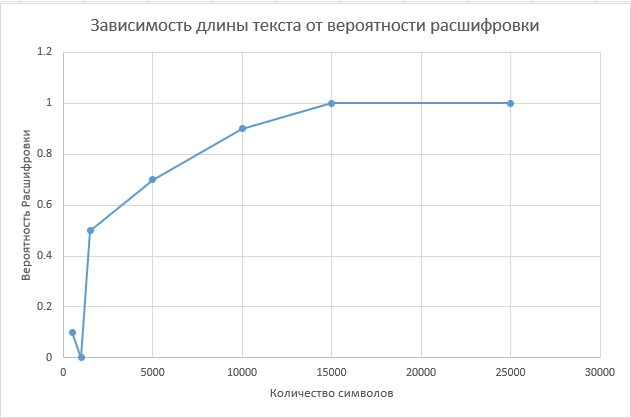
Доскоч Роман 4 курс 13 группа Лабораторная работа №1

Условие

* Реализовать программное средство, осуществляющее криптоанализ зашифрованного по методу Виженера текста. Для криптоанализа использовать тест Касиски.
* Провести экспериментальное исследование зависимости вероятности успешного проведения атаки по методу Касиски от длины шифротекста. Построить графики.
* Провести экспериментальное исследование зависимости вероятности успешного проведения атаки по методу Касиски от длины используемого при шифровании ключевого слова. Построить графики.

Результаты



Вывод:

По первому графику видно, что вероятность успешной расшифровки напрямую зависит от длинны текст: чем больше текст, тем выше вероятность расшифровать текст правильно.

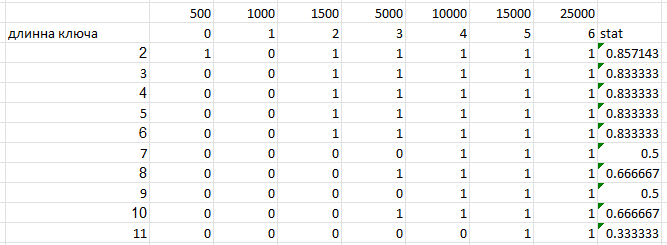
Это можно объяснить тем, что у больших текстов процентное соотношение частот встречаемости букв наиболее похож на всеобщих набор частот, который, к примеру показывает, что самая частая буква в английском алфавите является буква ‘e’ и это означает что при попытке расшифровки частотным анализом скорее всего самая частая буква в шифротексте и будет являться буквой ‘e’ и останется только сместить позицию обратно по формуле что бы получить изначальный символ

(буква шифра - самая встречаемая + 'E') mod 26

Из второго графика можно сделать вывод что при росте длины ключа растет и сложность расшифровки такого текста, обратнопропорционально.

Я проводил тесты на следующих длинах текстов

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 500 | 1000 | 1500 | 5000 | 10000 | 15000 | 25000 |



Такую зависимость можно обусловить тем, что при коротких ключах текст делиться на бо́льшие части из этого следует, как и говорилось ранее, частотный анализ провести легче. Но если мы возьмем достаточно большой текст то и достаточно большой текст может компенсировать его длину, главное что бы длина части (длинна текста / длинна ключа) была достаточно большой для проведения частотного анализа.