**Лабораторная работа № 5**

**Исследование криптографических шифров на основе перестановки символов**

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

**Задачи:**

1. Закрепить теоретические знания по алгебраическому описанию, алгоритмам реализации операций зашифрования/расшифрования и оценке криптостойкости перестановочных шифров.

2. Ознакомиться с особенностями реализации и свойствами различных перестановочных шифров на основе готового программного средства (L\_LUX).

3. Разработать приложение для реализации указанных преподавателем методов перестановочного зашифрования/расшифрования.

4. Выполнить исследование криптостойкости шифров на основе статистических данных о частотах появления символов в исходном и зашифрованном

сообщениях.

5. Оценить скорость зашифрования/расшифрования реализованных способов шифров.

6. Результаты выполнения лабораторной работы оформить в виде описания

разработанного приложения, методики выполнения экспериментов с использованием приложения и результатов эксперимента

**Вариант 15 (5)**.

**Основное** **задание**.

1. 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;

|  |  |
| --- | --- |
| 5 польский | 1. Маршрутная перестановка (маршрут запись –  по столбцам, считывание – по строкам таблицы;  параметры таблицы – по указанию преподавателя)  2. Множественная перестановка, ключевые  слова – собственные имя и фамилия (aliaksei charniauski) |

• формировать гистограммы частот появления символов для исходного и зашифрованного сообщений;

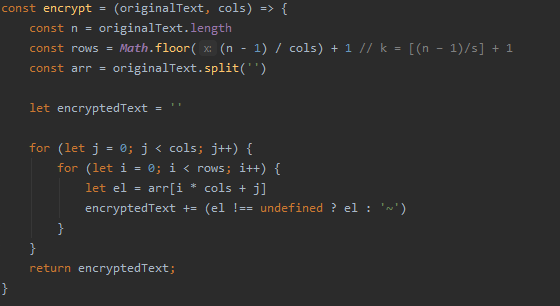
• оценивать время выполнения операций зашифрования/расшифрования

(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).

