МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образования «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Исследование криптографических шифров на основе подстановки перестановки символов

Студент: Евсеенко В. П.

ФИТ 3 курс 4 группа

Преподаватель: Савельева М. Г.

Минск 2025

Содержание

[Введение 3](#_Toc193146557)

[1 Практическое задание 4](#_Toc193146558)

[2 Гистограммы 10](#_Toc193146559)

[3 Оценка времени 11](#_Toc193146560)

[Вывод 12](#_Toc193146561)

# **Введение**

Цель лабораторной работы:

* изучение и приобретение практических навыков разработки и использования приложений для реализации перестановочных шифров.

Задачи:

* закрепить теоретические знания по алгебраическому описанию, алгоритмам реализации операций зашифрования/расшифрования и оценке криптостойкости перестановочных шифров;
* ознакомиться с особенностями реализации и свойствами различных перестановочных шифров на основе готового программного средства (L\_LUX).
* разработать приложение для реализации указанных преподавателем методов перестановочного зашифрования/расшифрования;
* выполнить исследование криптостойкости шифров на основе статистических данных о частотах появления символов в исходном и зашифрованном сообщениях;
* оценить скорость зашифрования/расшифрования реализованных способов шифров;
* результаты выполнения лабораторной работы оформить в виде описания разработанного приложения, методики выполнения экспериментов с использованием приложения и результатов эксперимента.

# **1 Практическое задание**

Разработать авторское приложение в соответствии с целью лабораторной работы. Приложение должно реализовывать следующие операции:

* выполнять зашифрование/расшифрование текстовых документов (объемом не менее 500 знаков), созданных на основе алфавита языка в соответствии с нижеследующей таблицей вариантов задания; при этом следует использовать шифры подстановки из третьего столбца данной таблицы (варианты задания в табл. 1.1).

Таблица 1.1 – Варианты задания

|  |  |  |
| --- | --- | --- |
| Вариант | Алфавит | Шифр |
| 1 | Белорусский | 1. Маршрутная перестановка (маршрут: запись – по строкам, считывание – по столбцам таблицы; параметры таблицы – по указанию преподавателя) 2. Множественная перестановка, ключевые слова – собственные имя и фамилия |
| 2 | Русский | 1. Маршрутная перестановка (маршрут –по спирали; параметры таблицы – по указанию преподавателя) 2. Множественная перестановка, ключевые слова – собственные имя и фамилия |
| 3 | Английский | 1. Маршрутная перестановка (маршрут – зигзагом; параметры таблицы – по указанию пре подавателя) 2. Множественная перестановка, ключевые слова – собственные имя и фамилия |
| 4 | Немецкий | 1. Маршрутная перестановка (маршрут змейкой; параметры таблицы – по указанию преподавателя) 2. Множественная перестановка, ключевые слова – собственные имя и фамилия |
| 5 | Польский | 1. Маршрутная перестановка (маршрут: за пись – по столбцам, считывание – по строкам таблицы; параметры таблицы – по указанию преподавателя) 2. Множественная перестановка, ключевые слова – собственные имя и фамилия |

Был реализован алгоритм шифрования и расшифрования с помощью маршрутной перестановки. Маршрут: запись – по строкам, считывание – по столбцам таблицы.

Пример работы алгоритма:

1. Допустим, исходное сообщение – «Das lässt sich nicht ändern».

2. Длина сообщения – 27 символов. Размер таблицы перестановки: 3×9. Расположенное сообщение по ячейкам находится в таблице 1.1

Таблица 1.1 – Исходное сообщение

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| D | a | s |  | l | ä | s | s | t |
|  | s | i | c | h |  | n | i | c |
| h | t |  | ä | n | d | e | r | n |

3. Далее для зашифрования сообщения таблица считывается по столбцам. Зашифрованное сообщение: «D hastsi cälhnä dsnesirtcn».

4. При расшифровании строится новая таблица, в которой столбцы и строки меняются местами. Т.е. если таблица была размеров 3×9, то новая таблица будет размеров 9×3. Расположение зашифрованного сообщения по ячейкам находися в таблице 1.2 Исходное сообщение считывается по столбцам.

Таблица 1.2 – Зашифрованное сообщение

|  |  |  |
| --- | --- | --- |
| D |  | h |
| a | s | t |
| s | i |  |
|  | c | ä |
| l | h | n |
| ä |  | d |
| s | n | e |
| s | i | r |
| t | c | n |

Расшифрованное сообщение: «Das lässt sich nicht ändern».

