Лабораторная работа №1

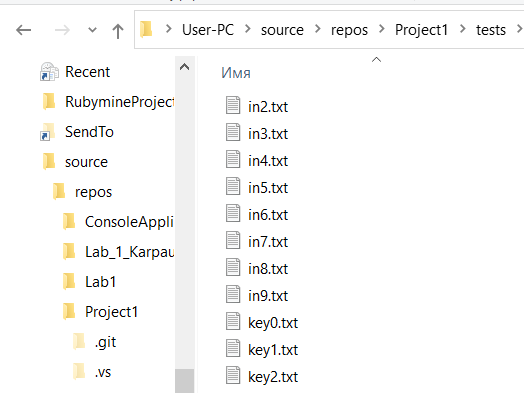
Карпов Алексей

12 группа кафедра ИСУ

В результате проведения лабораторной работы были достигнуты следующие результаты:

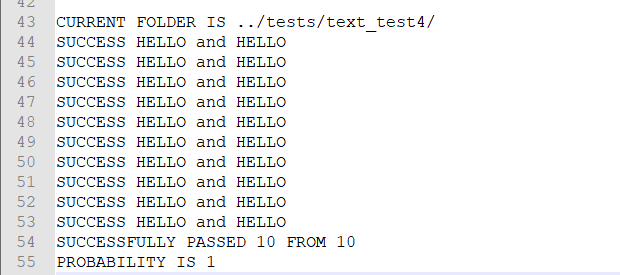
1. Написана программное средство, которое осуществляет по методу Виженера шифрование и дешифрование текстового файла на английском языке
2. Написано программное средство, которое проводит анализ зашифрованного текста с помощью теста Касиски.
3. Проведены исследования зависимости вероятности успешной атаки от длины использованного при шифровании ключевого слова и от длины шифротекста.

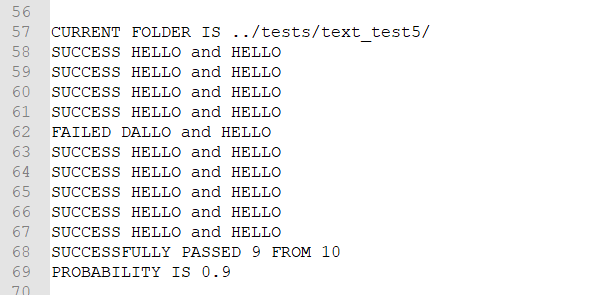
В процессе работы мною были подобраны ряд текстов, на которых проводилось тестирование моей программы.

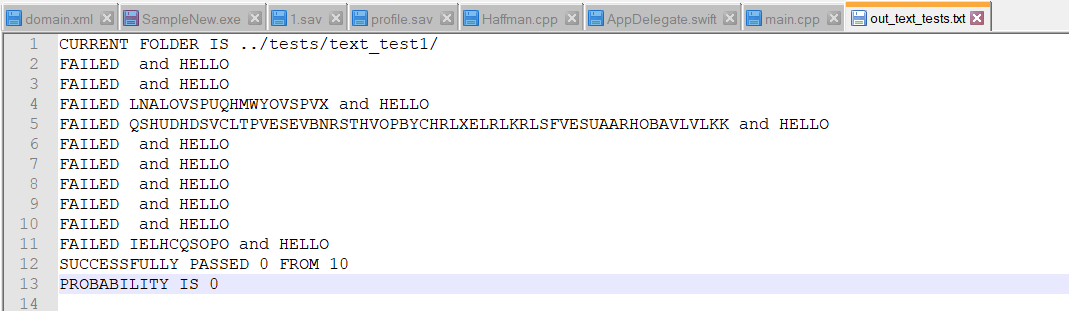


Они представлены в папке tests, они разбиты в зависимости от длины текста и от длины ключа.

Для взлома использовалась частотность букв английского языка

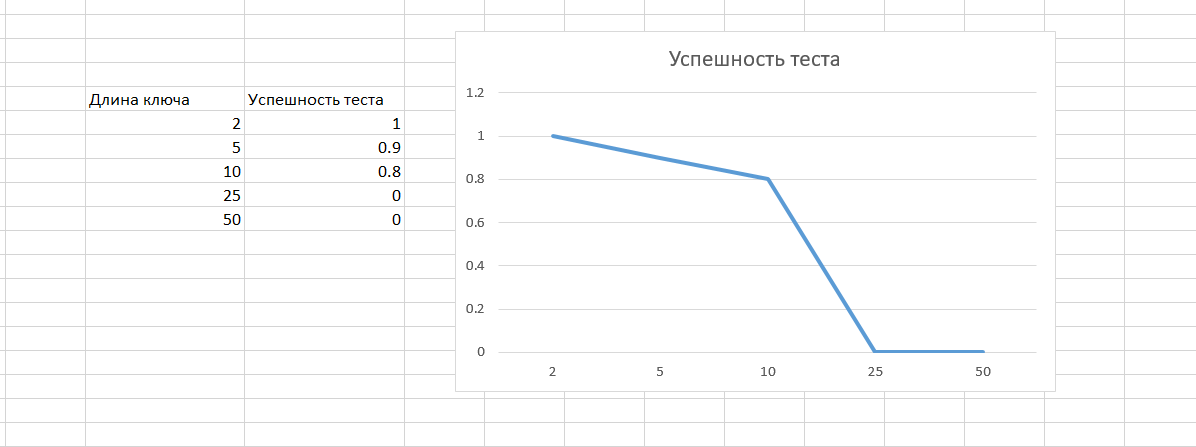
В результате экспериментов мы получили логичные результаты, которые полностью зависят от длины текста и длины ключа.





Можно делать следующие выводы:

1. Чем длина ключа больше, тем меньше вероятность взлома
2. Чем длина текста больше, тем больше вероятность взлома



Однако при увеличении длины текста можно наблюдать обратный результат:

