Лабораторная работа №7

Элементы криптографии. Однократное гаммирование

Дугаева Светлана Анатольевна

Содержание

[Цель работы 1](#_Toc89993092)

[Выполнение лабораторной работы 1](#_Toc89993093)

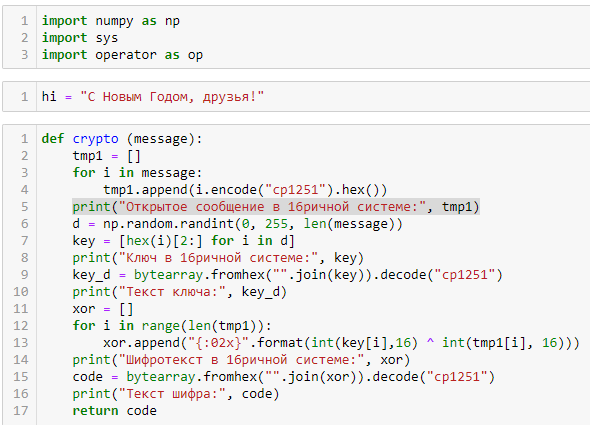
[Выводы 3](#_Toc89993094)

# Цель работы

Освоить на практике применение режима однократного гаммирования.

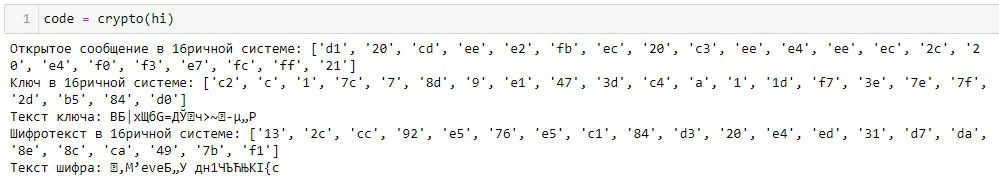
# Выполнение лабораторной работы

1. Сначала подключим нужные библеотеки. Затем в переменную hi запишем наше сообщение, которое требуется зашифровать. Наиболее удобным вариантом будет написать функцию (crypto), которая принимет на вход открытое сообщение(словами). После этого переведем сообщение в 16ричную систему исчисления(для этого используется библеотека sys). Создадим случайный ключ(выбор случайного значения от 0 до 255, и затем переведем ключ в 16ричную систему счисления. В дополнение я перевела ключ в символьный вид. Наложим гамму, то есть выполним операцию сложения по модулю 2(XOR) между элементами полученного случайного ключа и элементами подлежащего сокрытию текста Для получания шифротекста переведем значение из 16ричной системы в символную. (рис. @fig:001):



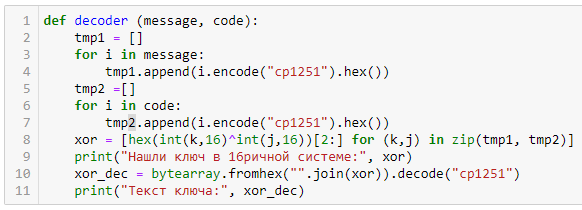
Функция кодирования

1. Вызовем функцию crypto, она возвращает закодированное сообщение в символьном виде, оно нам понадобится для следущего задания. Также именно на скриншоте можем увидеть все, что выводит функция (рис. @fig:002):



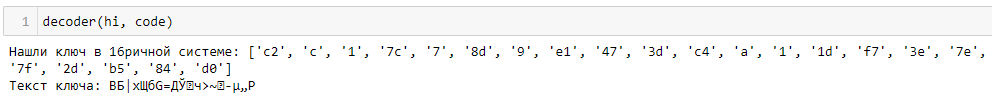
Вызов функции crypto

1. Напишем функция для нахождения ключа для декодирования сообщения. На вход принимается открытое сообщение и зашифрованное. Для начала переведем оба сообщения в 16ричную систему счисления. А затем снова выполним операцию гаммирования, т.е. сложим по модулю 2. Таким образом получим ключ. Затем для наглядности переведем ключ в символьный вид (рис. @fig:003):



Функция для получения ключа

1. Вызовем функию decoder, передадим ей открытый ключ и шифротекст в символьном виде. На эран выводится ключ в 16ричной системе счисления и в символьном виде (рис. @fig:004):



Вызов функции decoder

# Выводы

Освоила на практике применение режима однократного гаммирования. Закодировала сообщение с помощью создания случайного ключа и нашла ключ исходя из открытого текста и шифротекста.