Функция шифрования routeTranspositionEncode принимает на вход исходный текст и размер для таблицы. На основе исходного текста она формирует таблицу и начинает её обход по строкам. Код функции представлен в листинге 1.1.

|  |
| --- |
| export const routeTranspositionEncode = (text: string, tableSize: [number, number]): string  => {      let table = formEncryptionTable(text, tableSize);      let result: string = "";      for (let i = 0; i < table[0].length; i++) {          for (let j = 0; j < table.length; j++) {              result += table[j][i];}}      return result;} |

Листинг 1.1 – Функции шифрования с помощью маршрутной перестановки

Функция расшифрования routeTranspositionDecode принимает на вход зашифрованный текст и размер таблицы. Она формирует таблицу и обходит её по столбцам. Код функции представлен в листинге 1.2.

|  |
| --- |
| export const routeTranspositionEncode = (text: string, tableSize: [number, number]): string  => {      let table = formEncryptionTable(text, tableSize);      let result: string = "";      for (let i = 0; i < table[0].length; i++) {          for (let j = 0; j < table.length; j++) {              result += table[j][i];}}  return result;  } |

Листинг 1.2 – Функция расшифрования с помощью маршрутной перестановки

Результат работы функций шифрования и расшифрования немецкого алфавита с помощью маршрутной перестановки приведен на рисунке 1.1.

