Учреждение образования

«Белорусский государственный технологический университет»

**Кафедра информационных систем и технологий**

**«Отчёт по лабораторной работе №3»**

“ИССЛЕДОВАНИЕ КРИПТОГРАФИЧЕСКИХ ШИФРОВ НА ОСНОВЕ ПЕРЕСТАНОВКИ СИМВОЛОВ ”

**Выполнил:** студент 3 курса

3 группы специальности ИСИТ

Шедько Евгений Александрович

**Проверил:** преподаватель

Копыток Дарья Владимировна

Минск 2022

**Вариант 14**

**1. Перед выполнением задания ознакомиться с работой программы.** Исходный текст представлен на Рис.1. Результат шифрования на основе простой перестановки при использовании программы представлен на Рис. 2. Гистограммы распределения частот для исходного и зашифрованного текста на Рис. 3.

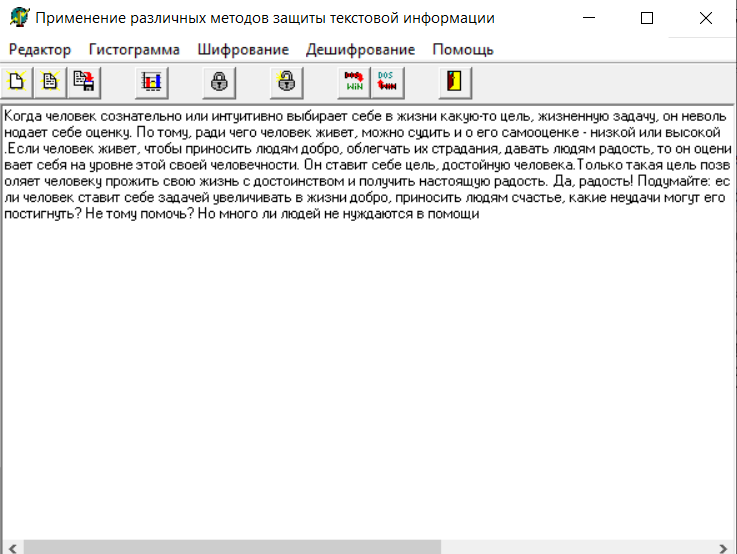


Рисунок 1 - Исходный текст для шифрования

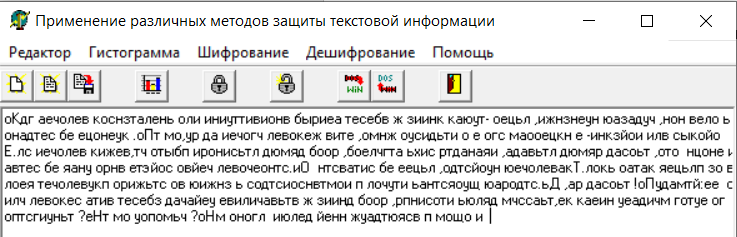


Рисунок 2 - Результат применения шифрования на основе простой перестановки

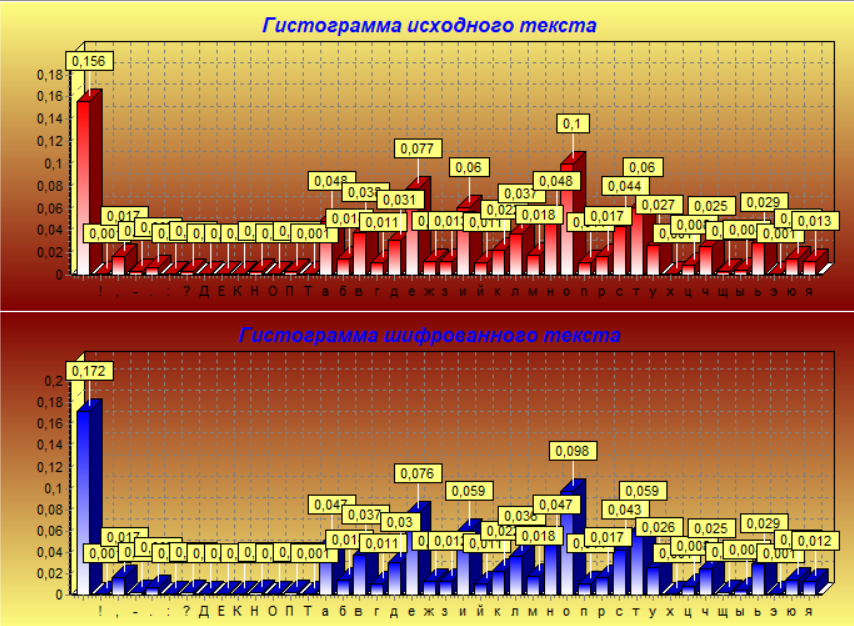


Рисунок - 3 Гистограммы распределения частот

**2. Разработать авторское приложение в соответствии с целью лабораторной работы. Приложение должно реализовывать следующие операции:**

• выполнять зашифрование/расшифрование текстовых документов (объемом не менее 5 тысяч знаков), созданных на основе алфавита Исследование криптографических шифров на основе подстановки (замены) символов языка в соответствии с нижеследующей таблицей вариантов задания; при этом следует использовать шифры подстановки из третьего столбца данной таблицы (вариантызадания представлены в табл. 2.6);

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

• оценить 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)).

