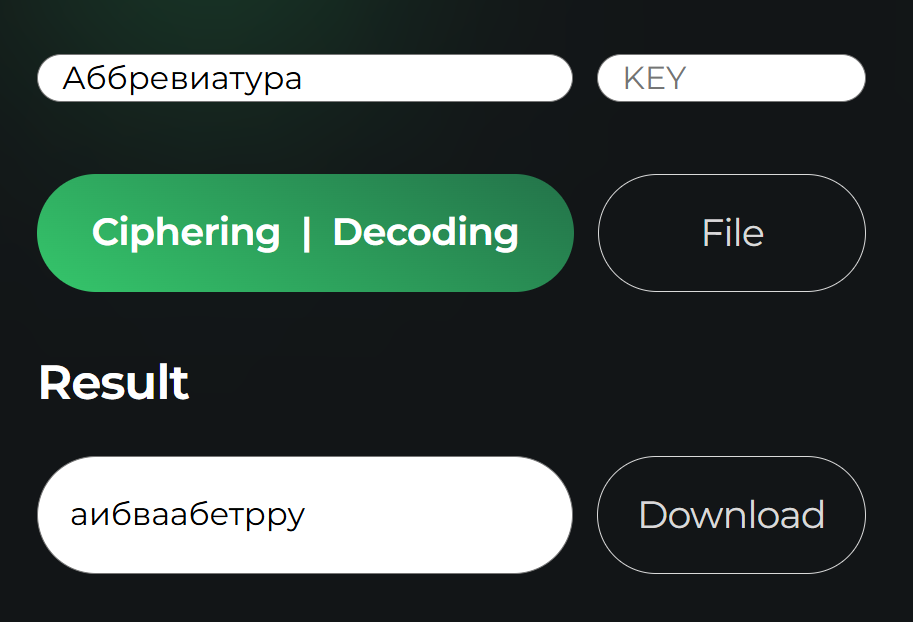
****

Рисунок 2.4.2 – Результат шифрования

**2.4.5** Теперь для процесса дешифрирования в поле ввода введём получившийся результат «аибваабетрру», а в поле ключа всё тот же невалидный ключ «?4фn» и проверим, получиться ли на выходе слово «аббревиатура» (см. рисунок 2.4.3).

