МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образование «Белорусский государственный технологический университет»

Кафедра информационных систем и технологий

**«Исследование криптографических шифров на основе подстановки (замены) символов»**

Студент:

Агапкина Диана Сергеевна

Вариант 7

Преподаватель:

Блинова Евгения Александровна

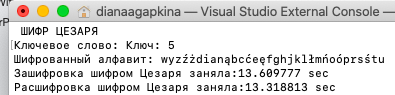
Минск 2020

**ЗАДАНИЕ 1.** Шифр Цезаря

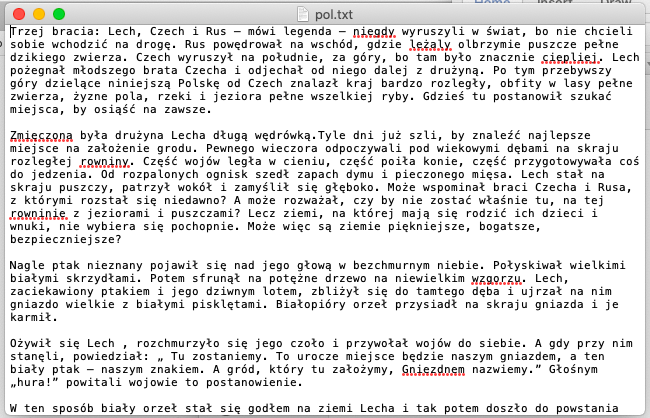
В данной разновидности шифра Цезаря ключ задается числом k (0<=k<=n-1) и коротким ключевым словом или предложением. Выписывается алфавит, а под ним, начиная с k-й позиции, ключевое слово. Оставшиеся буквы записываются в алфавитном порядке после ключевого слова. В итоге мы получаем подстановку для каждой буквы. Требование, чтобы все буквы ключевого слова были различными не обязательно - можно записывать ключевое слово без повторения одинаковых букв. Реализация методов шифрования и расшифровки сообщения представлена ниже.



Результат работы программы.

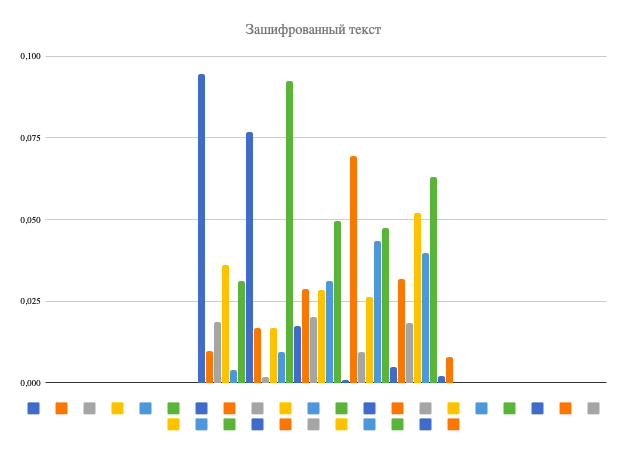


Исходный текст.

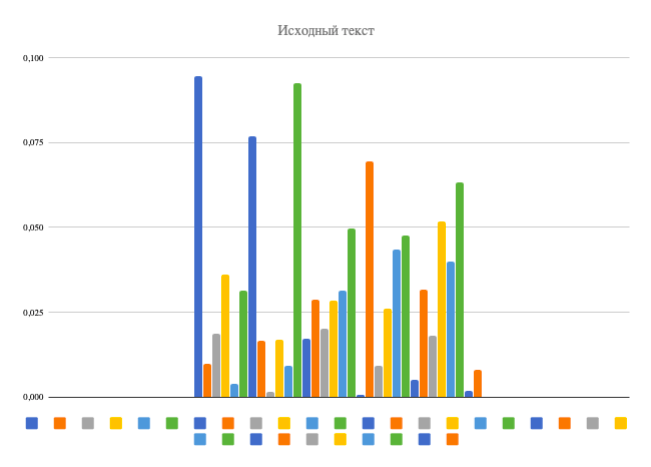


Зашифрованный.



