МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ КЫРГЫЗСКОЙ РЕСПУБЛИКИ

Государственное образовательное учреждение высшего профессионального образования

Кыргызско-Российский Славянский университет

Естественно-Технический факультет

Кафедра Информационно-вычислительных технологий

**Отчет к лабораторной работе**

**По дисциплине «Методы и средства защиты информации»**

**на тему «Реализация алгоритма шифрования, использующего линейные преобразования (Шифр Хилла)»**

Выполнил:

Студент 4 курса

Группы ЕПИ-1-20

Астаркулов А.С.

Проверил:

Демиденко А.П.

г. Бишкек 2023 г.

# Условие задачи

Реализация алгоритма шифрования, использующего линейные преобразования (Шифр Хилла). Матрица ключа выбирается размерностью от 2x2 до 6x6 и заполняется вручную и генератором случ. чисел. Реализовать

взлом шифра Хилла с использованием фрагментов исходного и шифрованного текста

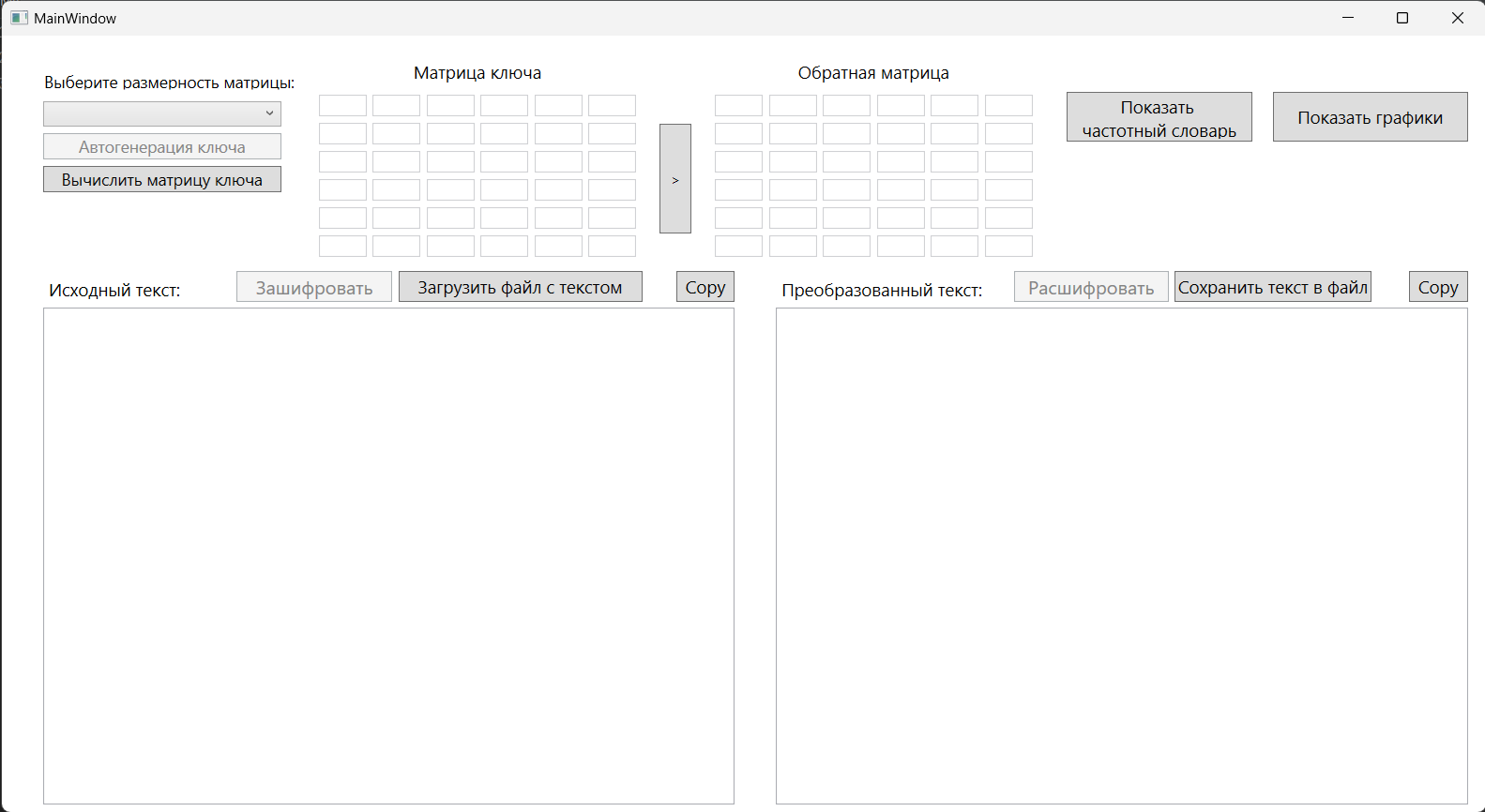
Реализация шифра Хилла.

