Учреждение образования

«Белорусский Государственный Технологический Университет»

**Лабораторная работа №1**

**«**Основы теории чисел и их использование в криптографии**»**

Выполнил:

Студент 3 курса 1 группы ФИТ

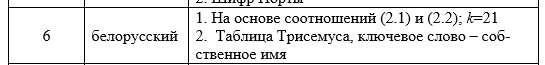
Волчкевич Денис Дмитриевич

Минск 2020

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

**Практическая часть**

1. 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 языка в соответствии с нижеследующей таблицей вариантов задания; при этом следует использовать шифры подстановки из третьего столбца данной таблицы;



• 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).

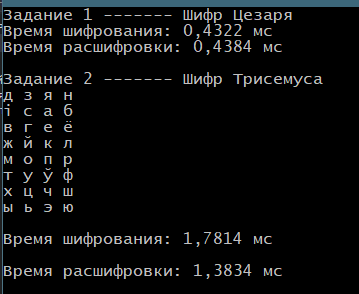
При анализе полученных гистограмм можно сопоставить полученные данные с аналогичными результатами выполнения лабораторной работы №2 из [1].

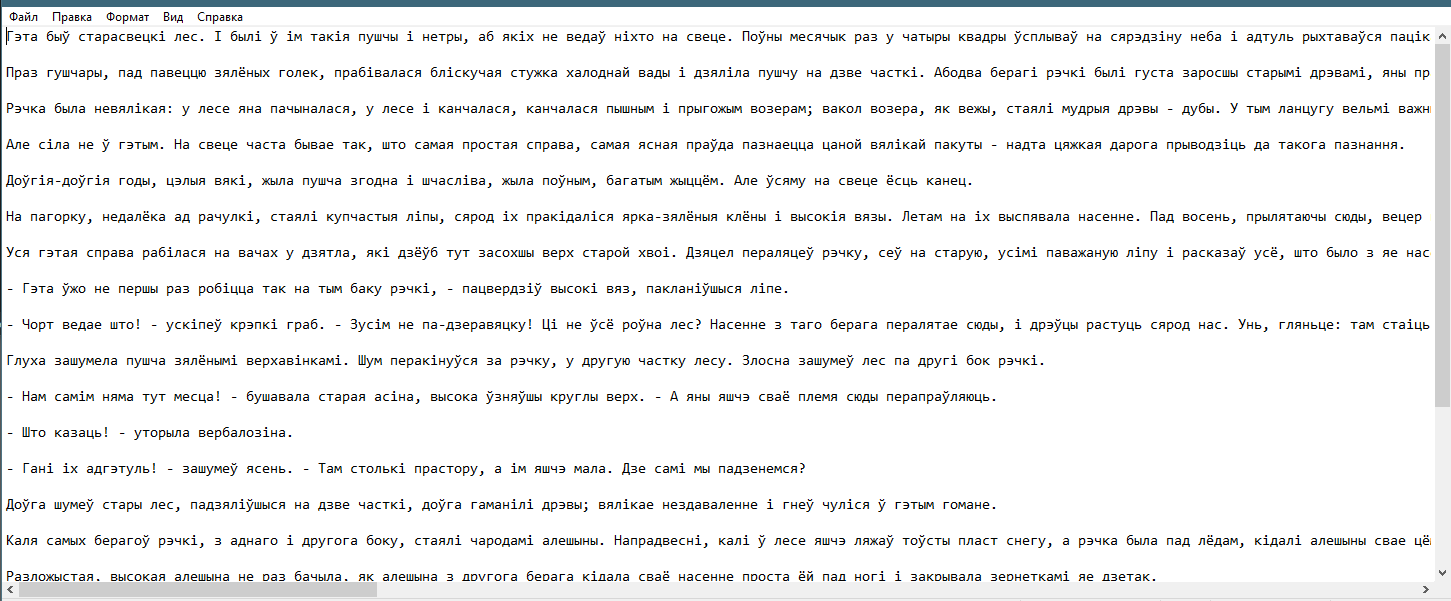
Если указанный в таблице язык исходного текста не известен разработчику программного средства, можно взять документ на требуемом языке и воспользоваться доступным электронным переводчиком (возникающие при этом отдельные семантические неточности не следует считать существенным недостатком выполняемого анализа).

