**Отчет по лабораторная работе 1**

В ходе выполнения лабораторной работы был реализован алгоритм шифрования и расшифрования виженера который не составил трудностей. А вот с методом Касиски сложнее. Хотя алгоритм кристально чистый и не должен был составить трудностей. В алгоритме не указанно как бороться с погрешностями и ошибками в виду чего уже на процессе выяснения длины ключа. Метод выдавал неверные результаты что делает работу по поиску самого ключа бесполезной.

Я не смог найти методов как бороться с погрешностями поэтому была сделана оптимизация в виде ограничения длины ключа от 4 до 50 знаков и введен коэффициент погрешности в 2 % что позволила хоть иногда получать верную длину ключа. Но стоит взять во внимание что метод очень плохо работает если в ключе содержатся повторяющиеся части (например и “пафпаф”) также если части слабо различаются например (“тиктак”) для данных ключей длина будет рафна длине повторяющейся части.

С частотным анализом дела обстоят лучше так так если длина ключа подобрана верно то слово даже если не находит полностью то по символам человек может восстановить ключ.

Стоит заметить что если внести человеческий фактор то метод взлома рабоатет куда лучше. Так я выводил на выбор топ из 5 длин ключей и далее проводил частотный анализ на тих длиннах что практически всегда позволяла добиться результата.

Также я считаю что можно улучшить результаты если сравнивать ключ со словарем в таком случае можно полностью автоматизировать процесс но это сработает только в том случае если ключ осмысленный и не содержит повторяющихся частей.

Тесты на выборках показали что чем больше текст и меньше ключевое слово тем вероятность правильно определить размер ключа а впоследствие и ключ больше.