Нахождение ключа, используя фрагменты исходного и шифрованного текста.

График частотных характеристик алгоритма.

# Выполненные задачи

1. Реализация алгоритма шифрования, использующего линейные преобразования (Шифр Хилла)
2. Нахождение ключа, используя фрагменты исходного и шифрованного текста
3. Построение частотного словаря. Разработан алгоритм построения частотного словаря для анализа текста.
4. Построение графиков частотного словаря



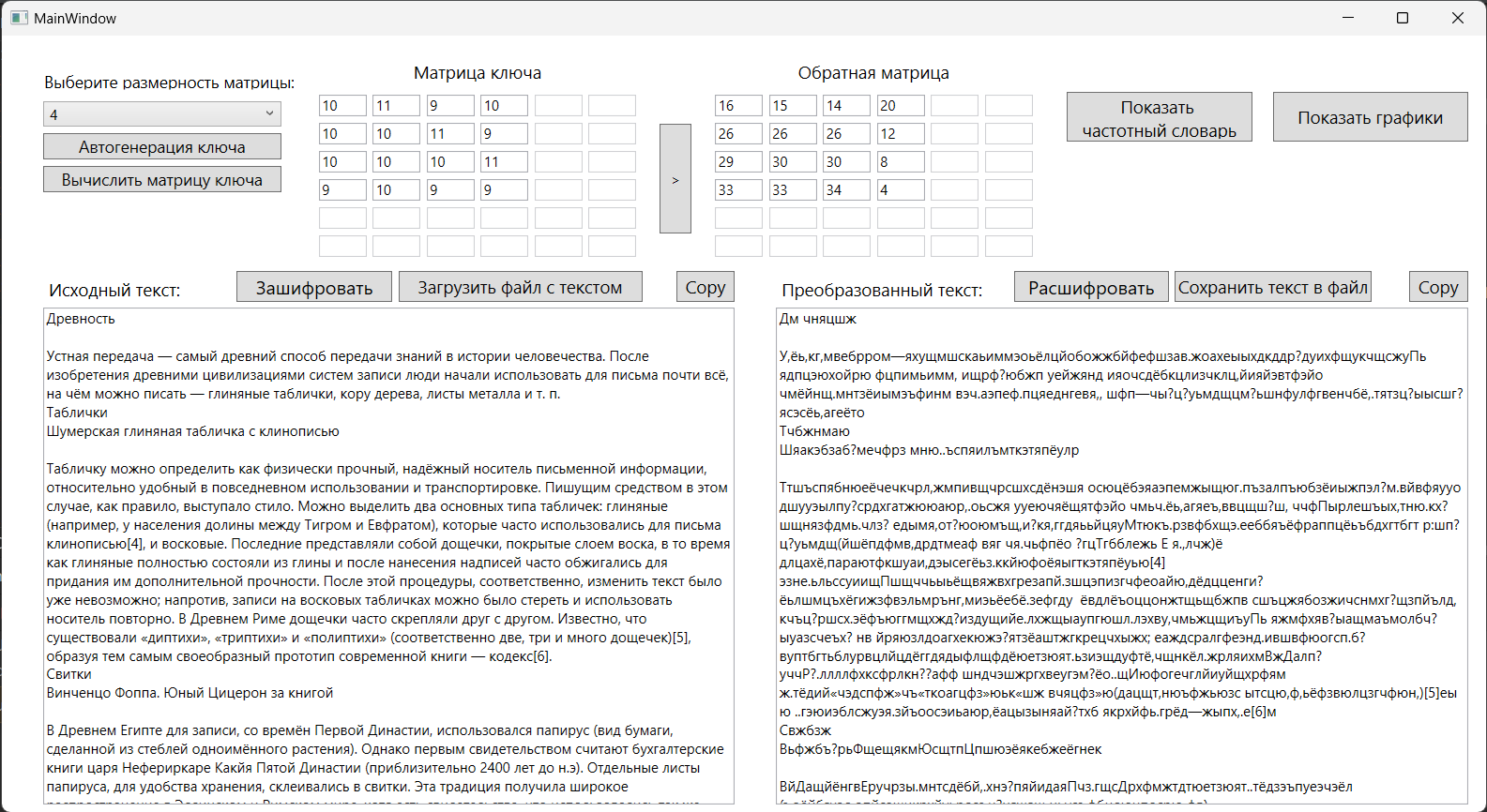
*Рис.1. Интерфейс программы*

Программа была разработана на языке C#, с использованием библиотеки WPF.

В верхней части программы находятся элементы управления: выбор размерности матрицы, кнопка «Автогенерация ключа» для генерации матрицы ключа, кнопка для показа частотного словаря, кнопка для показа графиков частотного словаря, ниже находятся поля для ввода текста и поле где будет зашифрованный текст, выше над полями находятся кнопки «Зашифровать», «Загрузить файл с текстом», «Copy» для копирования текста внутри поля, правее находятся кнопки «Расшифровать», «Сохранить текст в файл»

# Описание выполненных задач

1.Реализация алгоритма шифрования, использующего линейные преобразования (Шифр Хилла)