Исходный текст представлен на Рис.4.

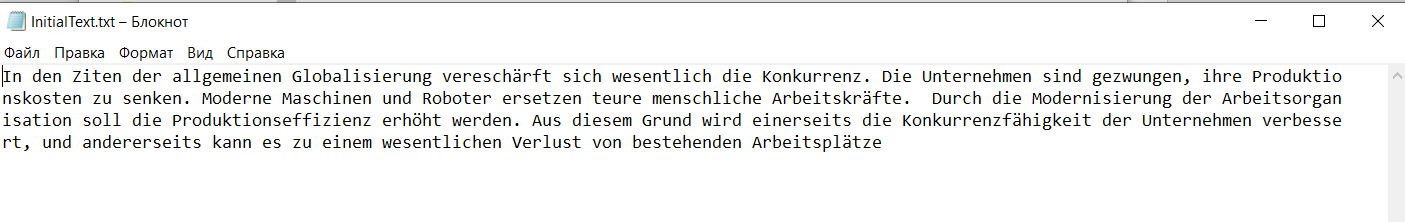


Рисунок 4 - Исходный текст для шифрования

Результат шифрования, используя шифр маршрутной перестановки(змейкой), представлен на Рис. 5.

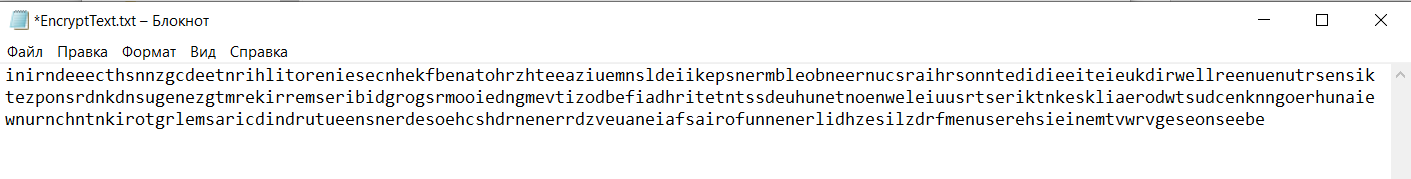


Рисунок - 5 Шифрование маршрутной перестановкой(змейкой)

Результат дешифрования, используя шифр маршрутной перестановки(змейкой), представлен на Рис. 6.

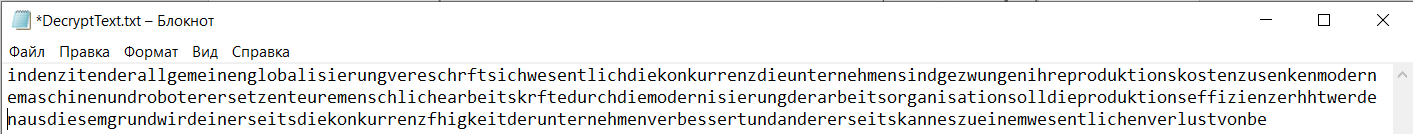


Рисунок 6 - Дешифрование шифром Виженера

Время работы шифрования/дешифрования, используя шифр маршрутной перестановки(змейкой), представлено на Рис. 7 - 8.

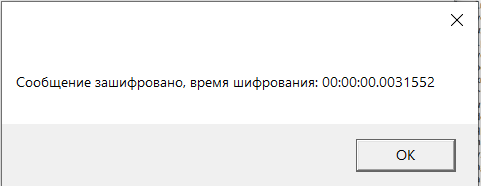


Рисунок 7 - Время работы шифрования

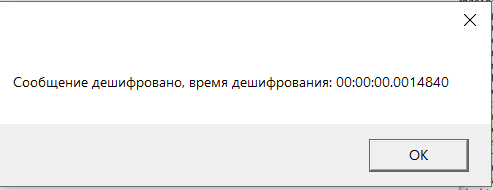


Рисунок 8 - Время работы дешифрования

Гистограммы частот символов, используя шифр маршрутной перестановки(змейкой), представлены на Рис. 9-10.