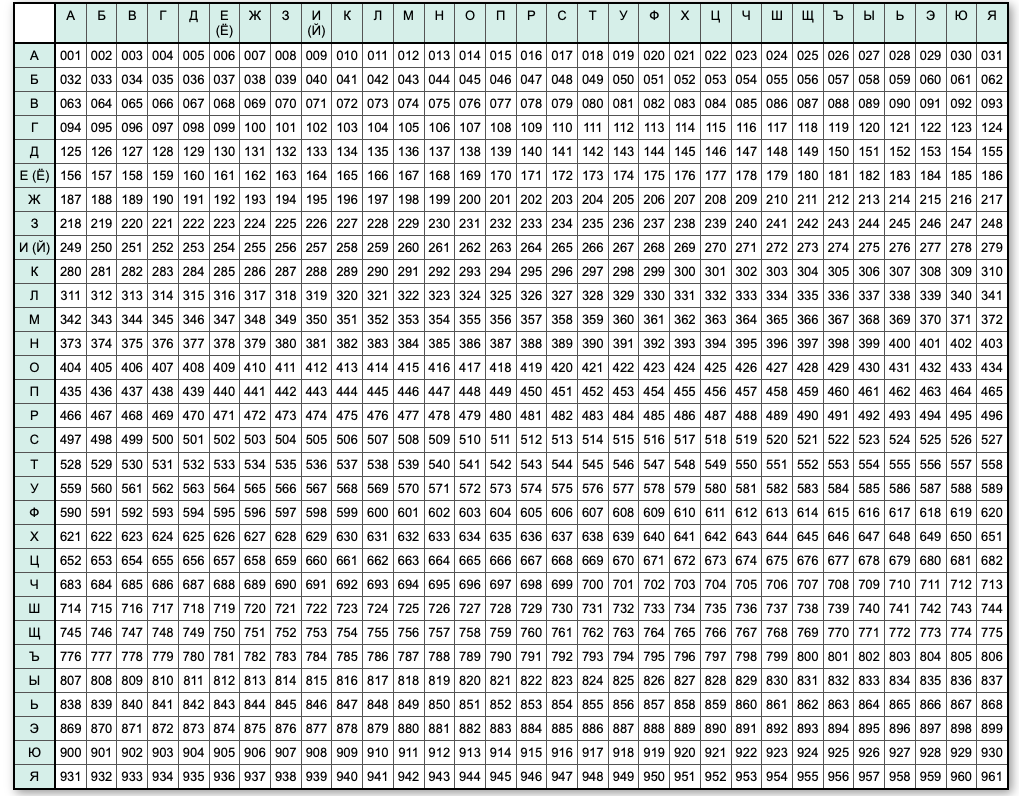
Также в рамках лабораторной работы требовалось построить гистограммы частоты появления символов в исходном тексте

а также в зашифрованном тексте



**ЗАДАНИЕ 2.** Шифр Порты

Шифр Порты, представленный им в виде таблицы, является первым известным биграммным шифром. Размер его таблицы составлял 20 х 20 ячеек; наверху горизонтально и слева вертикально записывался стандартный алфавит (в нем не было букв J, К, U, W, X и Z). В ячейках таблицы могли быть записаны любые числа, буквы или символы - сам Джованни Порта пользовался символами - при условии, что содержимое ни одной из ячеек не повторялось. Применительно к русскому языку таблица шифрозамен может выглядеть следующим образом.

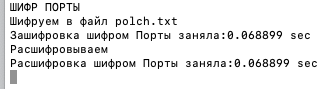


Шифрование выполняется парами букв исходного сообщения. Первая буква пары указывает на строку шифрозамены, вторая - на столбец. В случае нечетного количества букв в исходном сообщении к нему добавляется вспомогательный символ («пустой знак»). Например, исходное сообщение «АБ РА МО В», зашифрованное – «002 466 355 093». В качестве вспомогательного символа использована буква «Я».

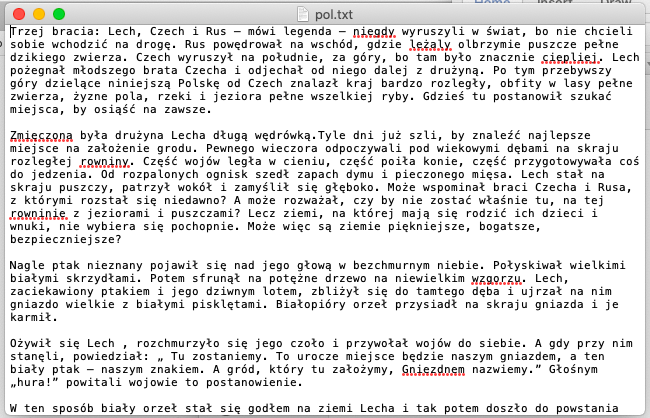
Реализация методов шифрования и расшифровки сообщения представлена ниже.



Результат работы программы.



Исходный текст.



Зашифрованный.