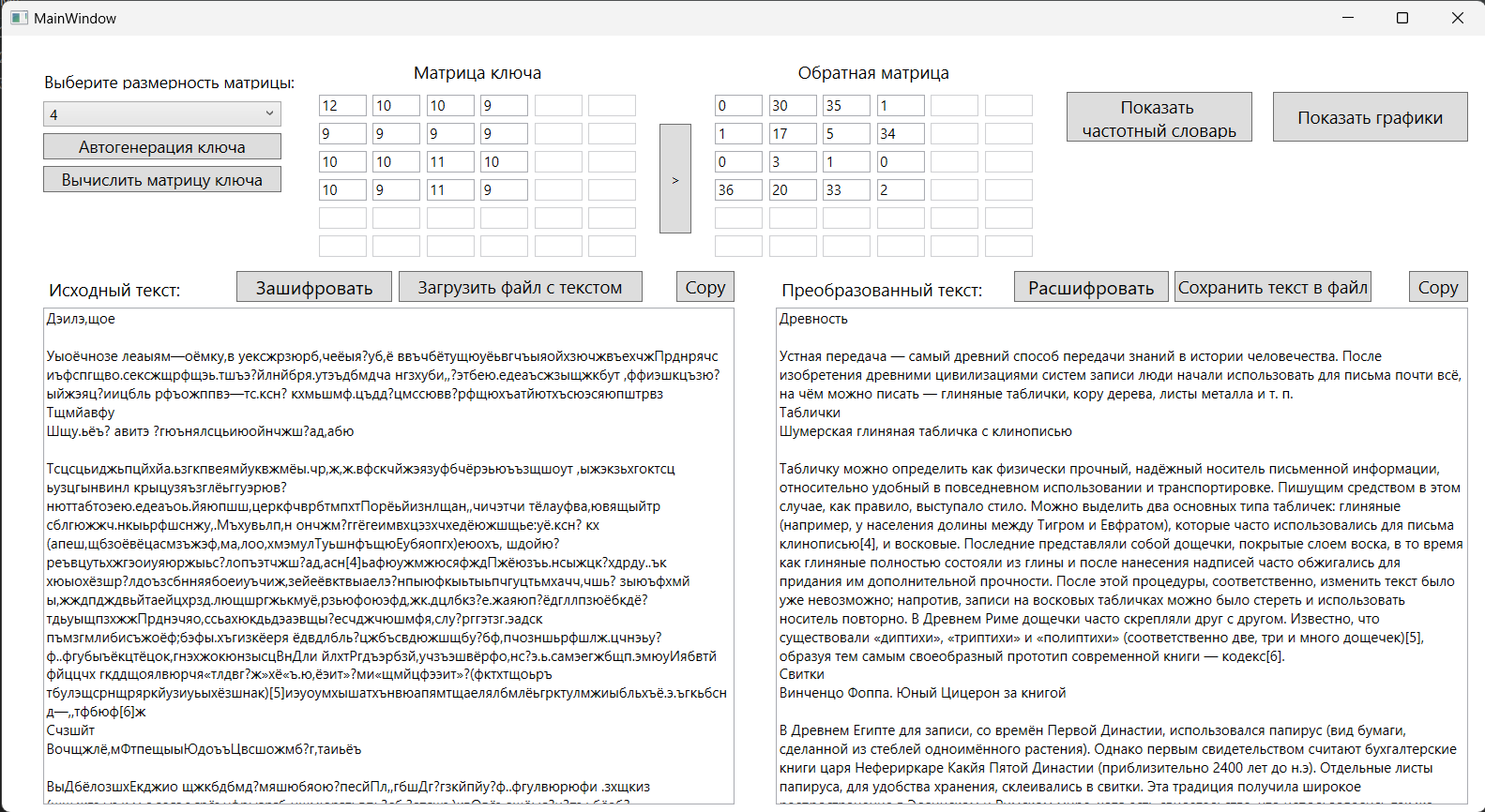


*Рис.2. Шифрование*

Шифр Хилла (Hill cipher) - это метод шифрования, который использует матрицу для преобразования текста. Он был разработан Лестером С. Хиллом в 1929 году. Шифр Хилла шифрует текст, разбивая его на блоки символов и умножая каждый блок на заданную матрицу. Результатом является зашифрованный текст, который можно далее передавать безопасно.

Основные шаги работы шифра Хилла:

* Генерация ключевой матрицы: Ключевая матрица должна быть обратимой и обычно представляет собой квадратную матрицу. Она используется для шифрования и дешифрования данных.
* Разбиение текста на блоки: Оригинальный текст разделяется на блоки равной длины.
* Умножение блоков на ключевую матрицу: Каждый блок символов умножается на ключевую матрицу и делится по модулю на размер алфавита. Результатом является зашифрованный блок символов.
* Объединение зашифрованных блоков: Зашифрованные блоки объединяются, чтобы получить зашифрованный текст.
* Расшифровка: Чтобы расшифровать текст, нужно знать обратную матрицу ключевой матрицы и выполнить обратное умножение.
* Основным преимуществом шифра Хилла является его способность работать с большими блоками текста и обеспечивать хорошую степень безопасности. Однако внимание к математическим деталям и обратимости ключевой матрицы важно для успешного применения этого шифра.

*Рис.3. Расшифровка*

2.Нахождение ключа, используя фрагменты исходного и шифрованного текста

Это процедура нахождения ключа шифра Хилла с использованием фрагментов исходного и зашифрованного текстов. Обратите внимание, что эффективность этого метода зависит от количества и качества выбранных фрагментов, а также от сложности ключа.

