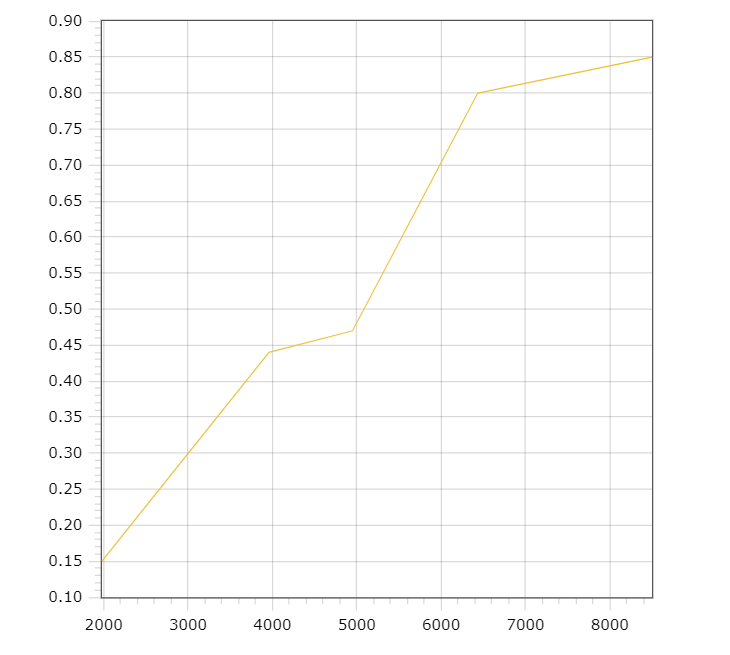
При выполнении лаб работы были выполнены следующие задачи:

1. реализовано шифрование и дешифрование текста на английском языке по методу Виженера на языке scala.
2. Произведен анализ зашифрованного текста по методу Касиски.
3. Проведены исследования зависимости вероятности успешной атаки от длины использованного при шифровании ключевого слова и от длины шифротекста.

Для метода Касиски была использована частота чаще всего встречающегося элемента алфавита(‘e’ в английском языке), также для анализа использовались только 3-граммы.

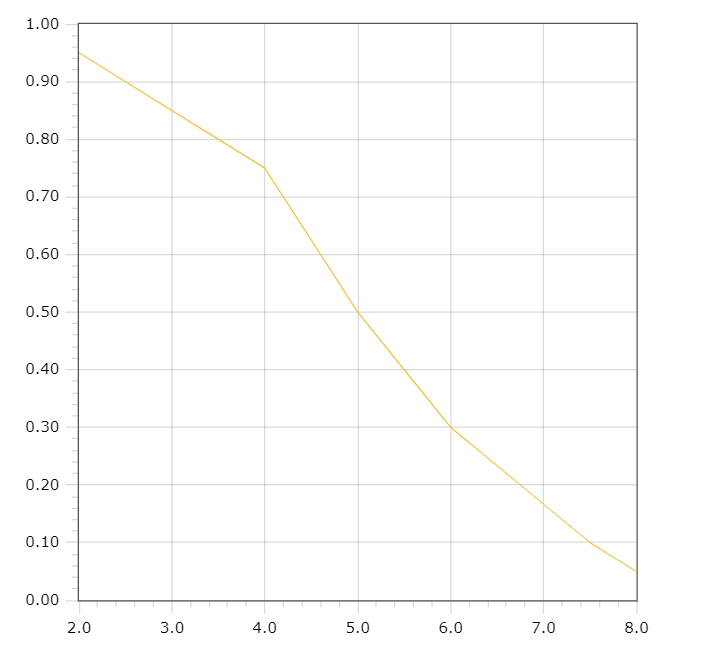
В результате экспериментов были построены графики зависимости вероятности взлома от длины ключа и шифртекста:

(Y – вероятность успешного взлома, X – количество символов в тексте)



Для анализа завивимости успешности взлома от длины ключа использовался текст с количеством символов около 7000

(Y – вероятность успешного анализа, X – длина ключа)



Исходя из графиков, напрашивается вывод, что чем длина ключа больше, тем меньше вероятность взлома, так же чем длина текста больше, тем больше вероятность взлома, за редкими исключениями.