2. Результаты оформить в виде отчета по установленным правилам

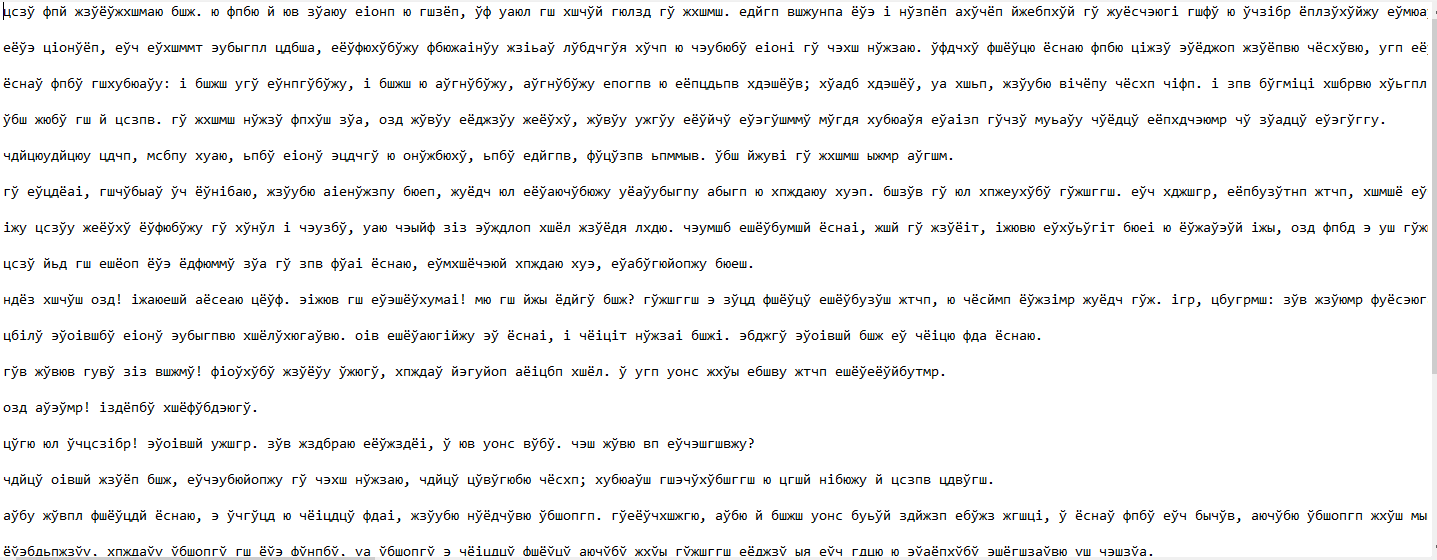
**Вариант 6**

1. Разработать авторское приложение в соответствии с целью лабораторной работы.

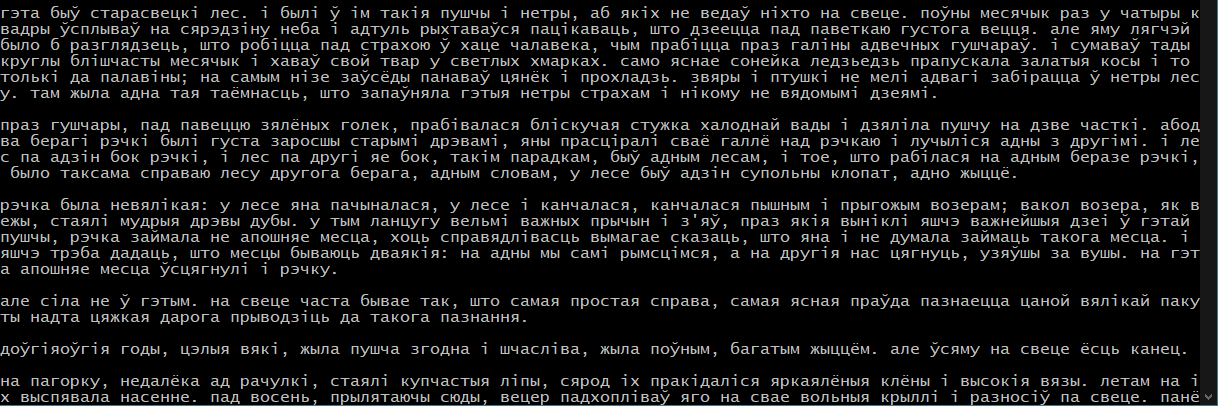


Часть исходного текста размеров 5500 символов.