Для нахождения ключа шифра Хилла по фрагментам исходного текста и соответствующим фрагментам зашифрованного текста:

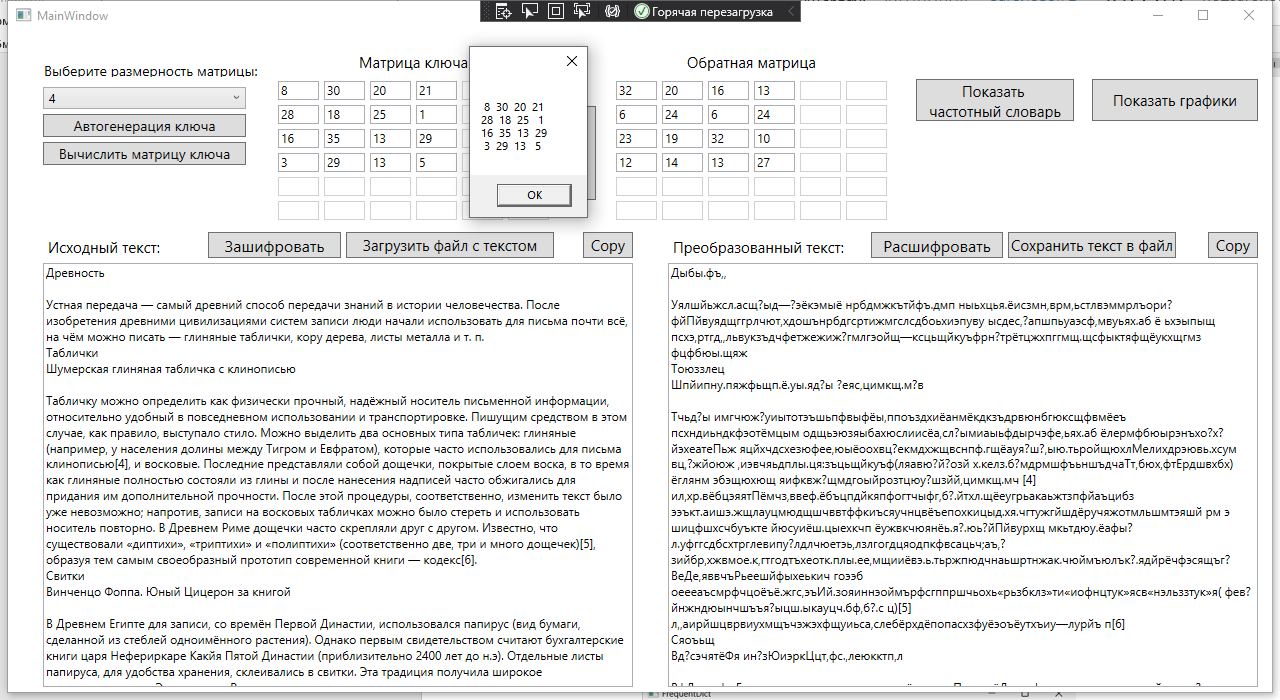
1. Выбрать фрагменты исходного и зашифрованного текстов.

2. Представить их как матрицы символов.

3. Составить систему уравнений: Матрица ключа = Обратная матрица фрагмента исходного текста \* Матрица фрагмента зашифрованного текста mod Длина алфавита

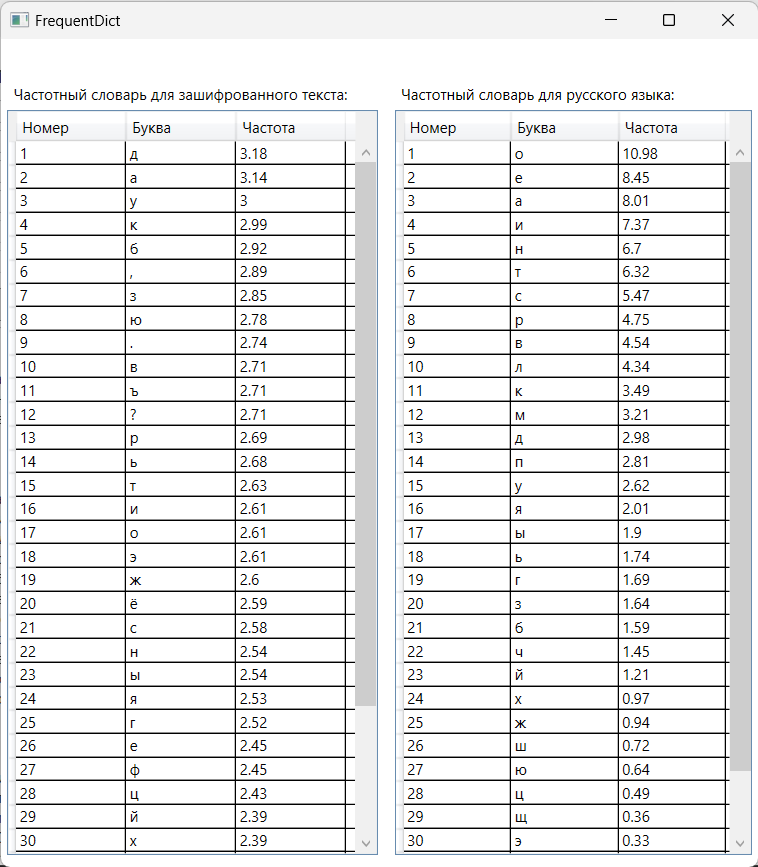
4. Решить систему уравнений, чтобы найти ключевую матрицу.