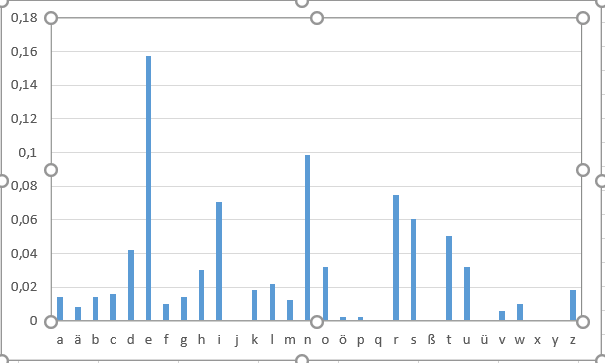


Рисунок 9 - Исходный текст

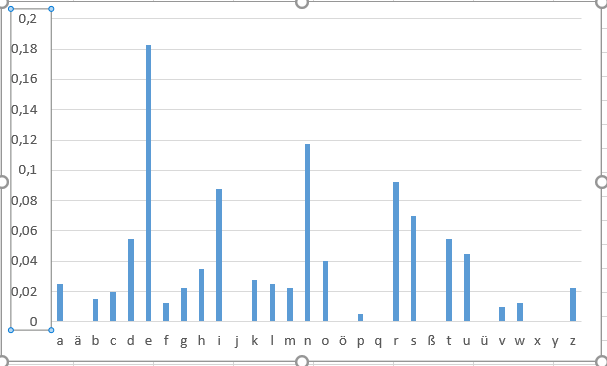


Рисунок 10 - Зашифрованный текст

Результат шифрования, используя шифр множественной перестановки, представлен на Рис. 11.

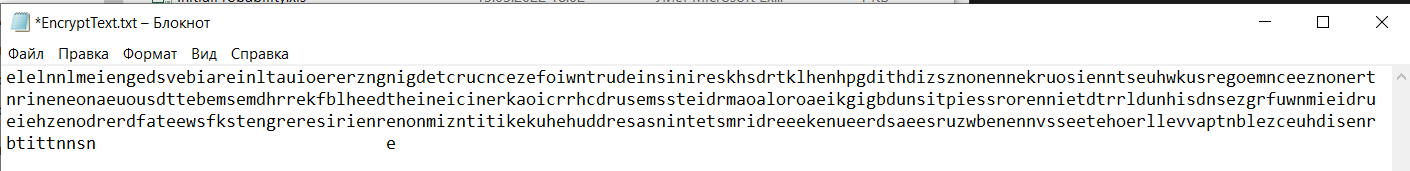


Рисунок 11 - Шифрование шифром множественной перестановки

Результат дешифрования, используя шифр множественной перестановки, представлен на Рис. 12.

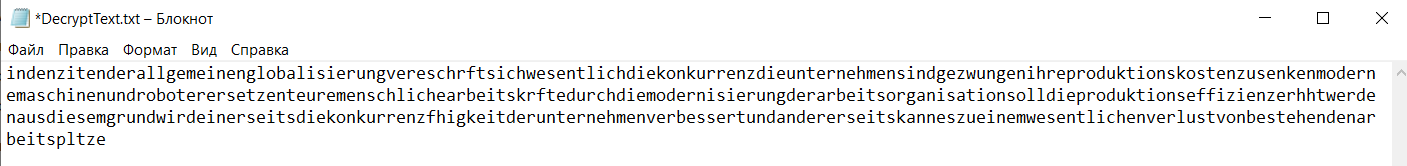


Рисунок 12 - Дешифрование шифром множественной перестановки

Время работы шифрования/дешифрования, используя шифр множественной перестановки, представлено на Рис. 13-14.

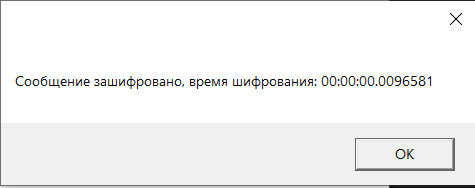


Рисунок 13 - Время работы шифрования

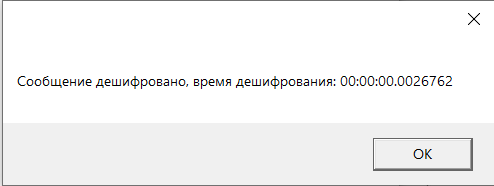


Рисунок 14 - Время работы дешифрования

Гистограммы частот символов, используя шифр множественной перестановки, представлены на Рис. 15.

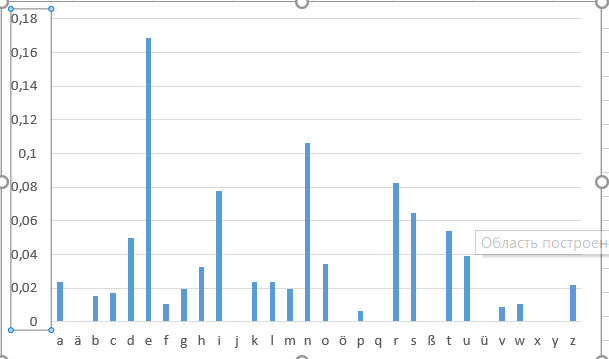


Рисунок 15 - Зашифрованный текст

**Вывод.** В ходе лабораторной работы были изучены криптографические шифры на основе подстановки и получены навыки разработки приложений, реализующие эти шифры.