Лабораторная работа №7

Элементы криптографии. Однократное гаммирование

Кекишева Анастасия Дмитриевна

Содержание

# 1 Цель работы

Освоить на практике применение режима однократного гаммирования.

# 2 Задание

Нужно подобрать ключ, чтобы получить сообщение «С Новым Годом, друзья!». Требуется разработать приложение, позволяющее шифровать и дешифровать данные в режиме однократного гаммирования. Приложение должно: 1. Определить вид шифротекста при известном ключе и известном открытом тексте. 2. Определить ключ, с помощью которого шифротекст может быть преобразован в некоторый фрагмент текста, представляющий собой один из возможных вариантов прочтения открытого текста.

# 3 Теоретическое введение

Гаммирование, или Шифр XOR, — метод симметричного шифрования, заключающийся в «наложении» последовательности, состоящей из случайных чисел, на открытый текст. Последовательность случайных чисел называется гамма-последовательностью и используется для зашифровывания и расшифровывания данных. Суммирование обычно выполняется в каком-либо конечном поле [1].

В соответствии с теорией криптоанализа, если в методе шифрования используется однократная вероятностная гамма (однократное гаммирование)той же длины, что и подлежащий сокрытию текст, то текст нельзя раскрыть. Даже при раскрытии части последовательности гаммы нельзя получить информацию о всём скрываемом тексте.

Наложение гаммы по сути представляет собой выполнение операции сложения по модулю 2 (XOR) (обозначаемая знаком ) между элементами гаммы и элементами подлежащего сокрытию текста. Такой метод шифрования является симметричным, так как двойное прибавление одной и той же величины по модулю 2 восстанавливает исходное значение, а шифрование и расшифрование выполняется одной и той же программой.

Если известны ключ и открытый текст, то задача нахождения шифротекста заключается в применении к каждому символу открытого текста следующего правила: > Ci = Pi Ki,

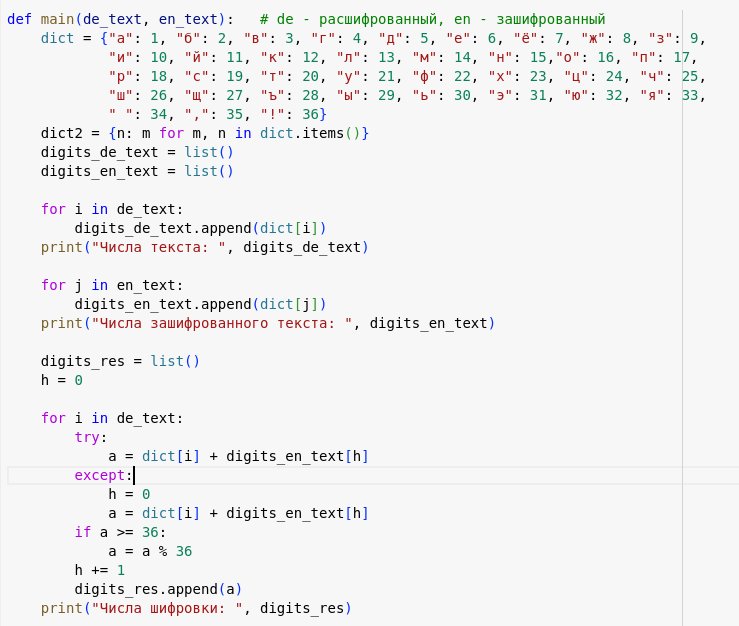
где Ci — i-й символ получившегося зашифрованного послания, Pi — i-й cимвол открытого текста, Ki — i-й символ ключа, i = 1, m. Размерности открытого текста и ключа должны совпадать, и полученный шифротекст будет такой же длины.

Если известны шифротекст и открытый текст, то задача нахождения ключа решается через формулу, а именно, обе части равенства необходимо сложить по модулю 2 с Pi: > Ci Pi = Pi Ki Pi = Ki, > Ki = Ci Pi.