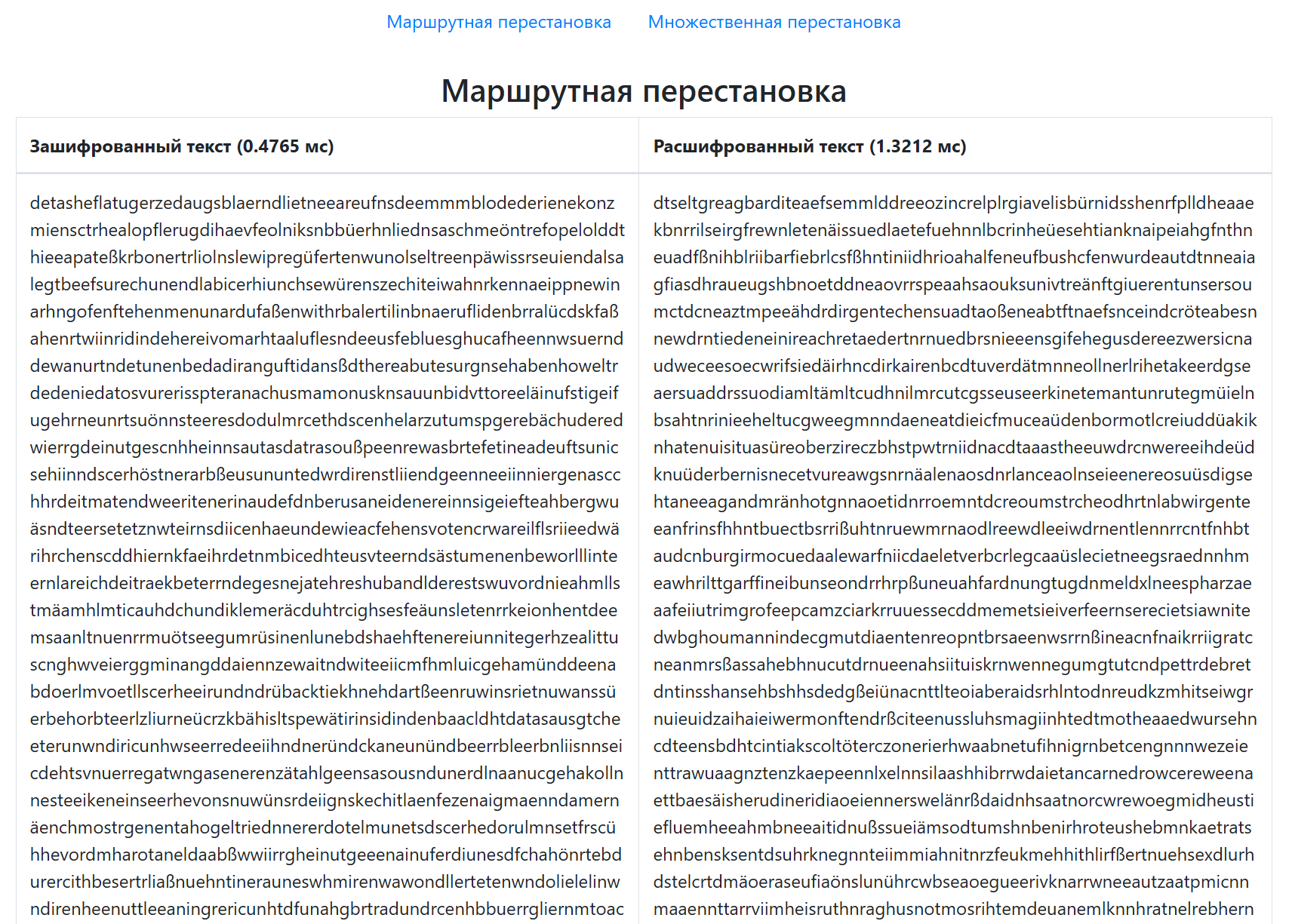


Рисунок 1.1 – Результат шифрования и расшифрования на основе немецкого алфавита с помощью маршрутной перестановки

После были разработаны несколько функций, выполняющих шифрование и дешифрование текста с использованием множественной перестановки, где ключевые слова – собственное имя и фамилия.

Сначала была разработана функция formSortedTable, которая принимает размер таблицы и таблицу с исходным порядком символов в сообщении. Далее, с помощью ключевых слов, она сортирует таблицу сначала по строкам, а затем по столбцам. Код функции представлен в листинге 1.3.

|  |
| --- |
| export const formSortedTable = (tableSize: [number, number], table: string[][]) => {  let sortedTable: string[][] = [];  const {nameKeywordIndexes, lastnameKeywordIndexes} = transformKeywords(tableSize);      for (let i = 0; i < nameKeywordIndexes.length; i++) {          sortedTable[nameKeywordIndexes[i][1]] = table[i];  }  table = structuredClone(sortedTable);      for (let i = 0; i < nameKeywordIndexes.length; i++) {          for (let j = 0; j < lastnameKeywordIndexes.length; j++) {    sortedTable[i][lastnameKeywordIndexes[j][1]] = table[i][j];          }      }  return sortedTable;  } |

Листинг 1.3 – Функция, формирующая таблицу перестановок

Функция шифрования multipleTranspositionEncode принимает на вход исходный текст и таблицу перестановок. Код функции представлен в листинге 1.4.

|  |
| --- |
| export const multipleTranspositionEncode = (text: string, table: string[][]) => {  let result: string = "";      for (let i = 0; i < table[0].length; i++) {          for (let j = 0; j < table.length; j++) {              result += table[j][i];          }      }      return result;  } |

Листинг 1.4 – Функция, формирующая таблицу перестановок

Функция расшифрования multipleTranspositionDecode принимает на вход зашифрованный текст и таблицу перестановок. Код функции представлен в листинге 1.5.

|  |
| --- |
| export const multipleTranspositionEncode = (text: string, table: string[][]) => {  let result: string = "";      for (let i = 0; i < table[0].length; i++) {          for (let j = 0; j < table.length; j++) {              result += table[j][i];          }      }      return result;  } |

Листинг 1.5 – Функции расшифрования с помощью множественных перестановок

Результат работы функций шифрования и расшифрования немецкого алфавита приведен на рисунке 1.2.



Рисунок 1.2 – Функции расшифрования с помощью множественной перестановки

# **2 Гистограммы**

Необходимо сформировать гистограммы частот появления символов для исходного и зашифрованного сообщений.

Гистограмма частот появления символов немецкого алфавита в исходном сообщении приведена на рисунке 2.1.



Рисунок 2.1 – Гистограмма частот появления символов немецкого алфавита в исходном сообщении

Гистограмма частот появления символов немецкого алфавита в зашифрованном сообщении с помощью маршрутной перестановки приведена на рисунке 2.2.



Рисунок 2.2 – Гистограмма частот появления символов немецкого алфавита в зашифрованном сообщении с помощью маршрутной перестановки

Гистограмма частот появления символов немецкого алфавита в зашифрованном сообщении с помощью множественной перестановки приведена на рисунке 2.3.



Рисунок 2.3 – Гистограмма частот появления символов немецкого алфавита в зашифрованном сообщении с помощью множественной перестановки

# **3 Оценка времени**

Оценить время выполнения операций зашифрования/расшифрования (напоминание: во многих языках программирования есть встроенные методы для замеров времени; при отсутствии такового в используемом языке можно воспользоваться разностью двух дат (например, в миллисекундах: время после выполнения программы – время до начала выполнения преобразования)).

