Лабораторная работа №8

Элементы криптографии. Шифрование (кодирование) различных исходных текстов одним ключом

Дугаева Светлана Анатольевна

Содержание

[Цель работы 1](#_Toc90566658)

[Выполнение лабораторной работы 1](#_Toc90566659)

[Выводы 3](#_Toc90566660)

# Цель работы

Освоить на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.

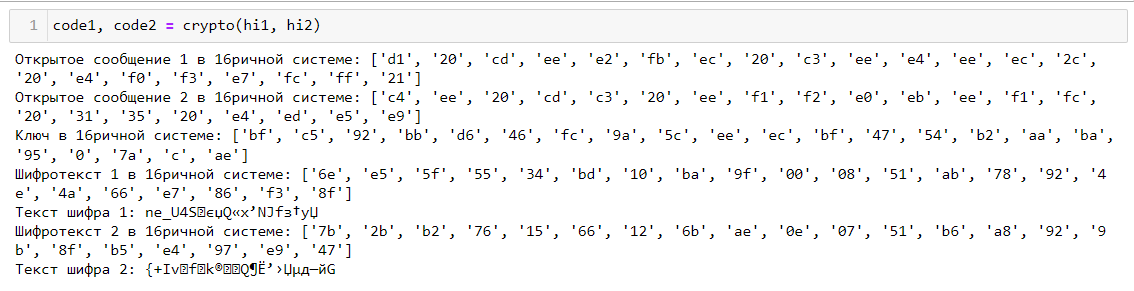
# Выполнение лабораторной работы

1. Сначала подключим нужные библеотеки. Затем в переменные hi1 и hi2 запишем 2 наших сообщения, которые требуется зашифровать. Наиболее удобным вариантом будет написать функцию (crypto), которая принимет на вход 2 открытых сообщения(словами). После этого переведем оба сообщения 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. Наложим гамму, то есть выполним операцию сложения по модулю 2(XOR) между элементами полученного случайного ключа и элементами подлежащего сокрытию текста (проведем данную операцию 2 раза, поскольку у нас 2 сообщения). Для получания шифротекста переведем значение из 16ричной системы в символную. (рис. @fig:001):



Функция кодирования

1. Вызовем функцию crypto, она возвращает 2 закодированных сообщения в символьном виде, они нам понадобится для следущего задания. Также именно на скриншоте можем увидеть все, что выводит функция (рис. @fig:002):



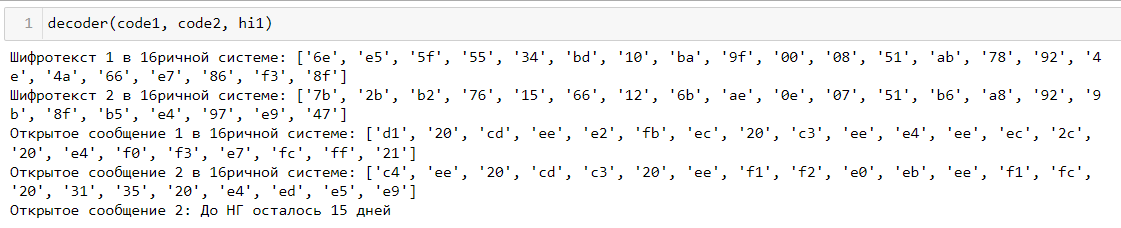
Вызов функции crypto

1. Напишем функцию decoder для нахождения ключа для декодирования 2го сообщения. На вход принимается 2 зашифрованных сообщения и одно открытое. Для начала переведем оба зашифрованных сообщения и одно открытое в 16ричную систему счисления. А затем снова выполним операцию гаммирования, т.е. сложим по модулю 2 между 2мя зашифрованными сообщениями, а потом проделаем ту же операцию между полученным резьтатом и открытым сообщением. Таким образом получим второе открытое сообщение в 16 системе сичисления. Затем для наглядности переведем данное сообщение в символьный вид (рис. @fig:003):



Функция для получения второго открытого сообщения

1. Вызовем функию decoder, передадим ей 2 зашифрованных сообщения и одно открытое в символьном виде. На эран выводятся сообщения в 16ричной системе счисления, а так же полученное открытое сообщение в символьном виде. Декодировка произведена верно, сообщение совпадает с изначальным (рис. @fig:004):



Вызов функции decoder

# Выводы

Освоила на практике применение режима однократного гаммирования на примере кодирования различных исходных тестов одним ключом. Закодировала два сообщения с помощью создания случайного ключа и нашла второе открытое сообщение исходя из открытого текста одного сообщения и двух зашифрованных.