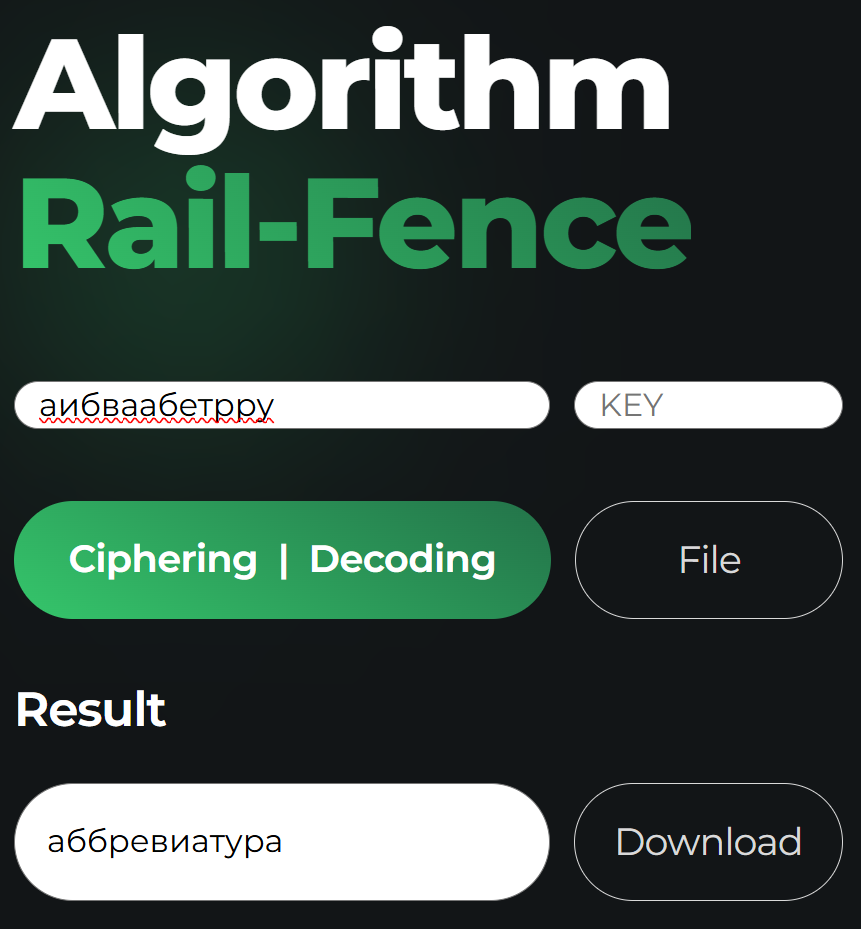


Рисунок 2.4.3 – Результат дешифрирования с невалидным ключом

Результаты, полученные на этапе дешифрирования, соответствуют ожидаемым. Тест пройден успешно.

**2.4.6** Случаи абсолютно невалидного ключа. Если ключ пустой или не содержит цифр, пользователь увидит в браузере сообщение об ошибке (см. рисунок 2.4.4)

