Лабораторная работа №1
КРИПТОАНАЛИЗ МЕТОДОВ ПРОСТОЙ ПОДСТАНОВКИ

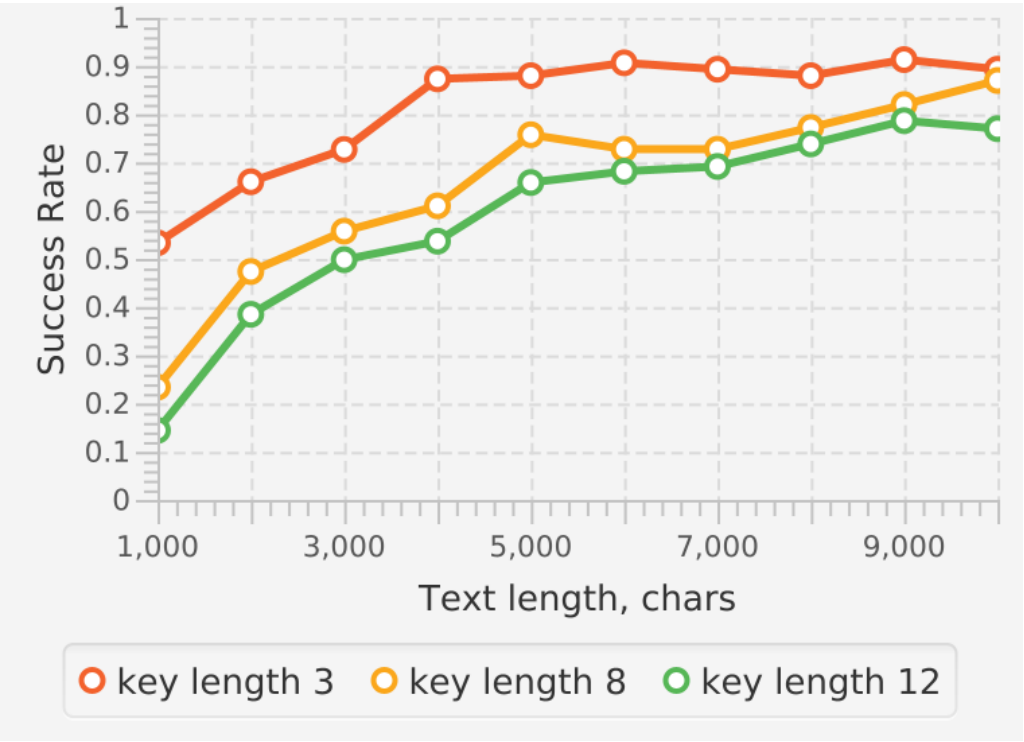
Выполнил Кордияко Ян, 1 группа, 4 курс

Задания:

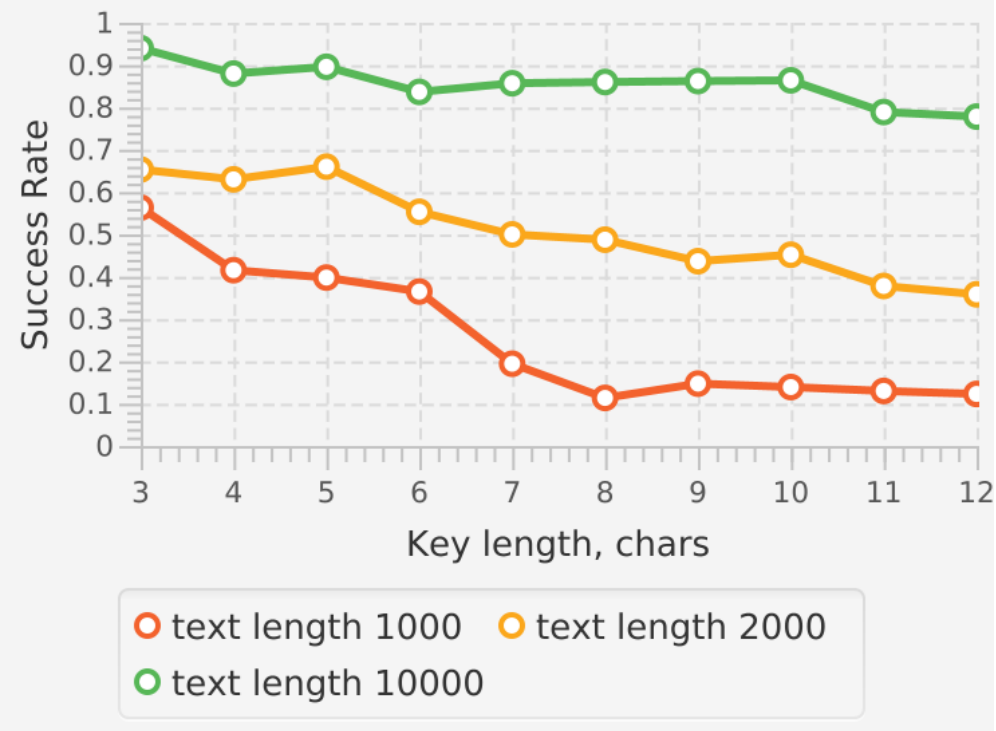
1. Реализовать программное средство, осуществляющее шифрование и дешифрование текстового файла, содержащего текст на заданном языке.
2. Реализовать программное средство, осуществляющее криптоанализ зашифрованного по методу Виженера текста. Для криптоанализа использовать тест Касиски.
3. Провести экспериментальное исследование вероятности успешного проведения атаки по методу Касиски от длины шифротекста.
4. Провести экспериментальное исследование вероятности успешного проведения атаки по методу Касиски от длины использованного при шифровании ключевого слова.

Экспериментальные результаты:

Зависимость успешного проведения атаки от длины шифротекста:



Зависимость успешного проведения атаки от длины использованного при шифровании ключевого слова:



Вывод:

Результаты экспериментов показали, что вероятность успешного проведения атаки зашифрованного по методу Виженера текста возрастает вместе с длиной зашифрованного текста, но снижается вместе с длиной использованного при шифровании ключевого слова.