Учреждение образования

«Белорусский государственный технологический университет»

**Лабораторная работа №4**

Исследование криптографических шифров на основе подстановки(замены) символов

Выполнил:

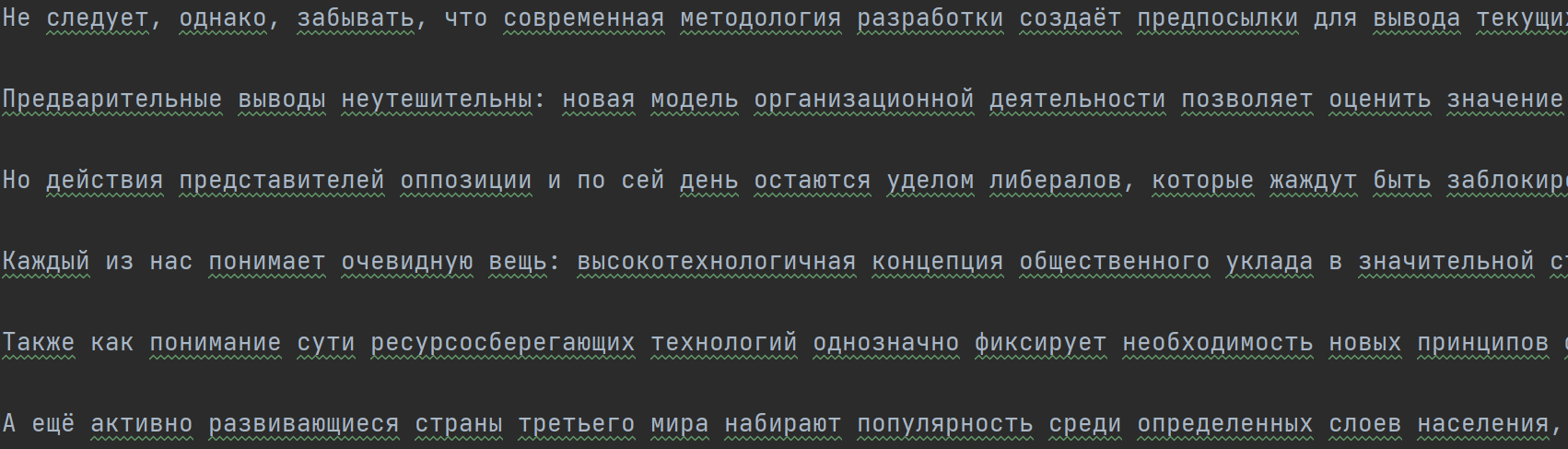
Студент 3 курса 5 группы ФИТ

Коршун Никита Игоревич

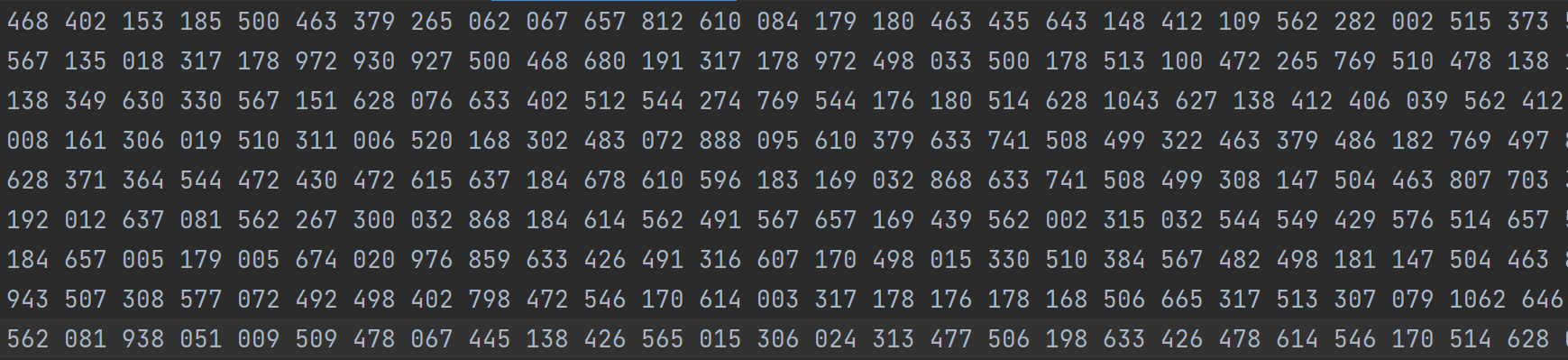
2024

**Задание 1.** Для зашифрования/расшифрования текстовых документов было создано приложение. В качестве входного документа