Отчёт по лабораторной работе №7

Элементы криптографии. Однократное гаммирование

Морозов Михаил Евгеньевич

Содержание

Список иллюстраций

Список таблиц

1 Цель работы

Освоить на практике применение режима однократного гаммирования.

2 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. Например, в поле Галуа суммирование принимает вид операции “исключающее ИЛИ (XOR)”. [1]

3 Выполнение лабораторной работы

Напишем функции на python и зададим переменные. (рис. 3.1)

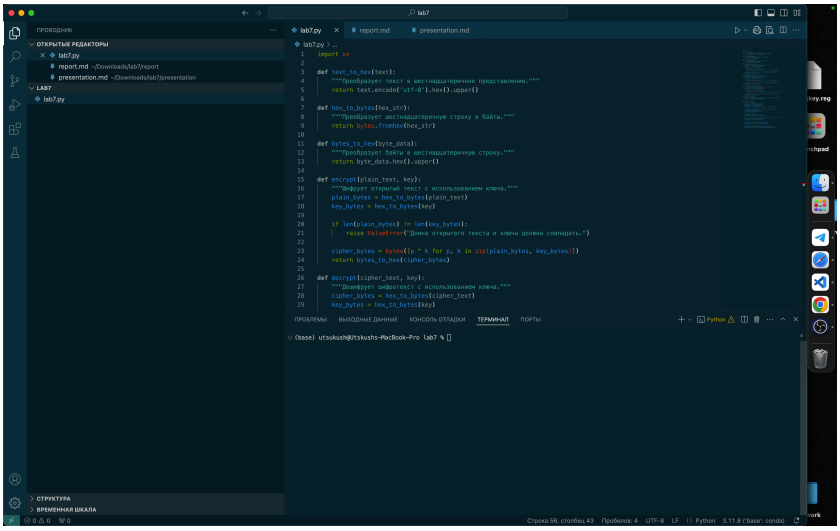

Рис. 3.1: Код. Часть 1

Напишем функции на python и зададим переменные. (рис. 3.2)

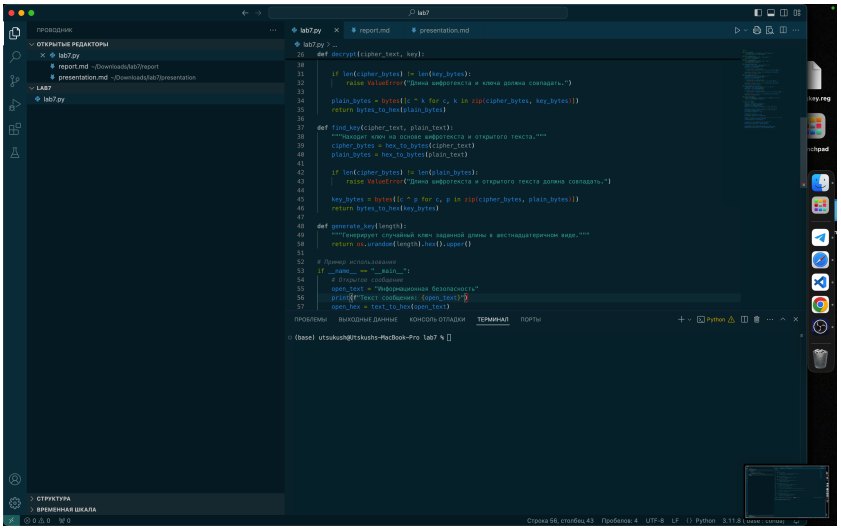

Рис. 3.2: Код. Часть 2

Напишем функции на python и зададим переменные. (рис. 3.3)

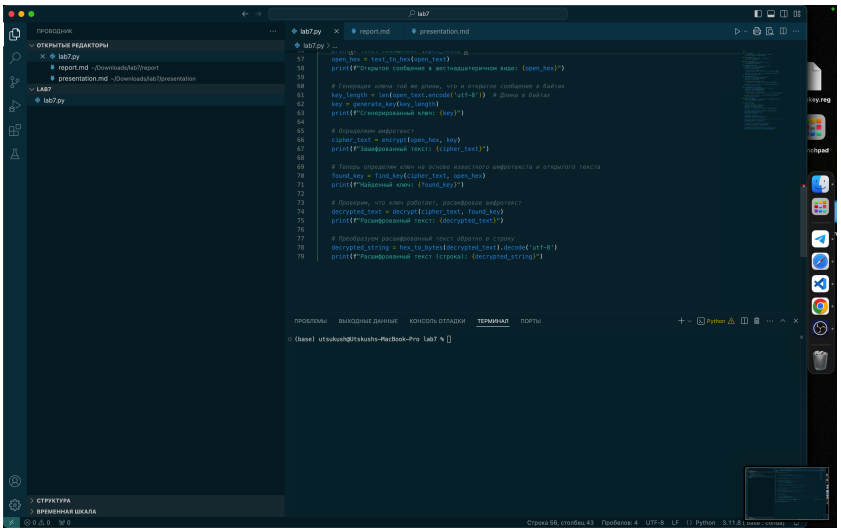

Рис. 3.3: Код. Часть 3

Применим написанные функции для создания ключа, шифрования текста и дешифрования. (рис. 3.4)

Рис. 3.4: Получили “С новым годом, друзья!”

4 Выводы

Освоили на практике применение режима однократного гаммирования.

Список литературы

1. Гаммирование [Электронный ресурс]. Wikimedia Foundation, Inc., 2024. URL: https://en.wikipedia.org/wiki/XOR_cipher.