Оценка времени выполнения операций шифрования и расшифрования в блочном шифре представлена на рисунке 2.1.

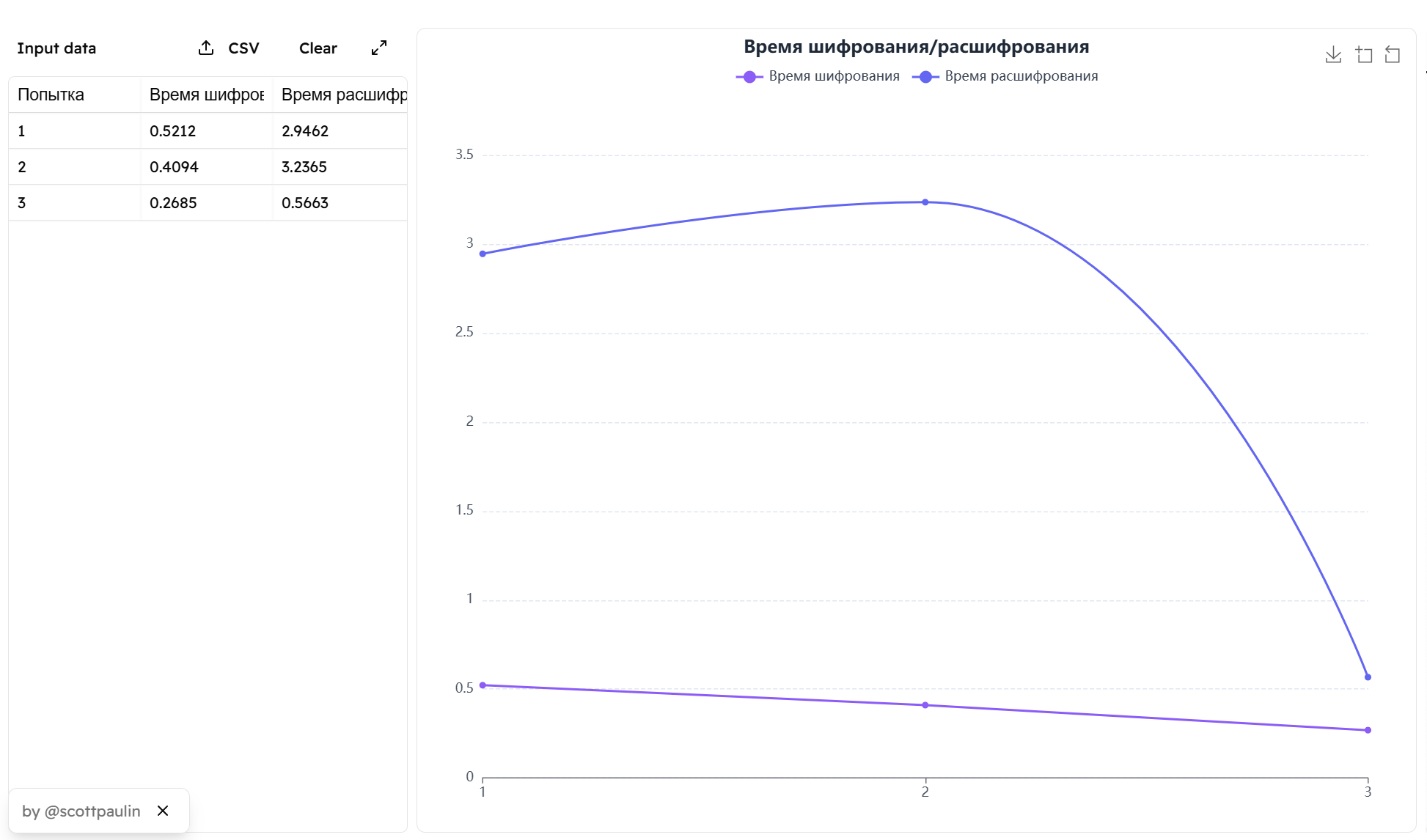


Рисунок 3.1 – Оценка времени операций с помощью маршрутной перестановки

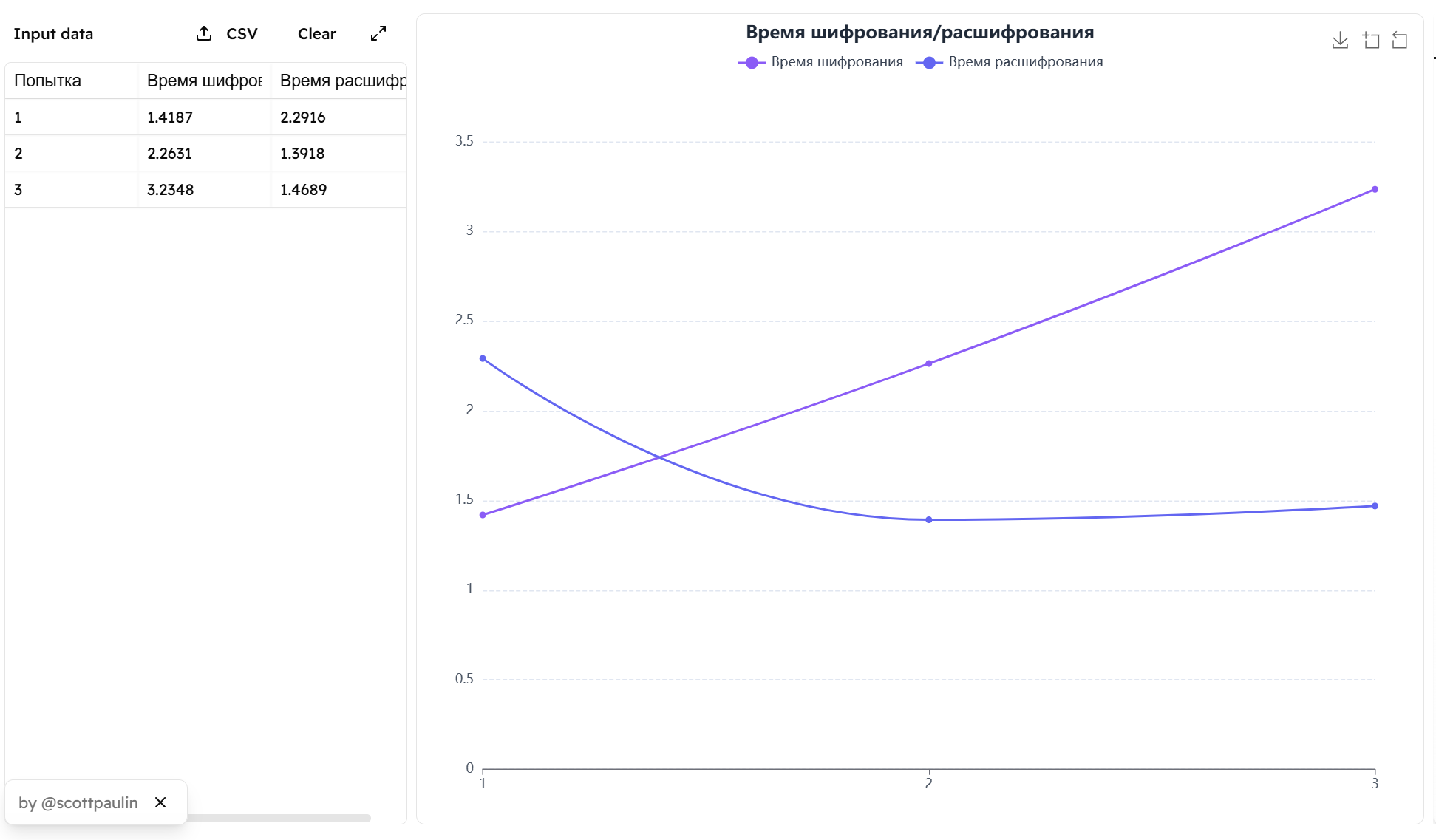


Рисунок 3.2 – Оценка времени операций с помощью множественной перестановки

# **Вывод**

В ходе выполнения лабораторной работы были изучены теоретические основы перестановочных шифров, их алгоритмическое описание и методы оценки криптостойкости. Ознакомление с программным средством L\_LUX позволило на практике проанализировать особенности различных перестановочных шифров.

Разработанное приложение реализует заданные методы шифрования и расшифрования, обеспечивая возможность исследования их криптостойкости. Проведённые эксперименты включали анализ частотного распределения символов в исходных и зашифрованных текстах, а также измерение скорости выполнения операций шифрования и дешифрования.

Полученные результаты позволили сделать выводы о степени защищённости изученных шифров и их эффективности. Оформление отчёта по лабораторной работе включает описание разработанного приложения, методику проведения экспериментов и анализ полученных данных.