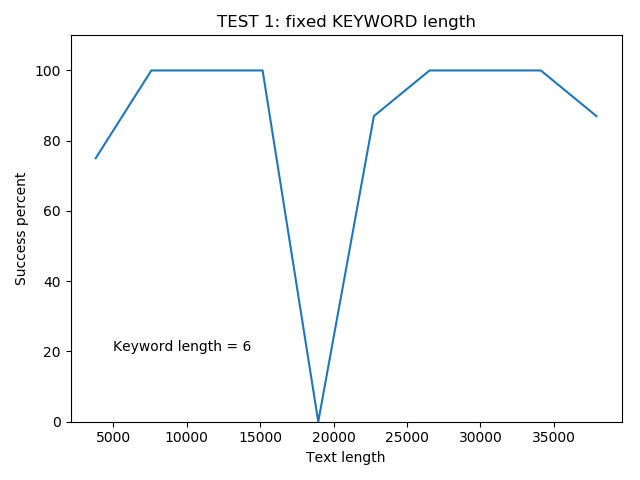
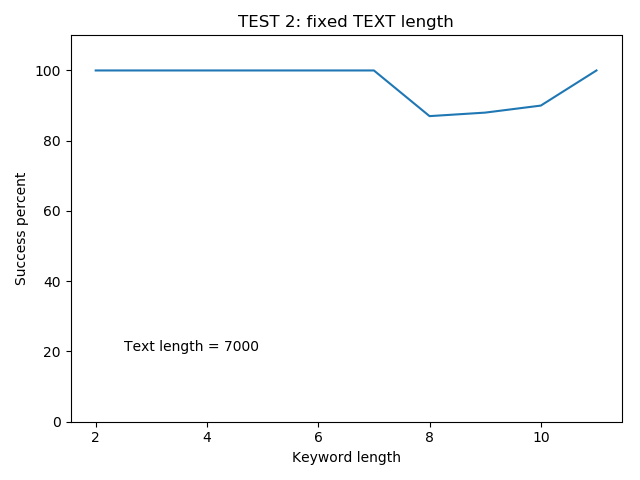
**Отчет по Лабораторной работе №1**

Шавела Вера, 12 группа

При проведении анализа с фиксированными длиной ключа и текста, были получены следующие результаты:



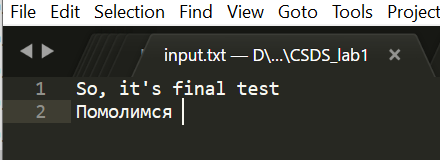


Приведеннные выше графики были получены с помощью библиотеки matplotlib.pyplot языка программирования python. Удобное отображение графиков и простота изучения – причины использования именно этого языка в данной лабораторной. Хотя время обработки все же оставляет желать лучшего, но вы говорили, что это на оценку не провлияет.

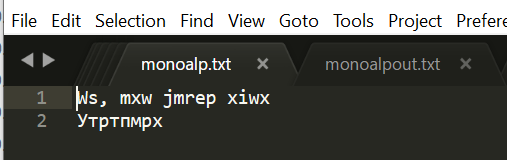
Для исследования был выбран английский язык. Попытка реализовать оба языка и на языке программирования С++ оказалась не совсем успешной и слишком трудоемкой. Плюс из-за совпадения кода буквы “я” русского алфавита и командного кода переноса строки, эта буква в моей программе не обрабатывалась:

Первое задание с моноалфавитным шрифтом и шифром Цезаря, тем не менее детальнее было сделано на языке С++:

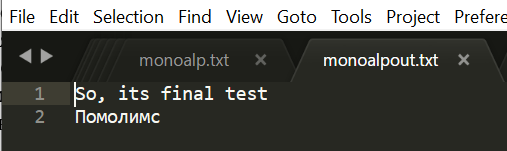
Входные данные:



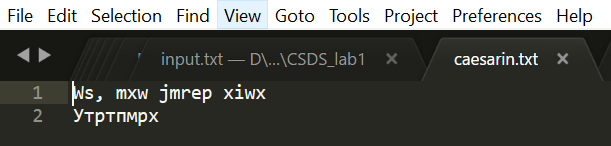
Результат шифрования моно-алфавитным шрифтом:



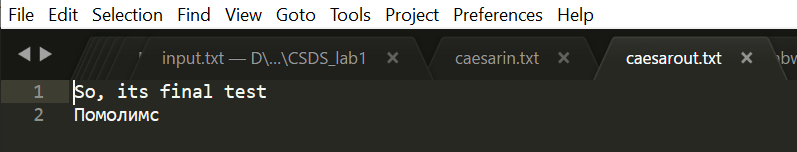
Результат дешифровки моно-алфавитного шрифта:



Результат шифрования шифром Цезаря:

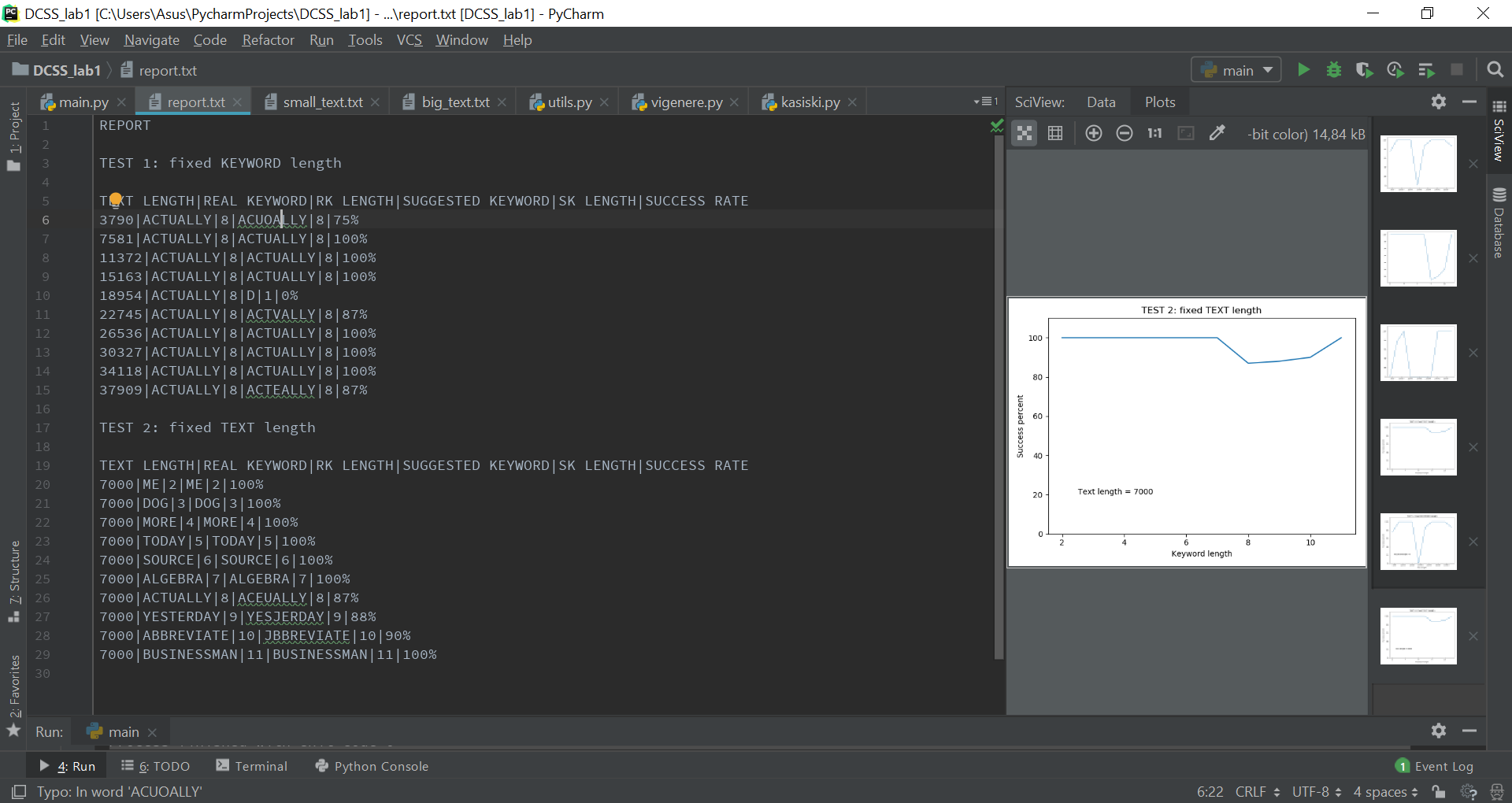


Результат дешифровки шифра Цезаря:

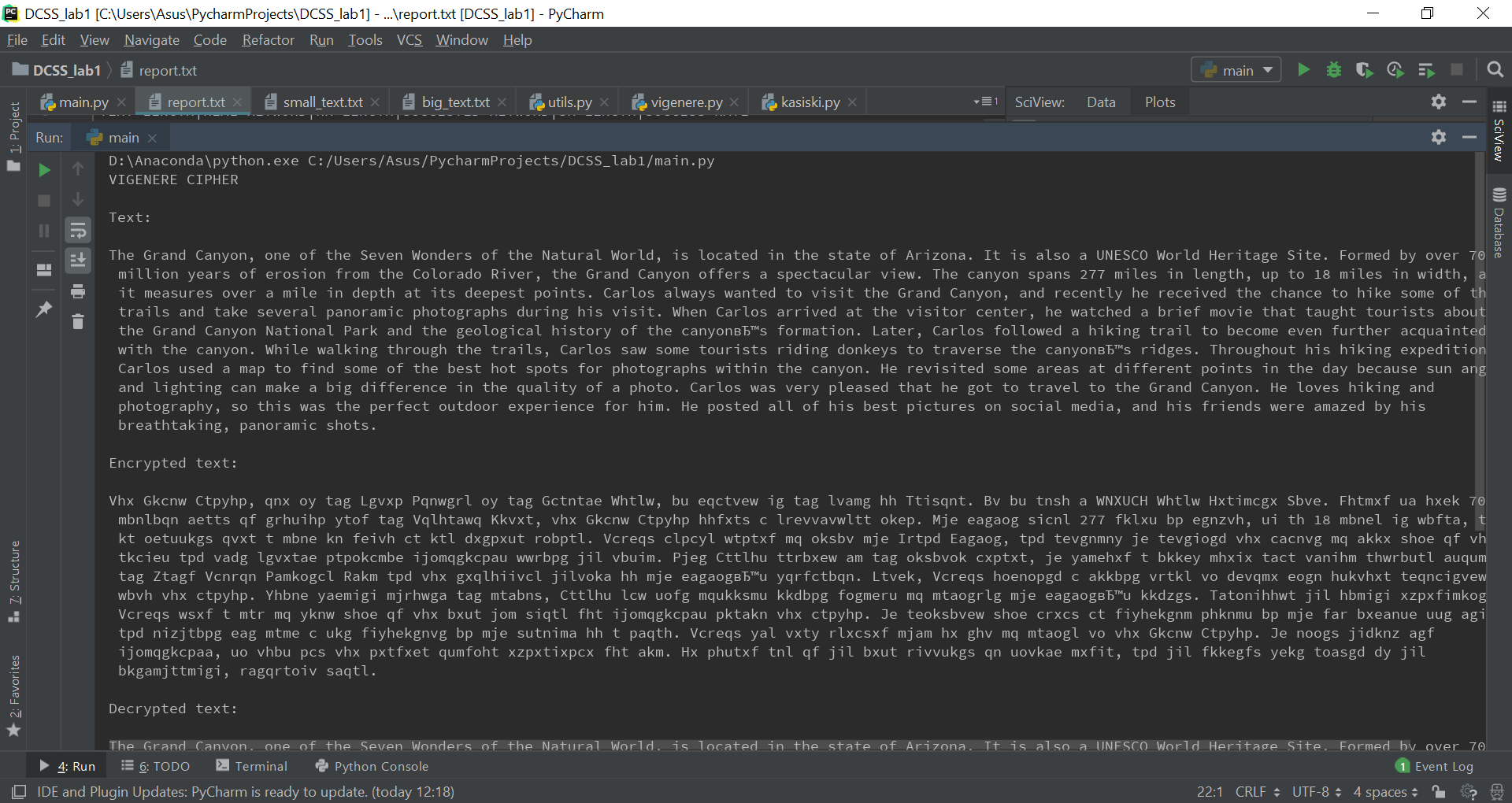


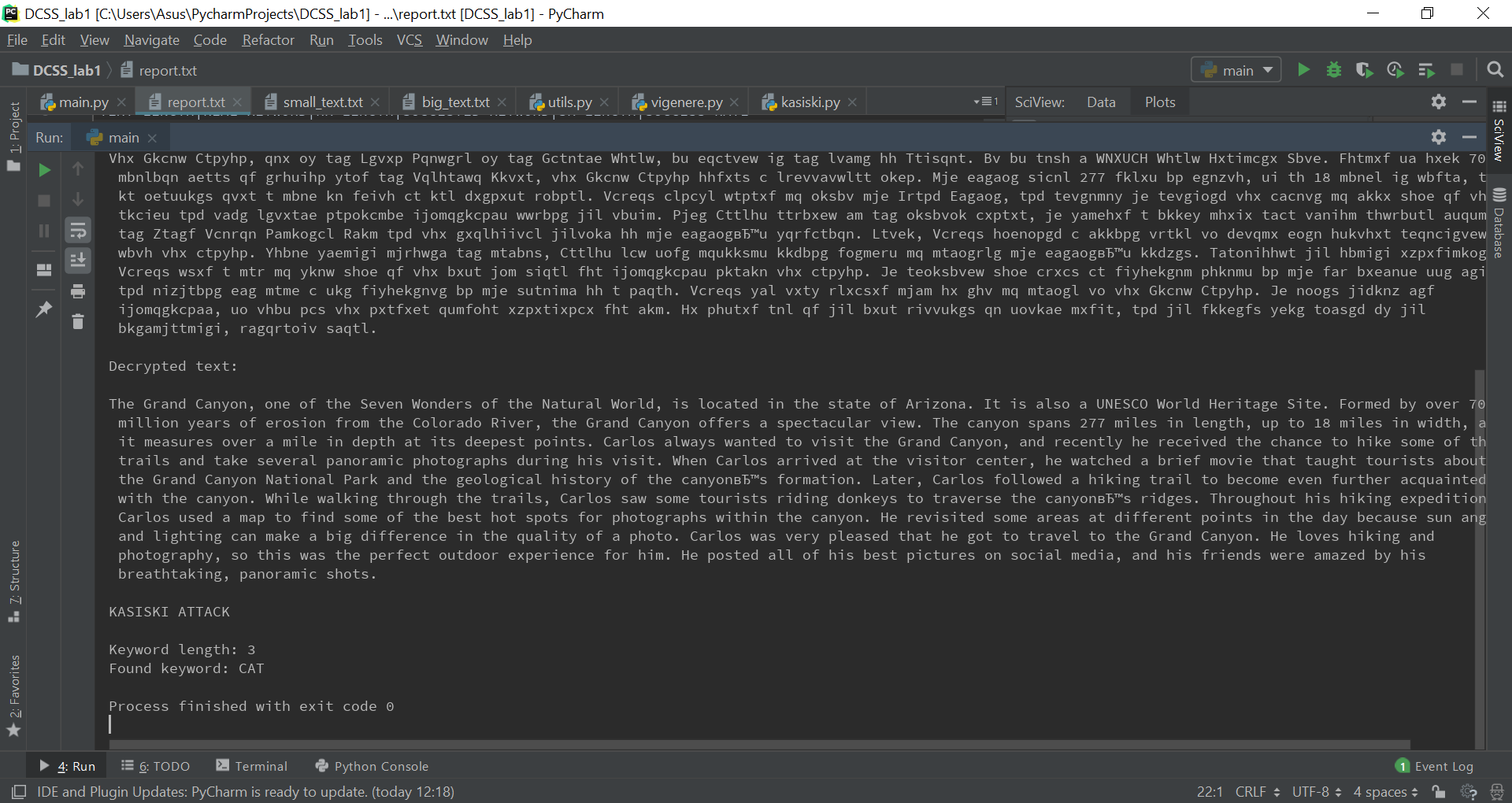
Исходные коды программ, как на С++, так и на Python, будут отправлены отдельными файлами. В программе на С++ сдвиг запрашивается с консоли непосредственно во время выполнения.

Программа на Python сложнее по своей структуре, т.к. состоит из модулей, но для анализа использует данные только из файлов данных или исходного кода. Она создает единый отчет с результатами проведения атак Касиски и частотного анализа. Для удобства, данные предоставляются в формате таблиц:



Работа шифрования и атаки простого примера с небольшим текстом и ключом длины 3 выводится на консоль пользователю:





**Вывод:** Результат анализа успеха проведения атаки в зависимости от длины ключа или текста для меня не совсем понятен, т.к. по какой причине происходит провал в тексте размером около 20000 символов, мне непонятно. Возможно, есть какие-то недочеты в реализации, которые я неточно или неправильно реализовала, потому что по логике вещей: чем больше текст – тем проще провести атаку Касиски, т.к. больше шансов встретить повторяющиеся блоки. И также мне непонятен провал после середины с длинами ключей (хоть и не такой колоссальный, как при изменении длины текста). Мое единственное предположение – кратность количества символов текста длине ключа, возможно я недостаточно хорошо реализовала обработку ситуации, когда это условие не выполняется.