использовался текстовый файл содержащий текст на русском языке (длина текста более 5000 символов).

Были разработаны три функции для зашифрования, расшифрования и создания таблицы Порты.

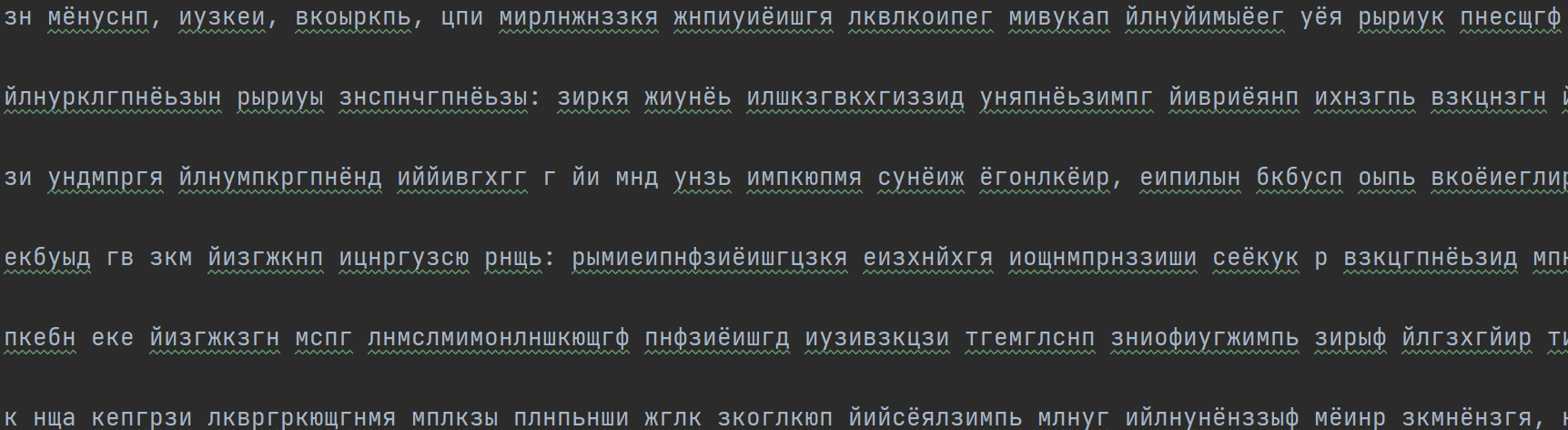


Листинг 1.1 – Входные данные на русском языке



Листинг 1.2 – Выходные данные зашифрованные шифром Порты

Были разработаны две функции для зашифрования и расшифрования сообщений в/из шифра Цезаря с ключом. Ключ – коршун.