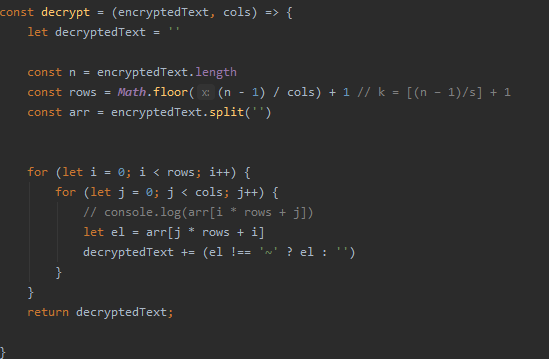
**Листинги:**

**Часть 1**

Функция зашифрования

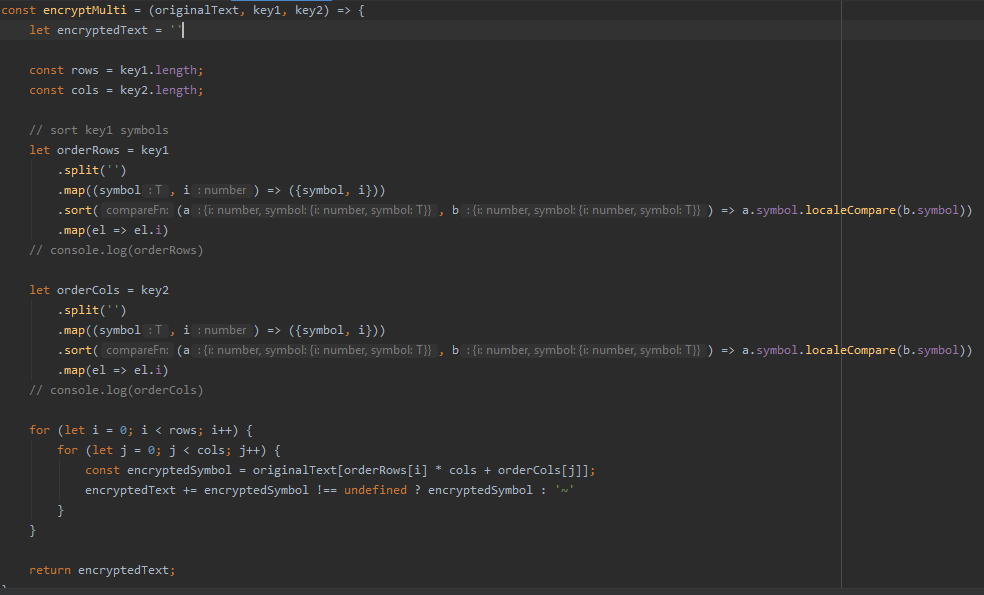


Функция расшифрования

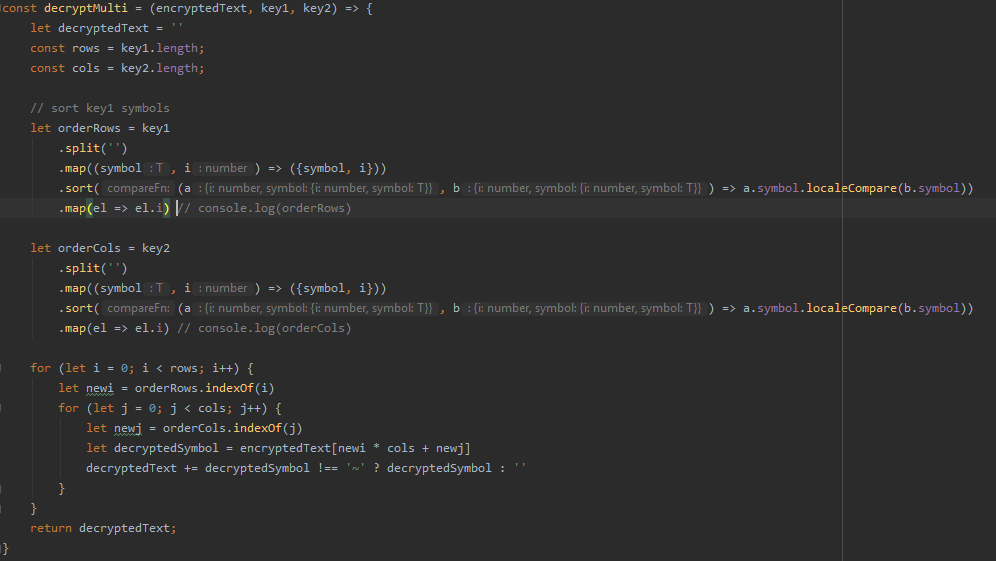


**Часть 2**

Функция зашифрования



Функция расшифрования

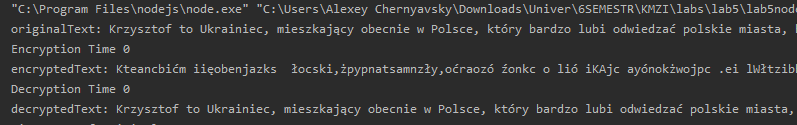


Функция вывода гистограммы

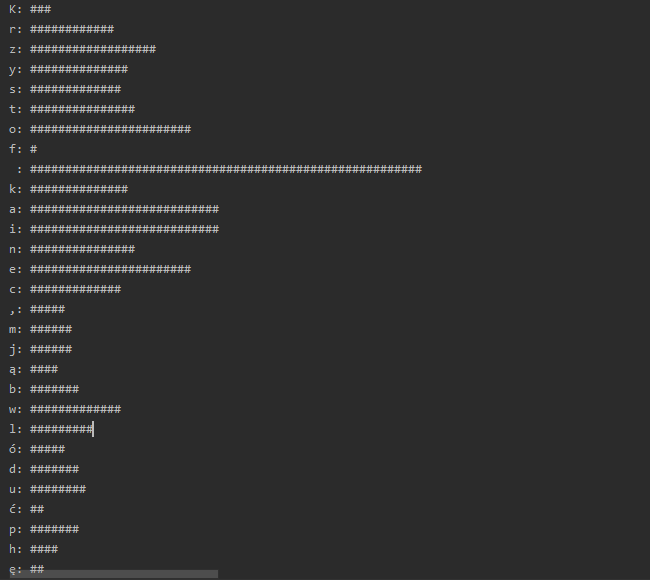


**Контрольный пример:**

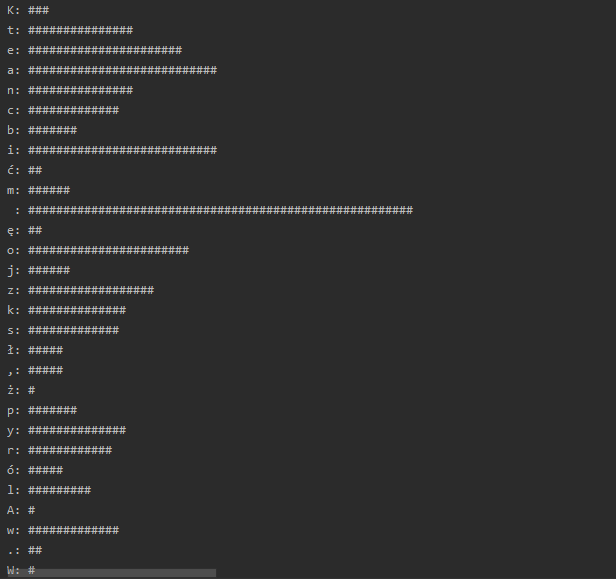
**1)**



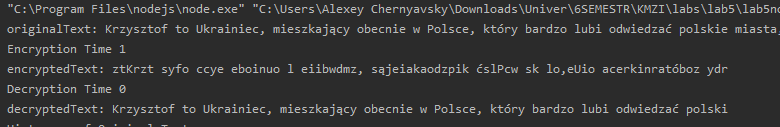
**Гистограмма исходного текста:**



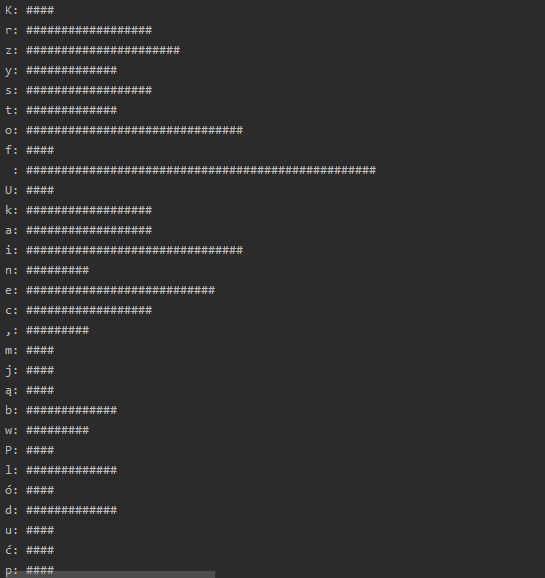
**Гистограмма зашифрованного текста:**



**2)**



**Гистограмма исходного текста:**



**Гистограмма зашифрованного текста**

