Отчёт по 1 лабораторной работе

Дворяков Максим

4 курс 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.

Результаты исследования приведены ниже.

В результате мы получили что при фиксированном размере ключа 8, чем меньше размер текста, тем меньше шанс на успешное нахождения ключа.

test 1: with fixed keyword length

text len|keyword|len|found keyword|len|success probability

583|ABSTRACT|8|ABWCAAAE|8|37%

729|ABSTRACT|8|ABXCVAHA|8|50%

1458|ABSTRACT|8|ABSTCACC|1|75%

2916|ABSTRACT|8|ABAARACT|1|75%

5103|ABSTRACT|8|ABSYRACT|8|75%

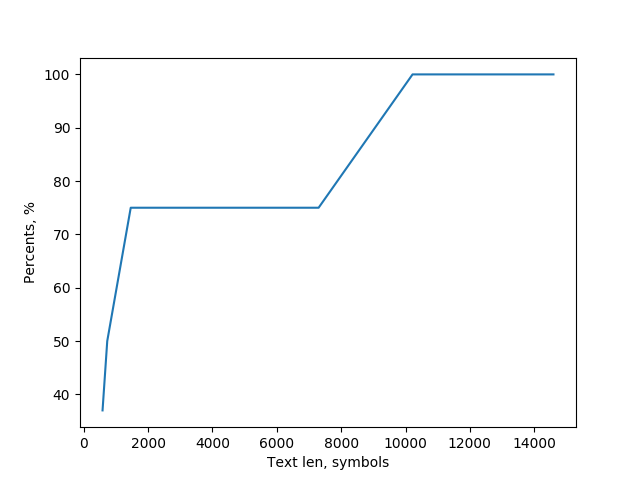
7290|ABSTRACT|8|ABGTDACT|8|75%

10206|ABSTRACT|8|ABSTRACT|8|100%

11664|ABSTRACT|8|ABGTRACT|8|100%

13122|ABSTRACT|8|ABSTRACT|8|100%

14581|ABSTRACT|8|ABSTRACT|8|100%



В результате этого теста видно, что чем больше ключ, тем шансов на успех становиться меньше. Я провёл ещё несколько прогонов и результаты были похожи.

test 2: with fixed text length

text len|keyword|len|found keyword|len|success probability

6000|AS|2|AS|2|100%

6000|KEY|3|KEY|3|100%

6000|SORT|4|SORT|4|100%

6000|FORCE|5|FORCE|5|100%

6000|SECRET|6|GECRET|6|100%

6000|COLORED|7|COLORED|7|85%

6000|ABSTRACT|8|ABSTRACT|8|75%

6000|YESTERDAY|9|F|1|100%

6000|FLYCATCHER|10|FLYCATCHER|10|90%

6000|OPPOSITIONS|11|I|1|63%

