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

Ивженко Кирилл

Проверил:

Демиденко А.П.

г. Бишкек 2023 г.

# Задача

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

Реализовать взлом шифра Хилла с использованием фрагментов исходного и шифрованного текста

Содержание

* Реализация шифра Хилла.
* Нахождение ключа, используя фрагменты исходного и шифрованного текста.
* График частотных характеристик алгоритма.

# Шифр Хилла

Шифр Хилла - это метод шифрования, который использует матрицу для преобразования блоков текста. Когда текст шифруется, он разбивается на блоки размером N, и каждый блок представляется в виде вектора-столбца длиной N, где каждый элемент представляет символ, представленный числом (например, A=0, B=1, и т. д.).

Шифрование: Каждый блок текста умножается на матрицу-ключ размера N x N, что дает зашифрованный блок. Результат берется по модулю размера алфавита (обычно 26 для английского алфавита). Зашифрованные блоки затем объединяются в зашифрованный текст.

Дешифрование: Зашифрованный текст разбивается на блоки длиной N, и каждый блок умножается на обратную матрицу-ключ (если существует) по модулю размера алфавита. Результат объединяется в исходный текст.

Выбор ключевой матрицы: При выборе матрицы-ключа важно, чтобы она была обратимой. Для обратимости матрицы ее определитель должен быть отличен от нуля. Помимо этого, определитель матрицы не должен иметь общих делителей с размером алфавита, чтобы обеспечить уникальность и невозможность возникновения конфликтов при дешифровании.

При выполнении этих шагов важно убедиться, что математические ограничения соблюдаются, чтобы обеспечить успешное шифрование и дешифрование.

# Условия Генерации Ключа

детерминант != 0 и длина алфавита должна быть взаимно простой с детерминантом ключа

# Получение ключа

Извлечение ключа шифра Хилла из зашифрованного текста и исходного текста — это процесс, который включает несколько шагов матричных операций и решения системы линейных уравнений. Сначала тексты представляются в виде матриц, затем уравнение, описывающее процесс шифрования, записывается с использованием ключевой матрицы. Для извлечения ключа необходимо вычислить обратную матрицу открытого текста и затем решить уравнение для получения ключевой матрицы. Полученные числовые значения в ключевой матрице затем интерпретируются обратно в буквенный ключ шифра. Однако процесс усложняется, если ключевая матрица необратима или если матрица слишком велика.

# Программа

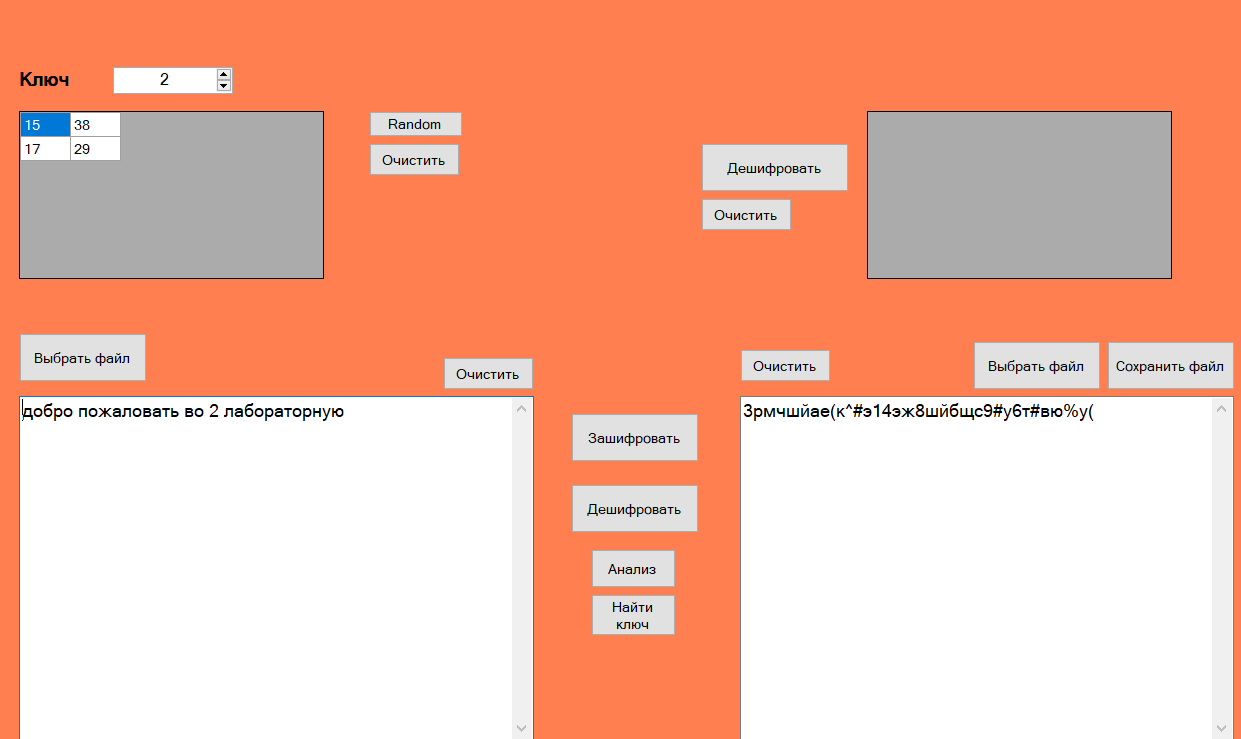


Рисунок 1 Шифровка и Дешифровка С помощью Шифра Хилла

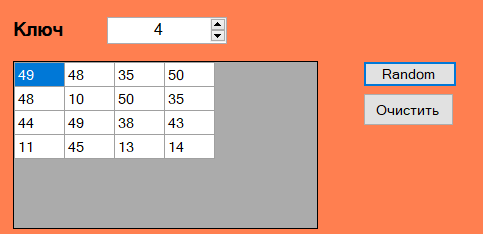


Рисунок 2 Генерация ключа, при этом должны выполняться условия описанные выше

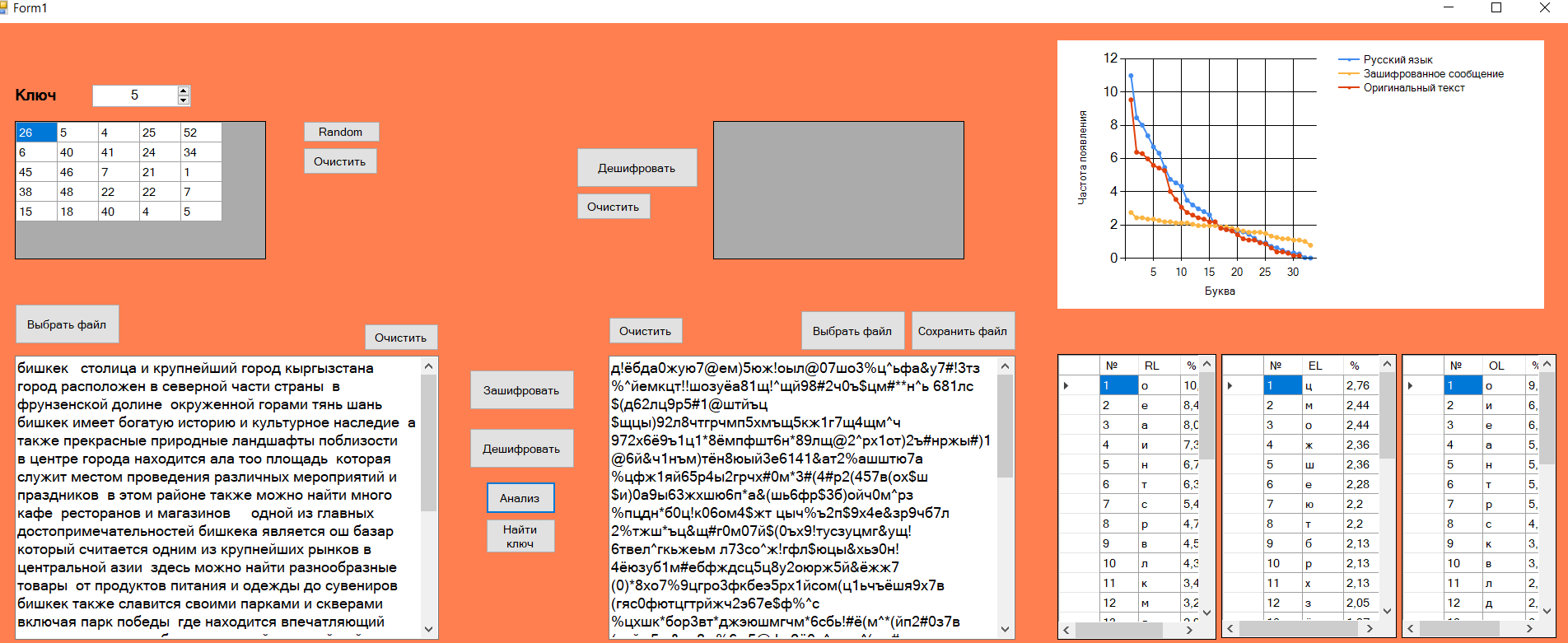


Рисунок 3 Частотные характеристики

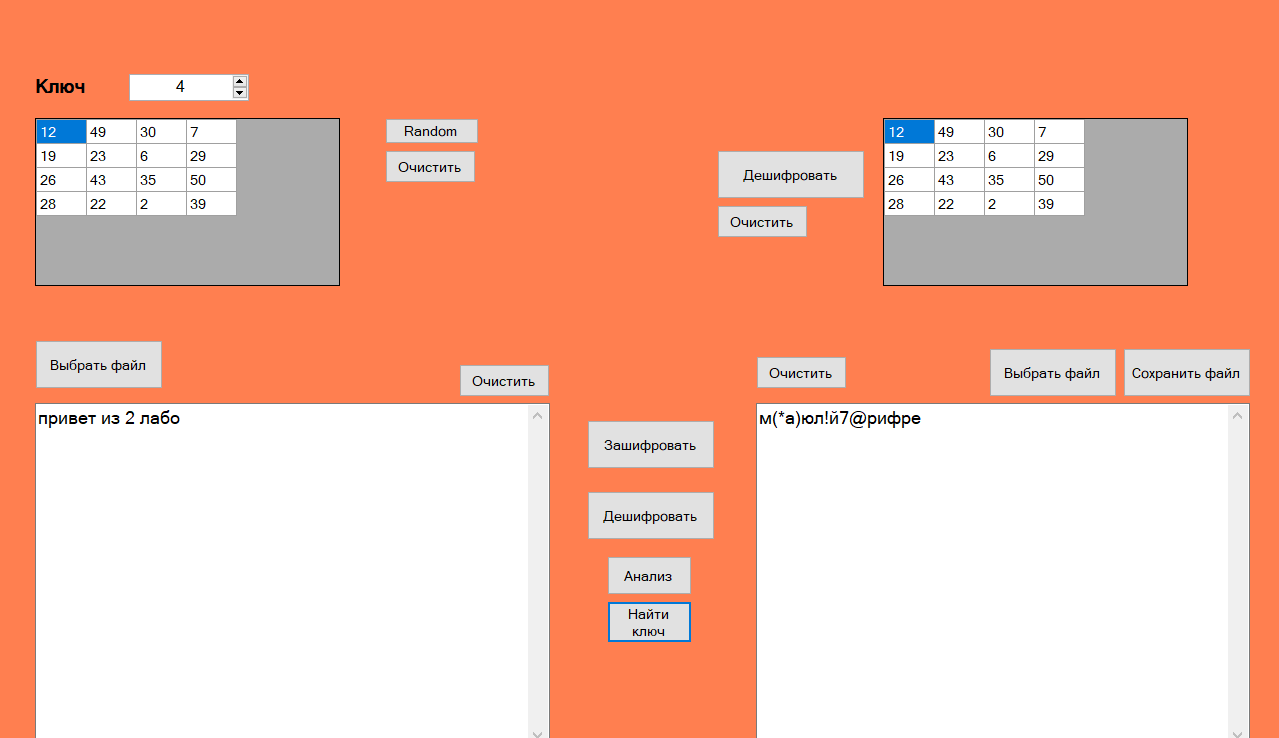


Рисунок 4 Нахождение ключа с использованием исходного и шифрованного текста

# Заключение

Данная лабораторная работа была выполнена, т.е. все задачи поставленные вначале были выполнены, а именно - Шифрование и Дешифрование Шифром Хилла, построение частотного словаря, Нахождение ключа, используя фрагменты исходного и шифрованного текста.