5. Проверить, что ключ обратим и правильно расшифровывает другие фрагменты текста.

**

*Рис.4. Вычисление матрицы ключа*

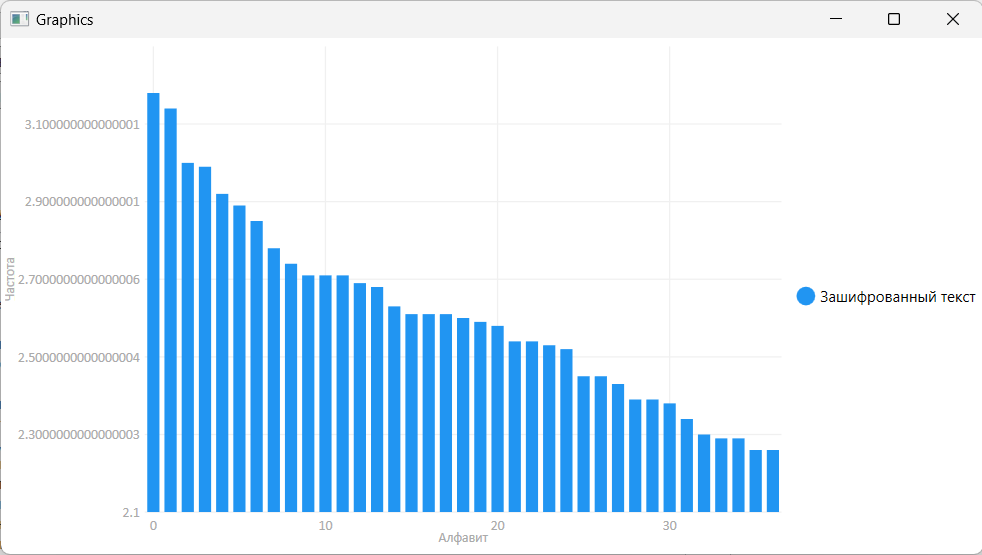
3.Построение частотного словаря. Разработан алгоритм построения частотного словаря для анализа текста.

Для проведения частотного анализа был разработан алгоритм построения частотного словаря. Этот словарь содержит информацию о частоте каждой буквы или символа в тексте.

*Рис.5. Частотный словарь*

4.Построение графиков частотного словаря

Для анализа данных частотного словаря было проведено построение графиков, отражающих частоту встречаемости каждой буквы или символа в анализируемом тексте. Графики предоставляют визуальное представление статистики по тексту, что может быть полезно при анализе текстов на предмет распределения символов.



*Рис.6. График частотного словаря*

# Выводы

В ходе выполнения лабораторной работы были изучены и реализованы алгоритм шифрования, использующего линейные преобразования. Был также рассмотрен метод нахождения ключа с помощью исходного текста и зашифрованного. Были успешно построены графики частотного словаря, которые предоставляют дополнительную информацию о распределении символов в анализируемом тексте.

В процессе выполнения лабораторной работы были приобретены навыки работы с шифром Хилла, алгоритмом шифрования, что может быть полезно при изучении криптографии и информационной безопасности.