Листинг 1.3 – Выходные данные зашифрованные шифром Цезаря с ключом



Рисунок 1.1 – Гистограмма частот символов в оригинальном сообщении



Рисунок 1.2 – Гистограмма частот символов в шифре Цезаря с ключом

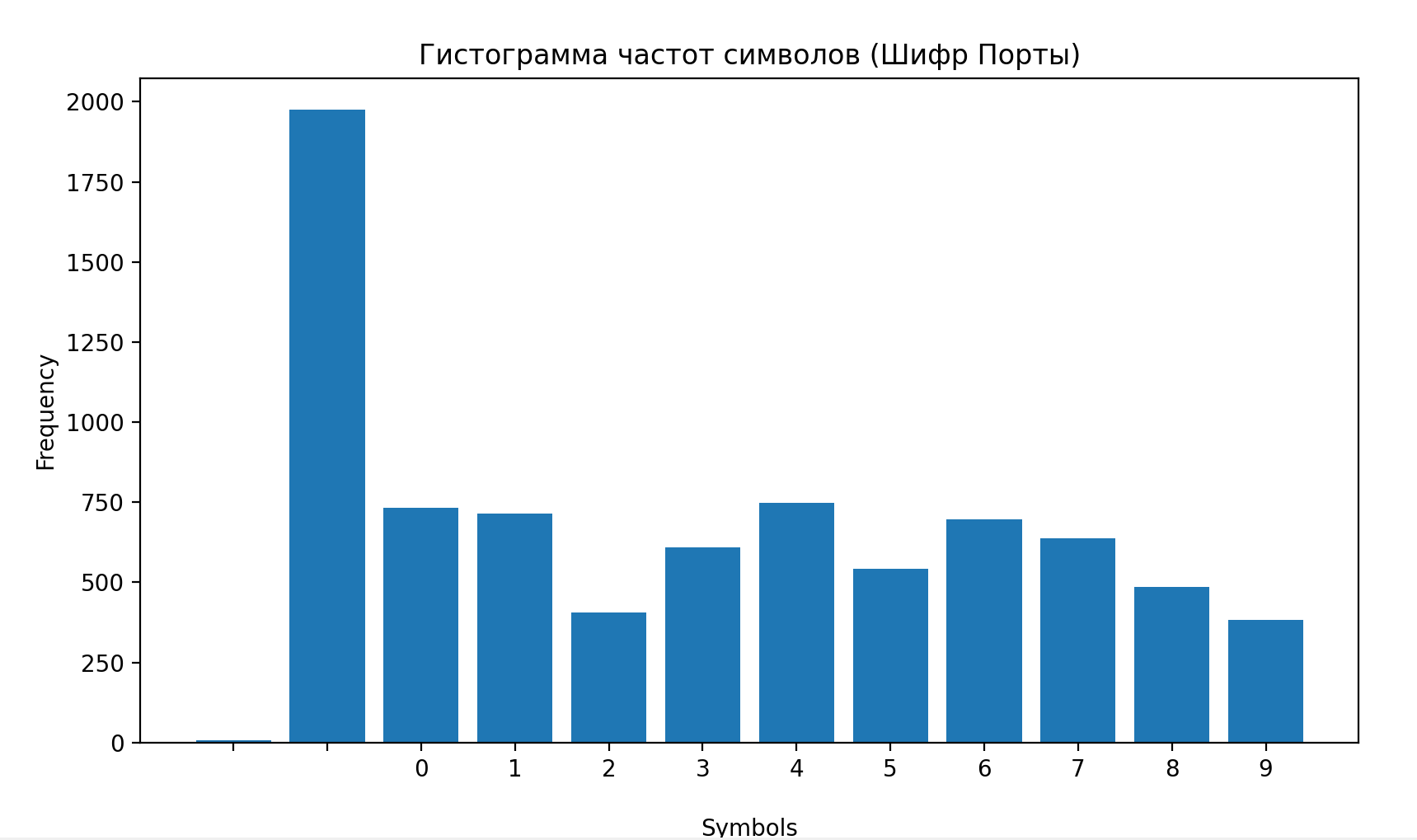


Рисунок 1.3 – Гистограмма частот символов в шифре Порты

Также было замерено время зашифрования и расшифрования для каждого шифра.

