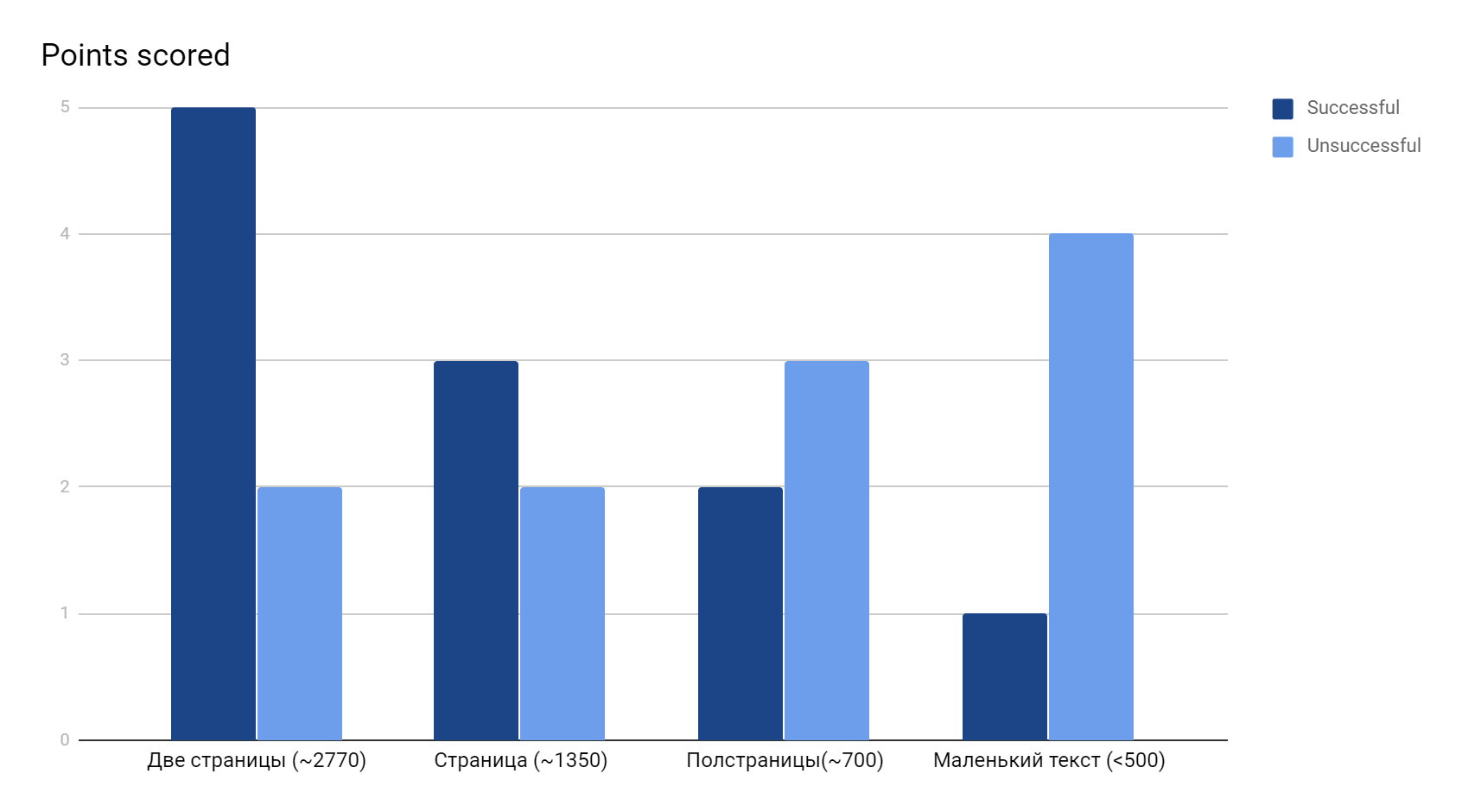
**Генерировал “Lorem Ipsum” текста.**

**Провести экспериментальное исследование зависимости вероятности успешного проведения атаки по методу Касиски от длины шифротекста.**

В данном эксперименте, фиксировал длину ключа - 3 и l=3.



**Провести экспериментальное исследование зависимости вероятности успешного проведения атаки по методу Касиски от длины используемого при шифровании ключевого слова.**

Размер исходного текста - 2500 слов.

При размере ключевого слова 3, ломает отлично, в связи с, по сути, разбиением исходного текста на три. По причине того, что “подтексты” достаточно большие, посредством частотной атаки, удается угадать смещение весьма успешно.

Увеличив размер ключевого слова до 5, успешные атаки стали проводиться реже, но не намного, в то же время, иногда, это удавалось исправить, изменением **l** (l-граммы).

Эксперимент дошел до выбора в качестве ключа: “**INFRACTRUCTURE**”. Касиска нашел размер ключа только при l >= 6. Однако на таком размере “подтекста” (2500 / 14), частотная атака теряет в эффективности.