МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образования «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Отчет по лабораторной работе №2**

**ИССЛЕДОВАНИЕ КРИПТОГРАФИЧЕСКИХ**

**ШИФРОВ НА ОСНОВЕ ПОДСТАНОВКИ**

**(ЗАМЕНЫ) СИМВОЛОВ**

Выполнил:

Cтудент 3 курса 1 группы

Парибок И. А.

Вариант 5

Минск 2022

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

**Практическое задание:**

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 (варианты задания представлены Рис. 1);

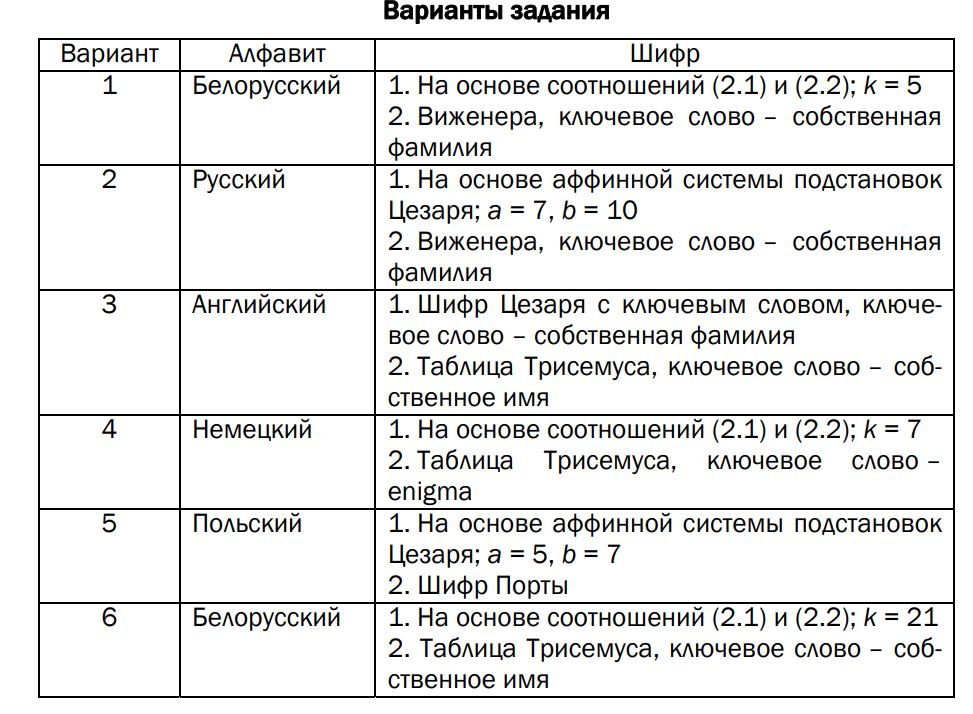


Рисунок 1 – Варианты заданий

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

• оценить время выполнения операций зашифрования/расшифрования;

2. Результаты оформить в виде отчета по установленным правилам.

**Выполнение работы:**

Были реализованы шифры на основе аффинной системы подстановок Цезаря и шифра Порты. На рисунках 2-3 представлены результаты выполнения приложения, а именно - шифрования и дешифрования текста на основе аффинной системы подстановок Цезаря. На рисунке 4 показана скорость выполнения программного кода шифрования и дешифрования. Исходя из полученных данных, можно сделать вывод, что в данной реализации дешифрование полученных данных более затратно по времени, чем шифрование.

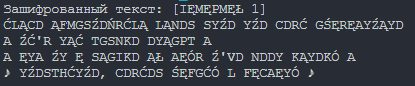


Рисунок 2 – Результат шифрования текста на основе аффинной системы подстановок Цезаря

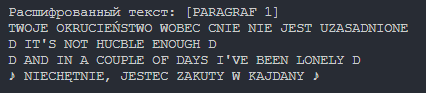


Рисунок 3 – Результат дешифрования текста на основе аффинной системы подстановок Цезаря



Рисунок 4 – Скорость выполнения шифрования и дешифрования текста основе аффинной системы подстановок Цезаря

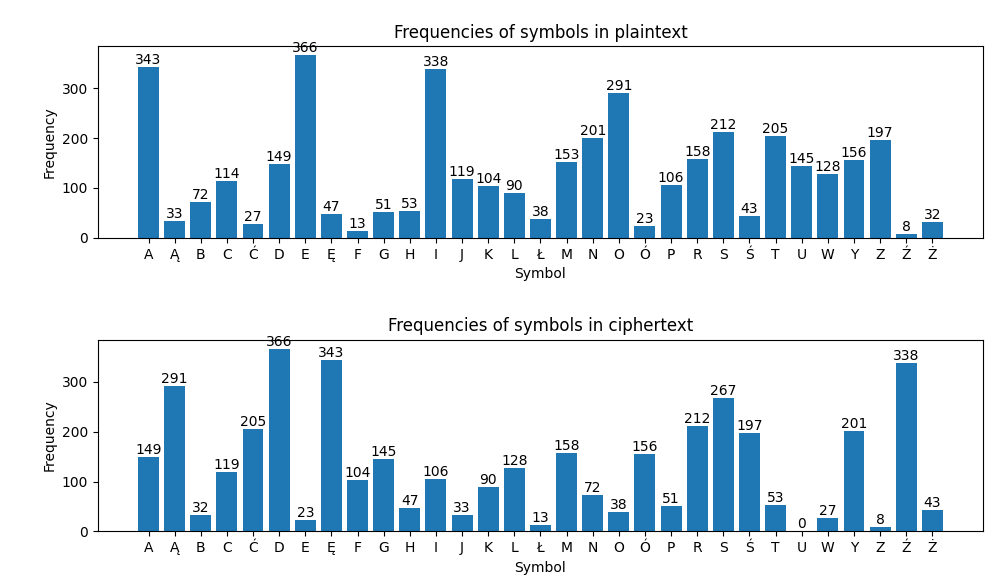


Рисунок 5 – Гистограмма использования символов до и после шифрования на основе аффинной системы подстановок Цезаря

На рисунках 5-6 представлены результаты выполнения приложения, а именно - шифрование и дешифрование с использованием шифра Порты. В качестве ключа использовалось слово "ilua". На рисунке 7 показана скорость выполнения программного кода шифрования и дешифрования. Исходя из полученных данных, можно сделать вывод, что в данной реализации дешифрование полученных данных занимает немного больше времени, чем шифрование.

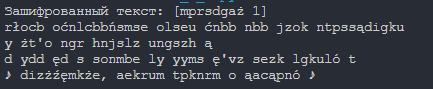


Рисунок 5 – Результат дешифрования текста на основе шифра Порты

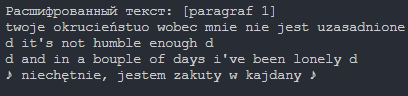


Рисунок 6 – Результат дешифрования текста на основе шифра Порты



Рисунок 7 – Скорость выполнения шифрования и дешифрования текста на основе шифра Порты

**Вывод:** в результате выполненной работы были реализованы два метода шифрования: на основе аффинной системы подстановок Цезаря и шифра Порты. В качестве шифруемых данных использовался файл с более чем 5000 символами. Программная реализация выводит гистограмму появления символов до и после шифрования сообщения. Также были получены данные о скорости работы шифрования.