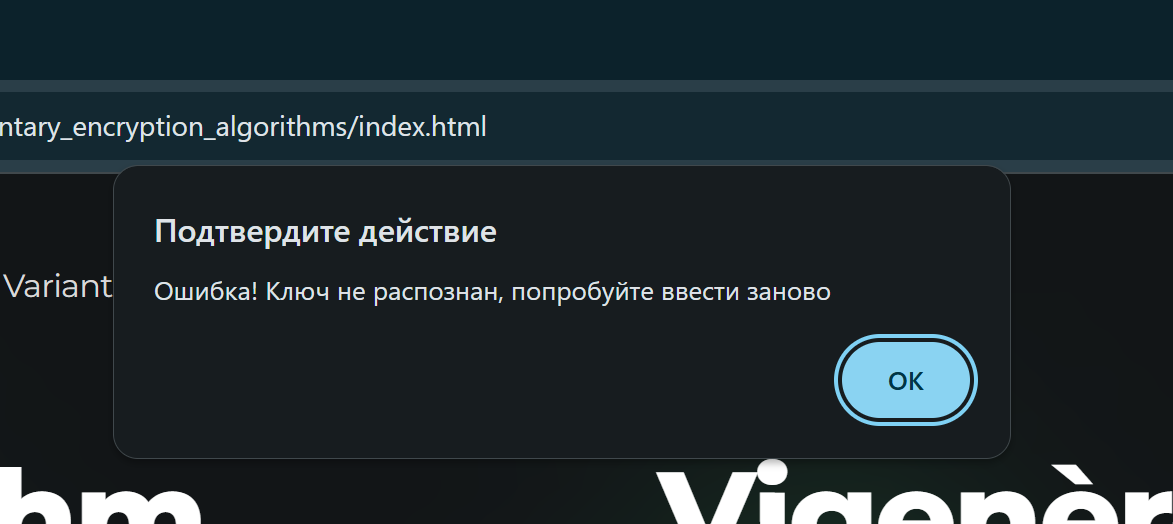


Рисунок 2.4.4 – Сообщение об ошибке

# 3 Алгоритм Виженера с прогрессивным ключом

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

