Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Исследования криптографических шифров на основе перестановки символов**

Студент: Яскович М.Э.

ФИТ 3 курс 6 группа

Преподаватель: Сазанова Д.В.

Минск 2023

1. **Описание приложения**

Приложение написано на языке программирования Java и позволяет зашифровать и расшифровать текстовый документ на основе польского языка с помощью:

* маршрутной перестановки (запись – по столбцам, считывания – по строкам таблицы);
* множественной перестановки, ключевые слова – собственные имя и фамилия;

Также приложение позволяет:

* формировать гистограммы частот появления символов для исходного и зашифованного сообщений;
* оценивать время выполнения операций за(рас)шифрования.

1. **Методика выполнения поставленных задач**

Для зашифрования исходного текста использована простая маршрутная перестановка. Сначала исходная строка разбивается на подстроки длиной k (ключ), после чего последовательно считываются первый символ каждой подстроки, затем второй и т.д. по возрастанию. Реализация данного алгоритма представлена на рисунке 2.1.

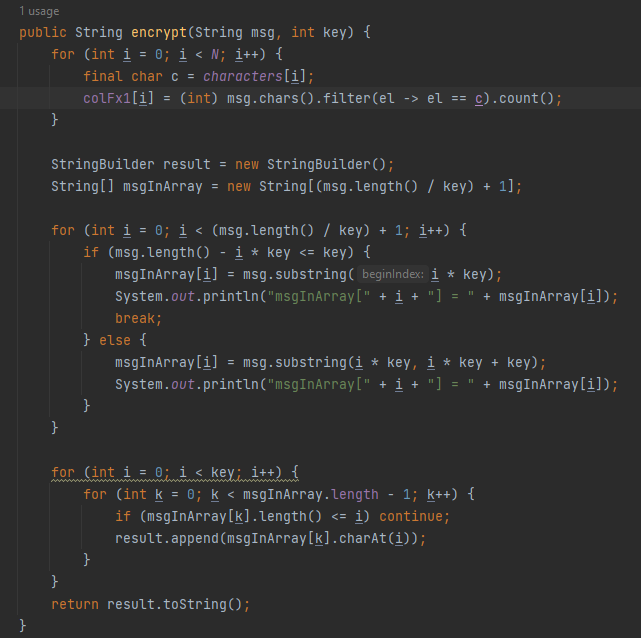


Рис. 2.1 – Реализация маршрутной перестановки

Для множественной перестановки используются ключи «ЮЛИЯ» и «ЧИСТЯКОВА», то есть соответствующие им порядки расположения символов в алфавите – «2103» и «725683410». Сначала исходная строка разбивается на подстроки длиной 4 (длина первого ключа), которые выводятся на консоль. Затем каждый символ a[ij] образовавшейся таблицы ставится в позицию [k1[i] k2[j]] соответствующего значения элемента ключа. Считывания производится по строкам. Реализация функции шифрования представлена на рисунке 2.2.

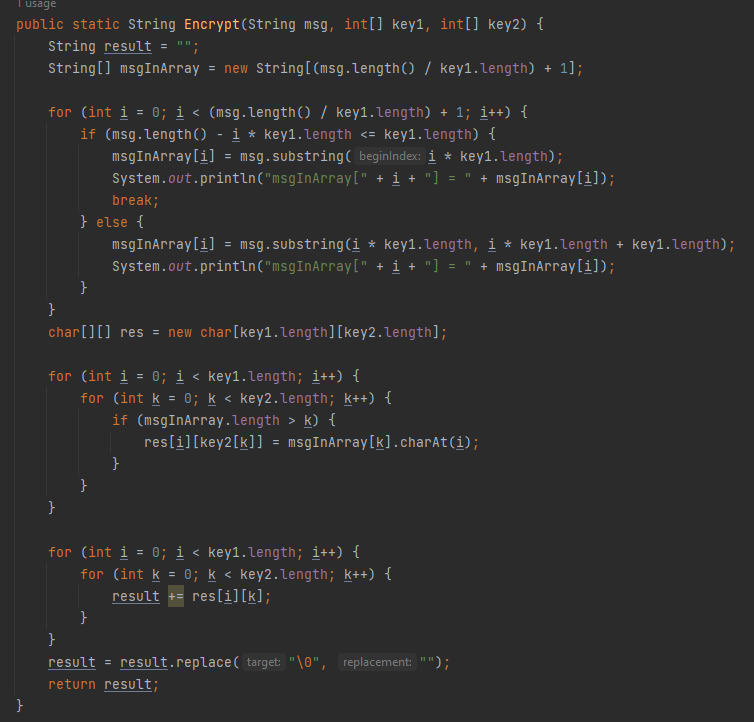
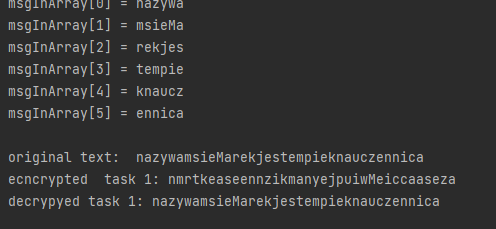


Рисунок 2.2 – Функция множественной перестановки

Промежуточные результаты разбивания исходной строки на подстроки а также конечные результаты зашифрования и затраченное время выводятся на консоль, представленную на рисунке 2.3.



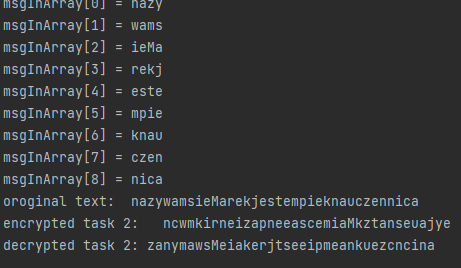


Рисунок 2.3 – Результаты выполнения функций

Приложение также генерирует гистограммы появления частот символов в исходном и зашифрованном тексте. Поскольку мы используем шифры перестановки, а не замены, то частоты появления символов остаются неизменными после зашифрования. Полученная гистограмма представлена на рисунке 2.4.

**Вывод**

В ходе лабораторной работы были приобретены навыки разработки и использования приложений для реализации перестановочных шифров.