МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образования «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Факультет Информационных Технологий

Кафедра Информационных систем и технологий

Специальность 1-40 01 01 Программное обеспечение информационных технологий

Направление специальности 1-40 01 01 10 Программирование интернет-приложений

**ОТЧЁТ К ЛАБОРАТОРНОЙ РАБОТЕ №4:**

по дисциплине «Криптографические методы защиты информации»

Тема «ИССЛЕДОВАНИЕ КРИПТОГРАФИЧЕСКИХ ШИФРОВ НА ОСНОВЕ ПОДСТАНОВКИ (ЗАМЕНЫ) СИМВОЛОВ»

Исполнитель

студент 3 курса группы 5 Шулаков Андрей Александрович

(Ф.И.О.)

Руководитель работы преподаватель Савельева М. Г.

(учен. степень, звание, должность, подпись, Ф.И.О.)

Минск 2023

Ход работы

Приложение было разработано на С#. В своем приложении согласно варианту 14 я использовал алфавит немецкого языка, а так же два способа шифрования: шифр Виженера, где ключевое слово - Shulakov и шифр Порты.

Задание №1

В данном задании я разработал шифр Виженера с ключевым словом Shulakov.

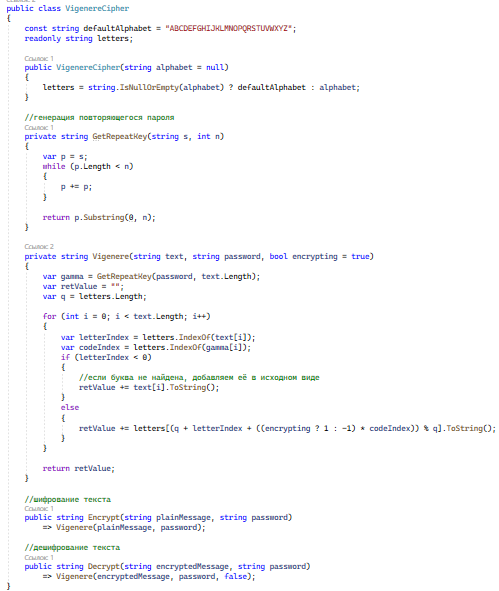


Рисунок 1 — реализация шифра Виженера

Задание №2

В данном задании я разработал шифр Порты. Реализовал данный шифр в виде двух статических методов.

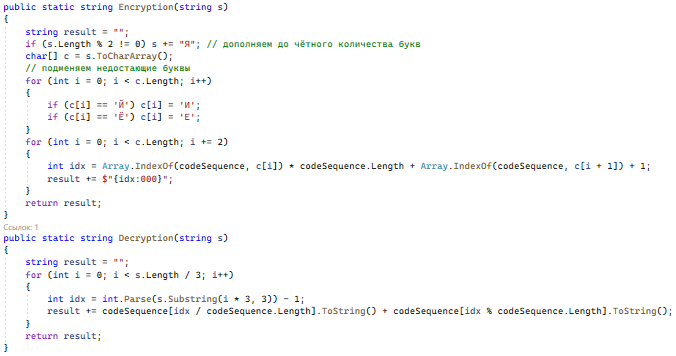


Рисунок 2 — методы Encryption и Decryption для шифра Порты.

Далее был произведен анализ гистограмм. Сами гистограммы представлены на рисунках 3-4. Гистограммы соответствующие частоте появления букв при шифровании и дешифровании текста при шифре Виженера, ключевое слово – Shulakov представлены на рисунках 3, 4 соответственно.



Рисунок 3 — Частота появления букв при шифровании Виженера

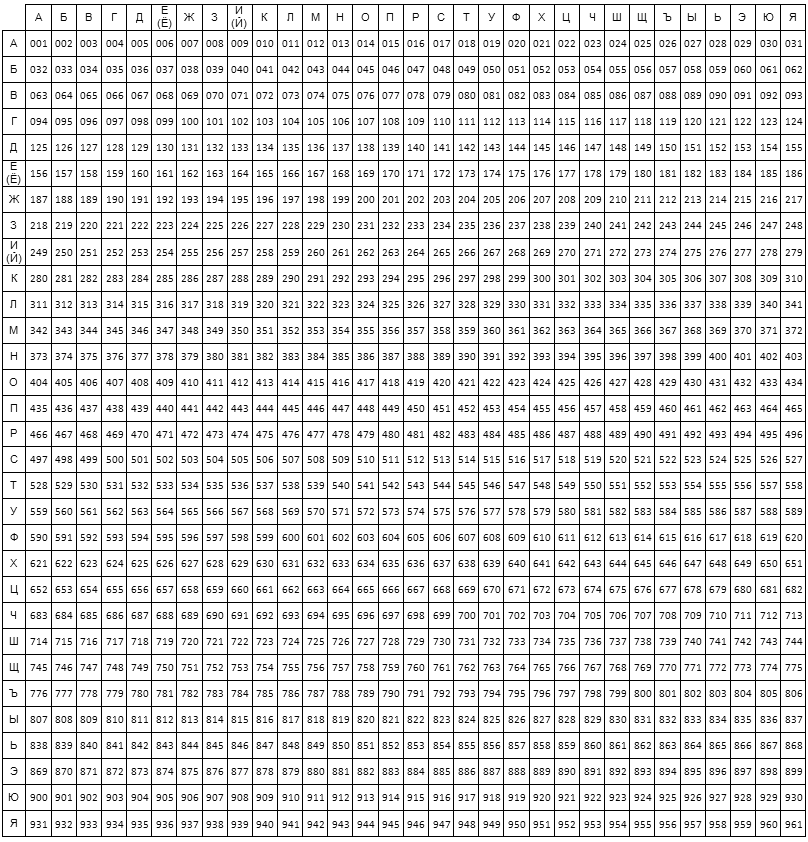


Рисунок 4 — Частота появления букв при дешифровании Виженера



Рисунок 5 — Частота появления букв при шифровании Порты

Шифр Порты для русского алфавита:

Рисунок 6 – шифр Порты

Далее будет приведен график зависимости времени выполнения шифрования и дешифрования от количества символов при разных способах шифрования и дешифрования.

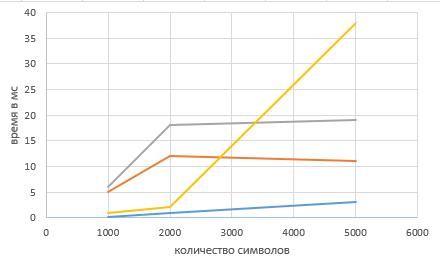


Рисунок 7 – график зависимостей

Оранжевый – шифр Виженера, синий – дешифрование Виженера, серый – шифрование Порты, желтый – дешифрование Порты.

Вывод: была произведена работа с разными шифрами, такими как: шифр Виженера и шифр Порты