## 3.1 Дымовое тестирование

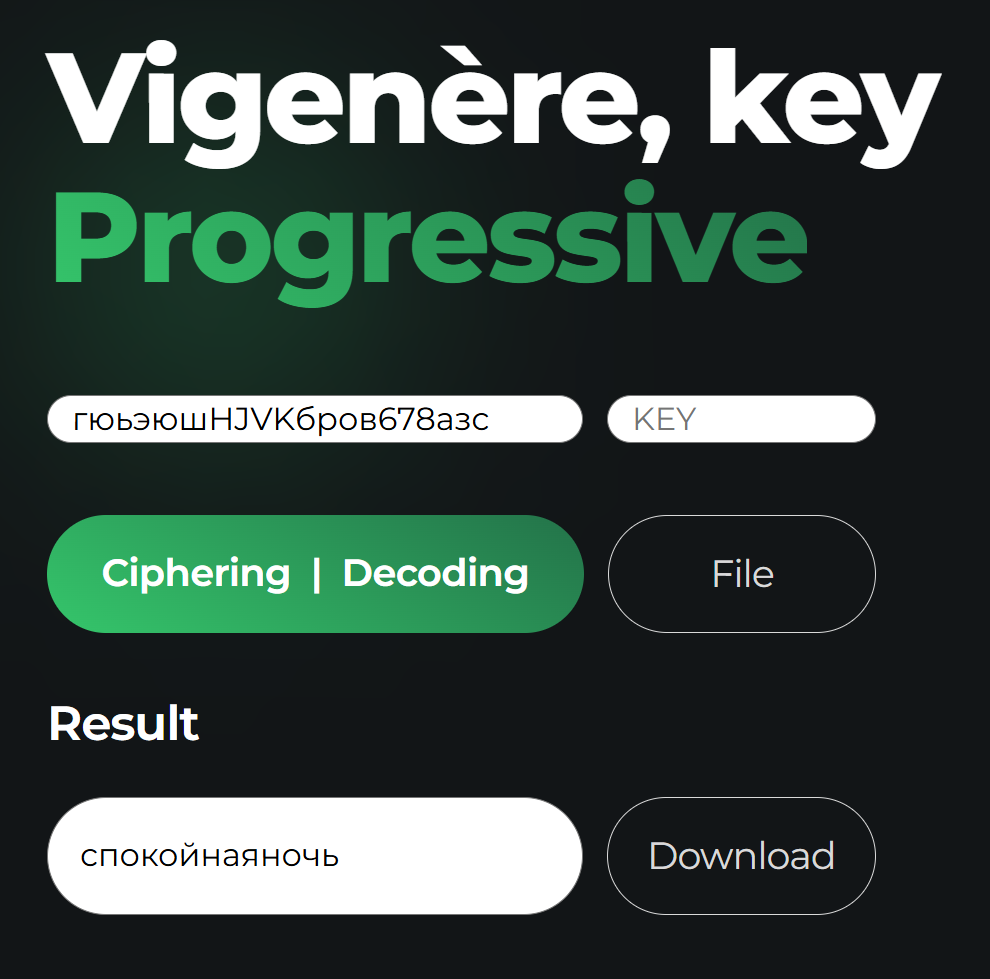
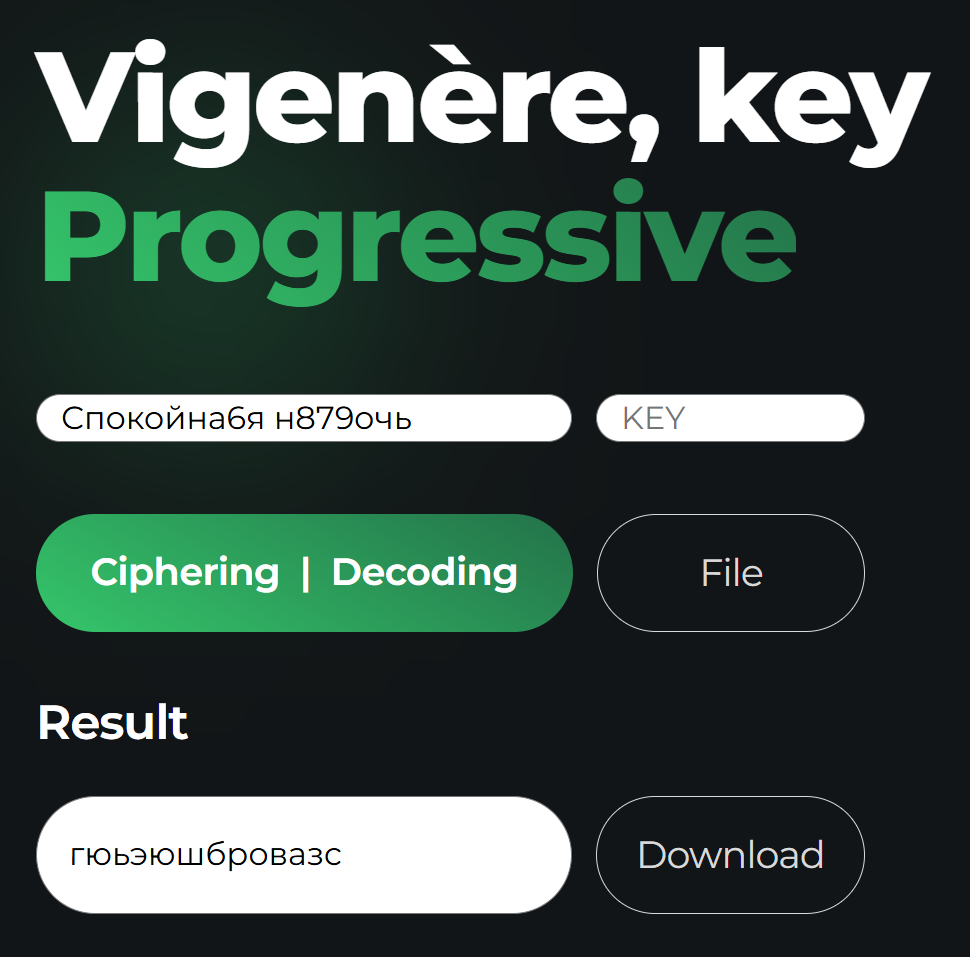
**3.1.1** Тестовая фраза: «Спокойная ночь», ключ: «сон» (см. табл. 3.1.1).