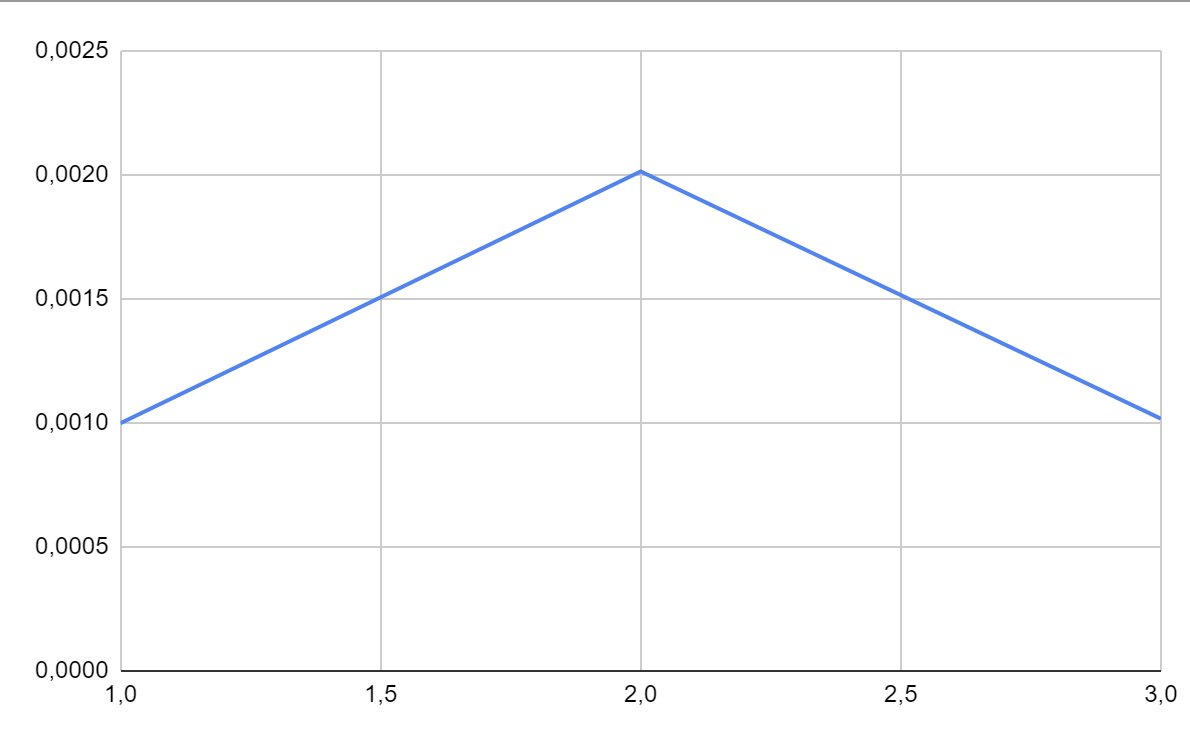


Рисунок 1.4 – Время зашифрования в шифр Цезаря с ключом

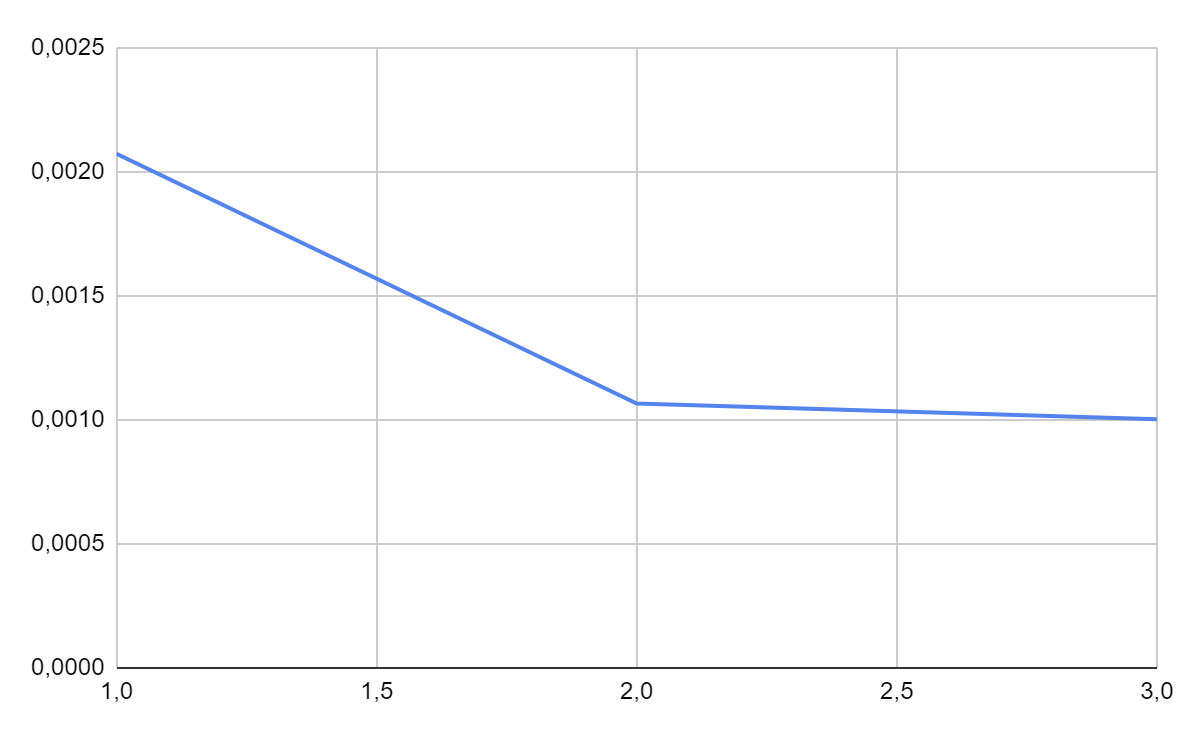


Рисунок 1.5 – Время расшифрования из шифра Цезаря с ключом

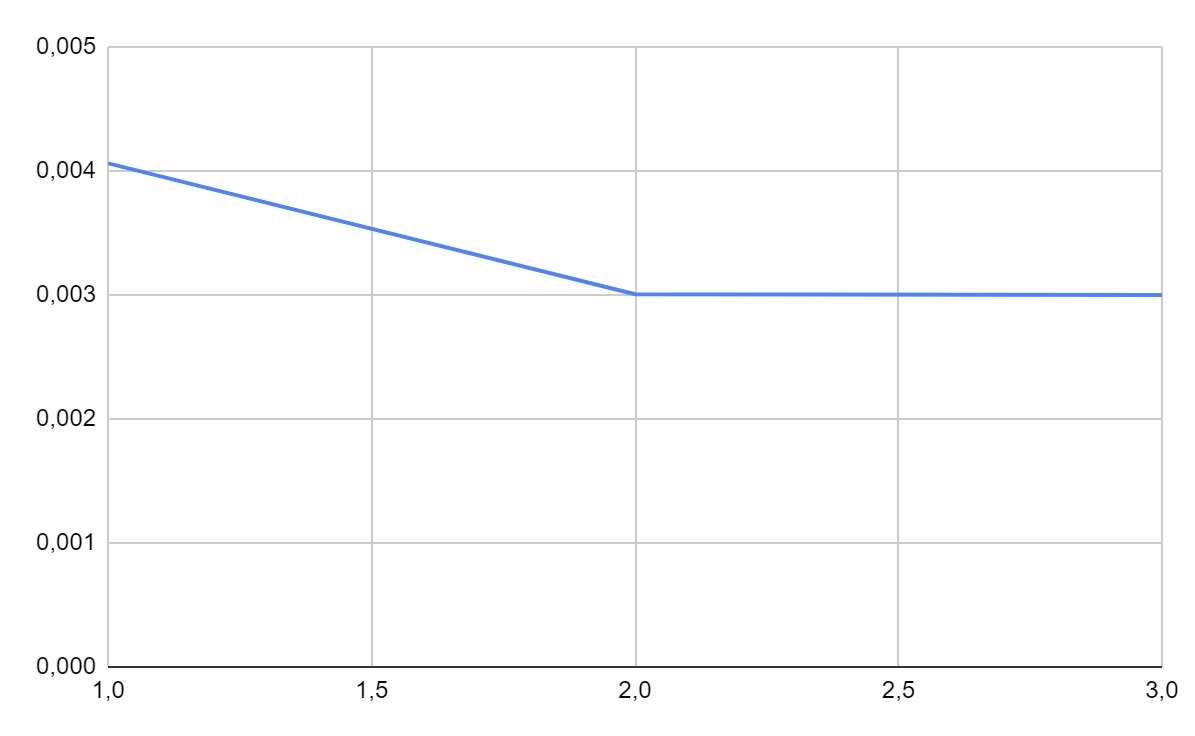


Рисунок 1.6 – Время зашифрования в шифра Порта

