Lab 2 report

Расшивровка ширфротекста в данной лабораторной работе базировалась на идее, что если в ходе шифрования не использовать соль или нонс и использовать один и тот же ключ больше чем 1 раз - то уязвимость алгоритма состоит в следующем (опишу формулами)

X1 (+) key = cipherText1

X2 (+) key = cipherText2

cipherText1 (+) cipherText2 = X1 (+) X2

далее, зная, что у нас два проксоренных логических текста, мы можем попробовать подобрать слово, которое скорее всего будет в сообщении и пробовать проксорить строки с этим словом. В итоге, если слово таки присутствует в тексте, то сделав ксор с X1 (+) X2 мы получим часть логичного текста, который сообтветсвует позиции слова, которое мы продобрали. В после долгих попытокб перебирания самых и не самых популярных слов и выбора зазных строк в https://toolbox.lotusfa.com/crib_drag/ я смогла получить две строки, вбив которые в гугл можно получить произведение If Редьярда Киплинга