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| С | П | О | К | О | Й | Н | А | Я | Н | О | Ч | Ь |
| С | О | Н | Т | П | О | У | Р | П | Ф | С | Р | Х |
| Г | Ю | Ь | Э | Ю | Ш | Б | Р | О | В | А | З | С |

Таблица 3.1.1 – Тестовая фраза, ключ, шифротекст

**3.1.2** Шифротекст: **гюьэюшбровазс**.

**3.1.3** Шифрование и дешифрирование представлено на рисунках 3.1.1 и 3.1.2 соответственно.



Рисунки 3.1.1 и 3.1.2 – Шифрование и дешифрирование

**Тест пройден успешно.**

## 3.2 Тестовая фраза с буквой «ё»

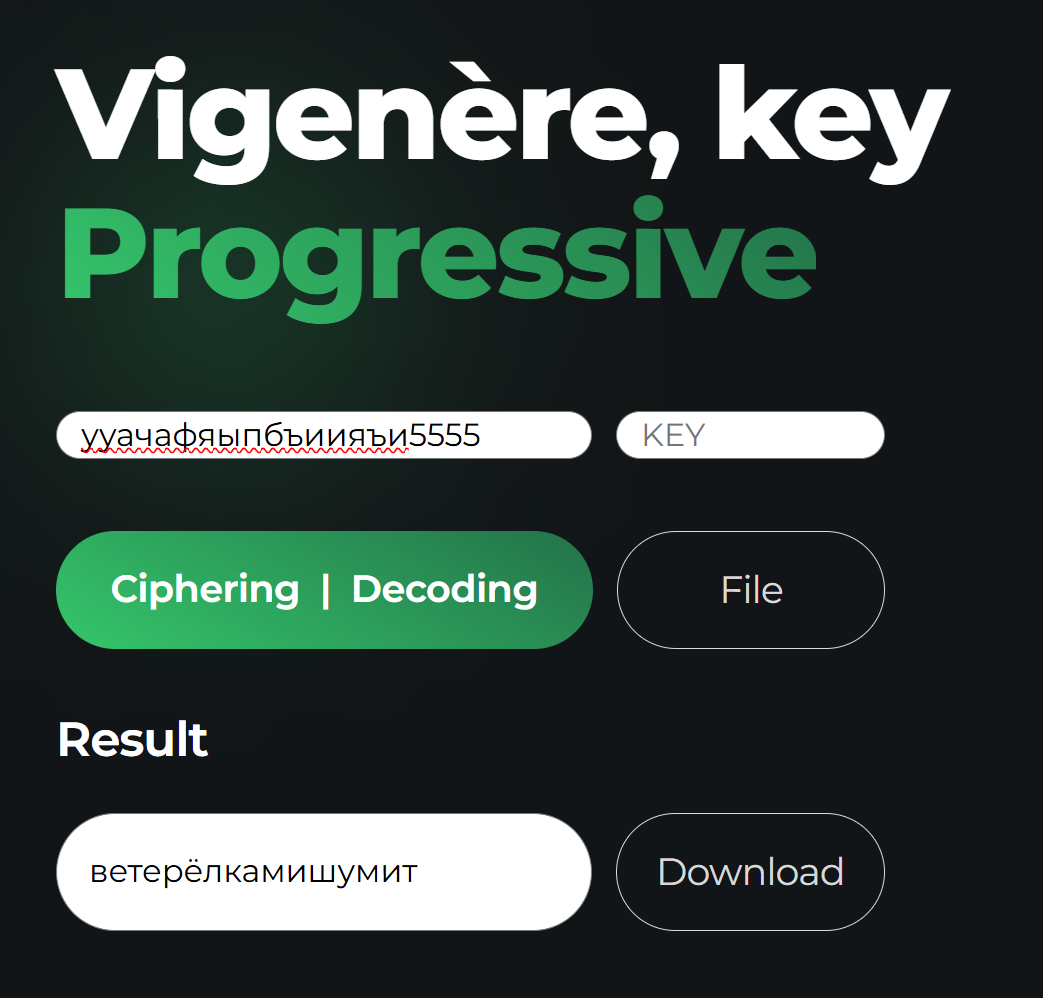
**3.2.1** Тестовая фраза: «Ветер ёлками шумит», ключ: «сон» (см. табл. 3.2.1).

Таблица 3.1.1 – Тестовая фраза, ключ, шифротекст

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| В | Е | Т | Е | Р | Ё | Л | К | А | М | И | Ш | У | М | И | Т |
| С | О | Н | Т | П | О | У | Р | П | Ф | С | Р | Х | Т | С | Ц |
| У | У | А | Ч | А | Ф | Я | Ы | П | Б | Ъ | И | И | Я | Ъ | И |

**3.2.2** Шифротекст: **ууачафяыпбъиияъи**.

**3.2.3** Шифрование и дешифрирование представлено на рисунках 3.2.1 и 3.2.2 соответственно.

Рисунки 3.2.1 и 3.2.2 – Результаты шифрования и дешифрирования

**Тест пройден успешно.**

## 3.3 Случай невалидного ключа

В случае, когда ключ содержит как валидные, так и не валидные символы, вторые игнорируются и рассматривается только часть актуальная часть. Если в пункте 3.1 вместо «сон» ввести «6сонQIE» результат не изменится и ключ обработается корректно (см. рисунки 3.3.1, 3.3.2).



Рисунок 3.3.1 – Ввод невалидного ключа



Рисунок 3.3.2 – Результат шифрования

Результат такой же, как и при вводе валидного ключа – тест успешен.

В случае, когда ключ не содержит ни одного валидного символа, шифротекст на выходе окажется пустым (см. рисунки 3.3.3, 3.3.4).



Рисунок 3.3.3 – Вводимый абсолютно невалидный ключ



Рисунок 3.3.4 – Результат алгоритма с абсолютно невалидным ключом

**Тест пройден успешно.**

# Обратите внимание!!!

Для того чтобы страница выглядела **«очень красиво»** необходимо при открытии html-файла задать масштабирование. Это очень просто и делается в два клика (см. рис. 4.1): нажать на три точки в верхнем правом углу – сразу можно увидеть пункт «Масштаб».

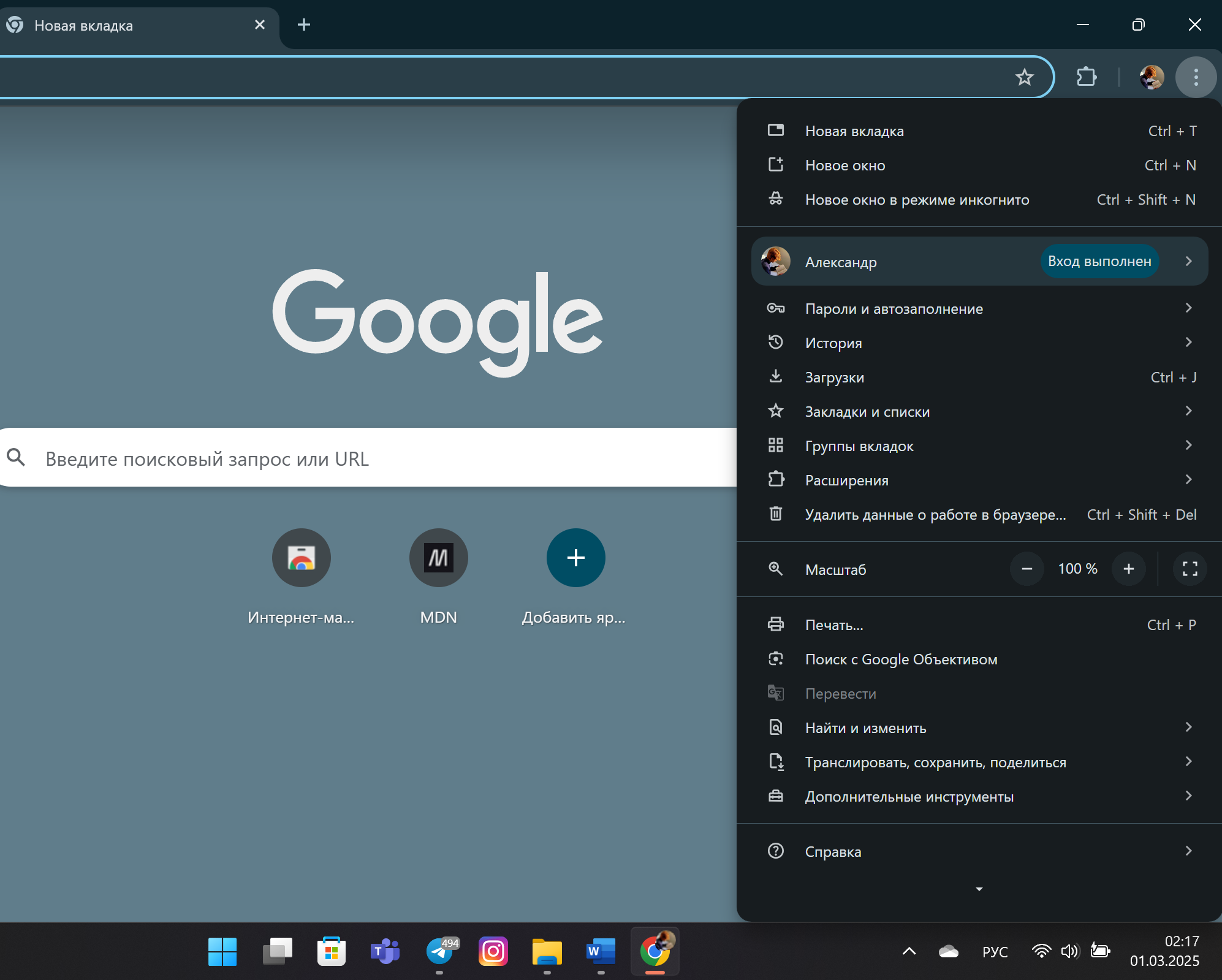


Рисунок 4.1 – Масштабирование в Chrome

**В идеале** страница должна выглядеть, как