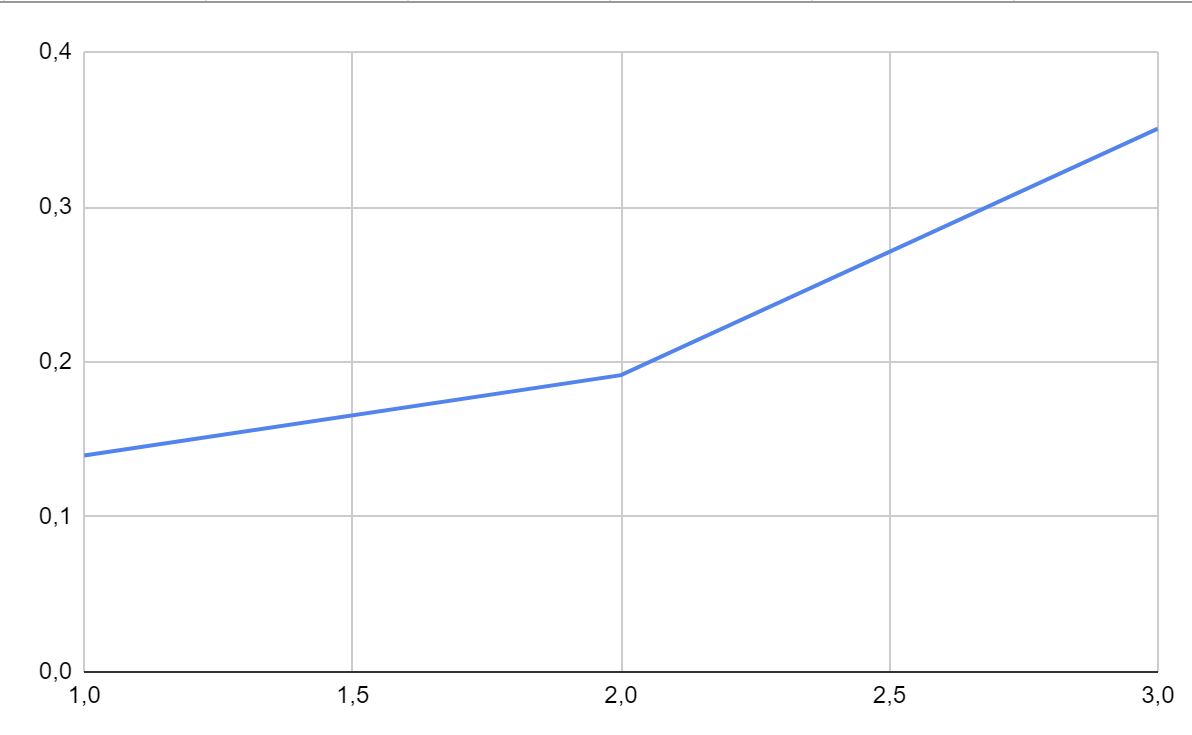


Рисунок 1.7 – Время расшифрования сообщения из шифра Порты

**Вывод:** Из полученных результатов видно, что шифр Цезаря работает значительно быстрее шифра Порты как при зашифровании, так и при расшифровании текста. Однако шифр Порты обладает более высокой степенью надежности благодаря использованию полиграфического метода шифрования.

При необходимости обеспечения более высокого уровня безопасности данных, лучше использовать шифр Порты, несмотря на его более высокую вычислительную сложность.