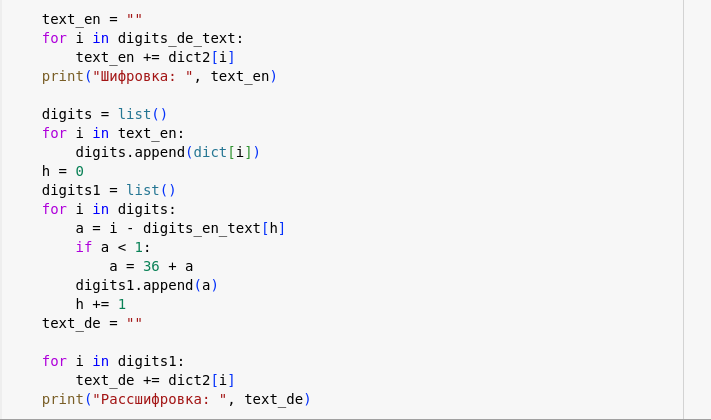
Открытый текст имеет символьный вид, а ключ — шестнадцатеричное представление. Ключ также можно представить в символьном виде, воспользовавшись таблицей ASCII-кодов [2].

# 4 Выполнение лабораторной работы

1. Написала код (рис. ??, ??), который определяет вид шифротекста при известном ключе и известном открытом тексте, а также определяет ключ.

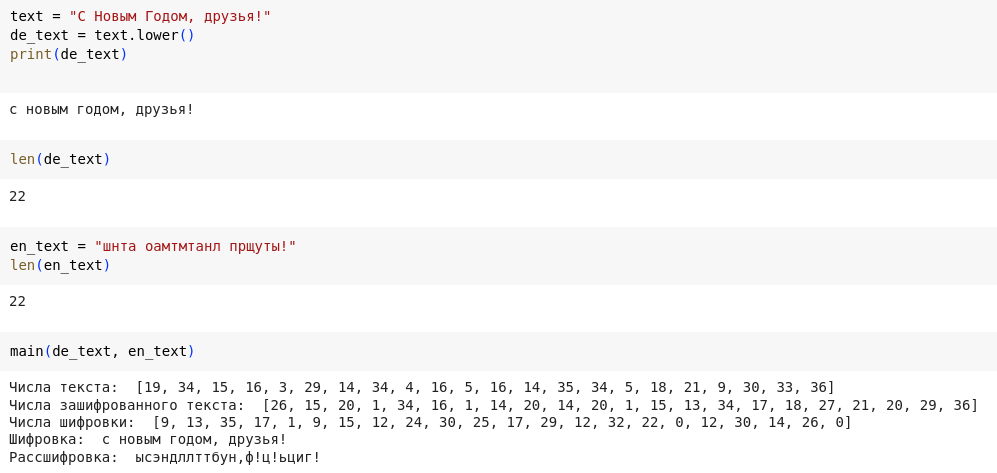


Первая часть алгоритма



Вторая часть алгоритма

Мой код преобразет текст, написанный в нижнем регистре, поэтому первоначальную фразу я сделала таковой, командой lower(). Далее проверила, чтобы текст для шифровки также состоял из такого же количества символов и запустила программу. Результат: ысэндллттбун,ф!ц!ьциг!



Результат

# 5 Выводы

Освоила на практике применение режима однократного гаммирования, написав программу, которая определяет вид шифротекста при известном ключе и известном открытом тексте и определяет ключ.

# Список литературы

1. Однократное гаммирование [Электронный ресурс]. URL: <https://studfile.net/preview/272674/page:7/>.

2. Лабораторная работа No 7. Элементы криптографии. Однократное гаммирование [Электронный ресурс]. URL: <https://esystem.rudn.ru/pluginfile.php/2090421/mod_resource/content/2/007-lab_crypto-gamma.pdf>.