МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образования «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Отчет по лабораторной работе №4**

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

Выполнил:

студент 3 курса 5 группы

Храмых В. О.

Проверила: Блинова Е. А.

Минск 2020

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

Задачи:

1. Закрепить теоретические знания по алгебраическому описанию, алгоритмам реализации операций зашифрования/расшифрования и оценке криптостойкости подстановочных шифров.

2. Ознакомиться с особенностями реализации и свойствами различных подстановочных шифров на основе готового программного средства (L\_LUX).

3. Разработать приложение для реализации указанных преподавателем методов подстановочного зашифрования/расшифрования.

4. Выполнить исследование криптостойкости шифров на основе статистических данных о частотах появления символов в исходном и зашифрованном сообщениях.

5. Оценить скорость зашифрования/расшифрования реализованных способов шифров.

6. Результаты выполнения лабораторной работы оформить в виде описания разработанного приложения, методики выполнения экспериментов с использованием приложения и результатов эксперимента.

В результате данной лабораторной работы было создано приложение для зашифрования и расшифрования текста по разным методам (Аффинные перестановки Цезаря, Виженера с ключевым словом).

Реализация функции для зашифрования исходного текста по методу аффинных перестановок Цезаря, представлен на рисунке 1.

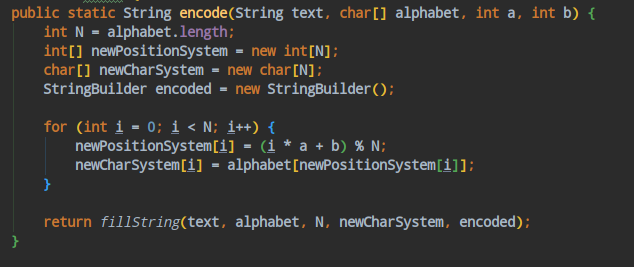


Рисунок 1 –зашифрование по методу аффинных перестановок Цезаря

Результат зашифрования и метод дешифрования представлены на рисунка 2 и 3 соответственно.

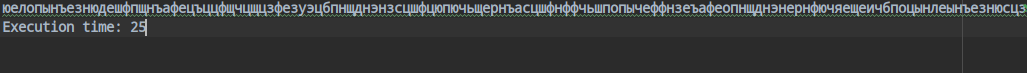


Рисунок 2 – результат зашифрования по методу 1

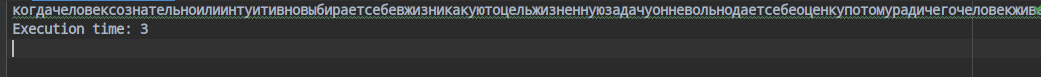


Рисунок 3 – метод дешифрования метода 1

Реализация функции для шифрования текста по методу Виженера (метод 2) с ключевым словом, показан на рисунке 4.



Рисунок 4 – шифрования текста по методу Виженера

Результат выполнения функции для шифрования по методу Виженера с ключевым словом представлен на рисунке 5.

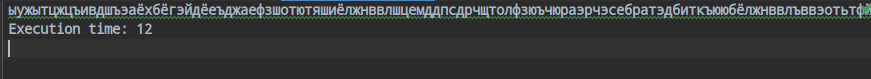


Рисунок 5 – результат шифрования по методу 2

Теперь проведём дешифрование. Метод, используемый для дешифрования представлен на рисунке 6.

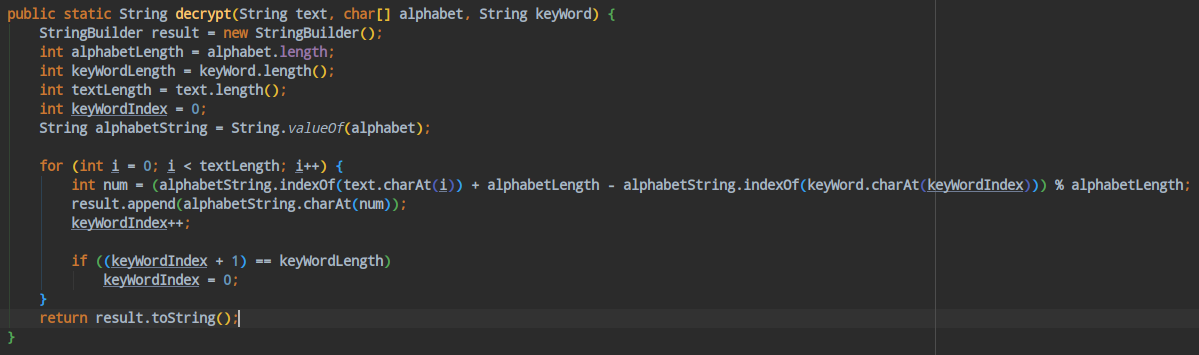


Рисунок 6 –функция дешифрования по методу 2

Результат дешифрования представлен на рисунке 7.

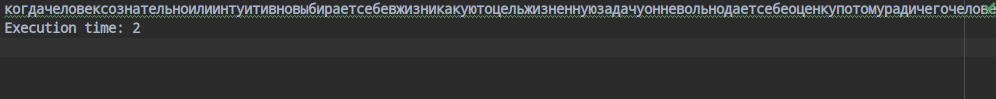


Рисунок 7 –результат дешифрования по методу 2

Execution time во всех файлах .txt – время выполнения того или иного методы де/зашифрвания.

Гистограммы вероятностей приложены в файле gistograms.xlsx текущего директория.

Вывод: в ходе данной лабораторной работы, было разработано приложение для за/дешифрования сообщения по методам аффинных перестановок Цезаря и Виженера с ключевым словом.