показано на рисунке 4.2.

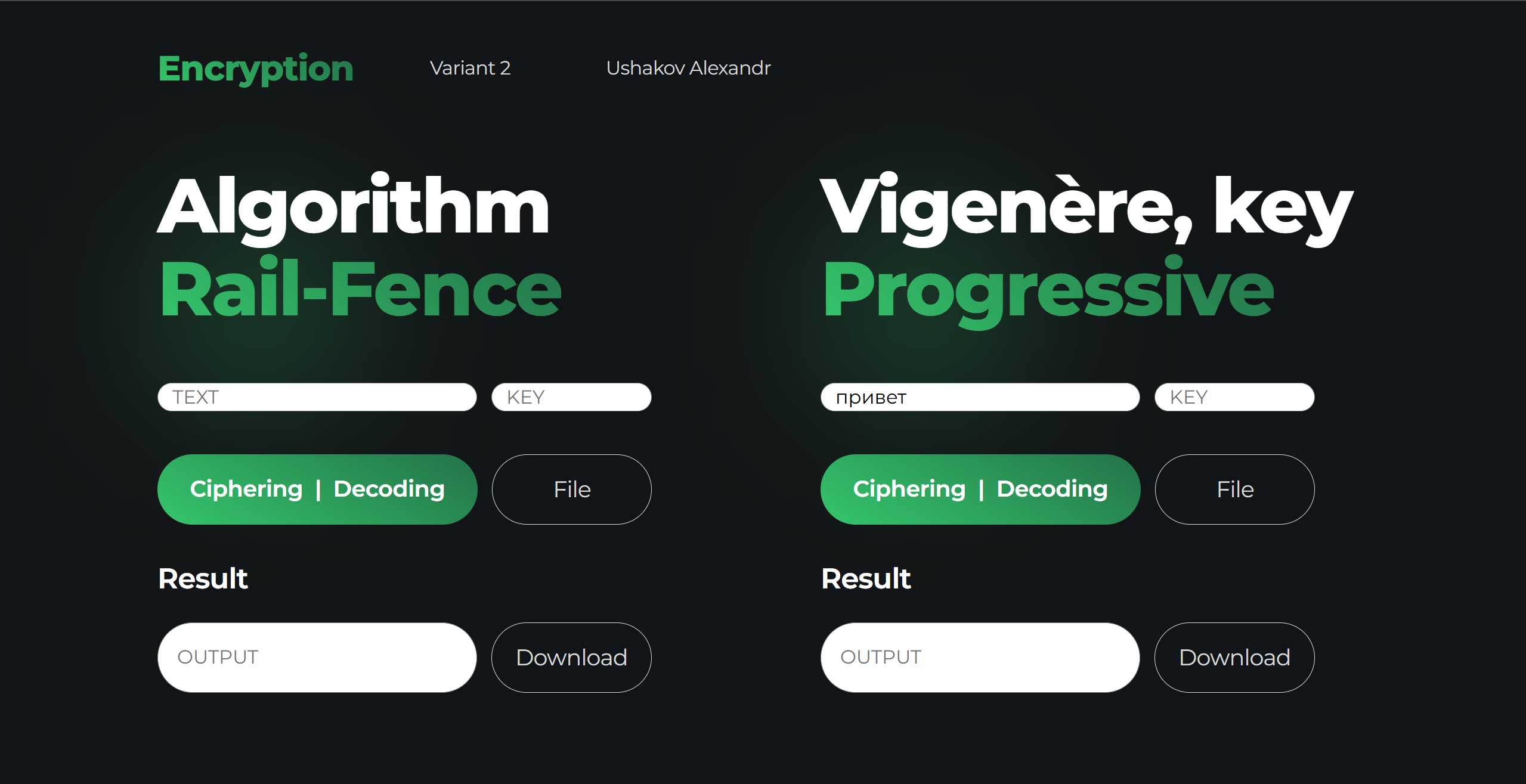


Рисунок 4.2 – Корректные настройки отображения страницы