Часть зашифрованного текста (шифр Цезаря)



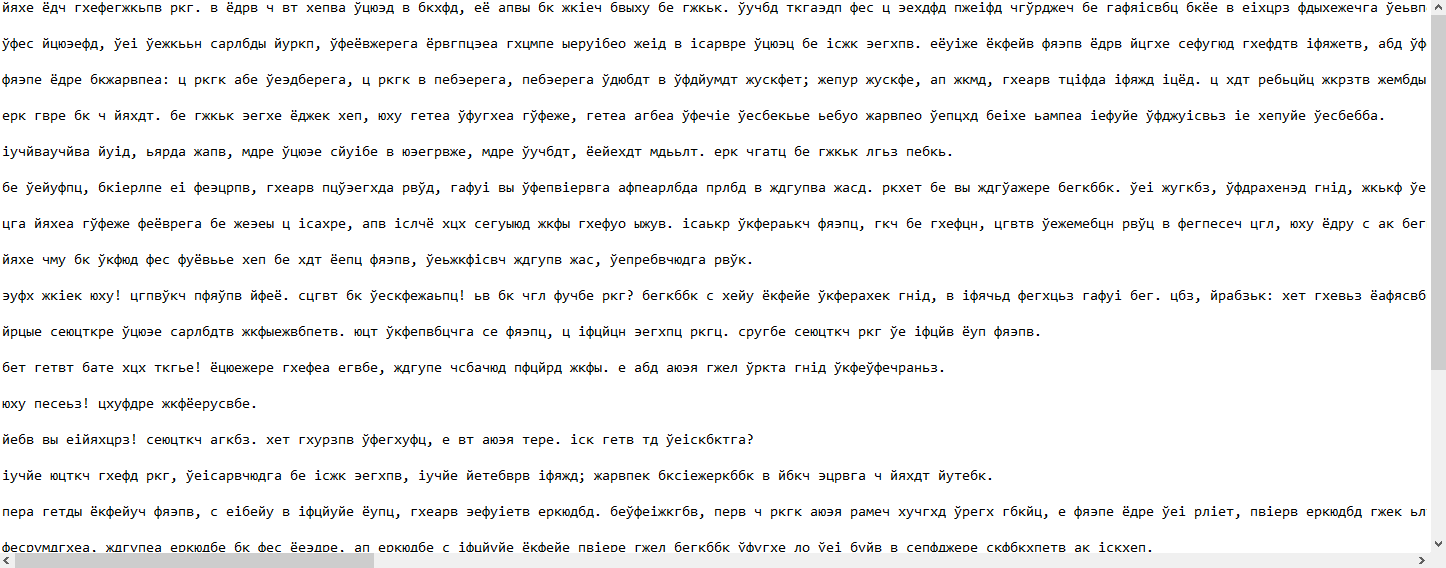
Часть расшифрованного текста (шифр Цезаря)



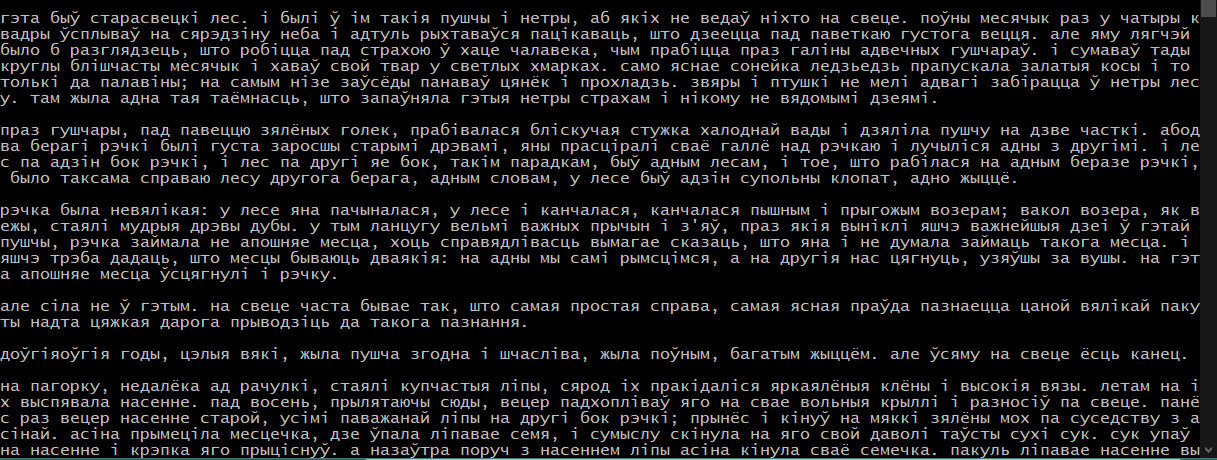
Время необходимое на операции шифрования и расшифровки (шифр Цезаря)



Часть зашифрованного текста (шифр Трисемуса)



Часть расшифрованного текста (шифр Трисемуса)



Время необходимое на операции шифрования и расшифровки (шифр Трисемуса)



**Гистограммы**

