Отчёт

по лабораторной работе 7

Агеева Анастасия Борисовна

Содержание

# Цель работы

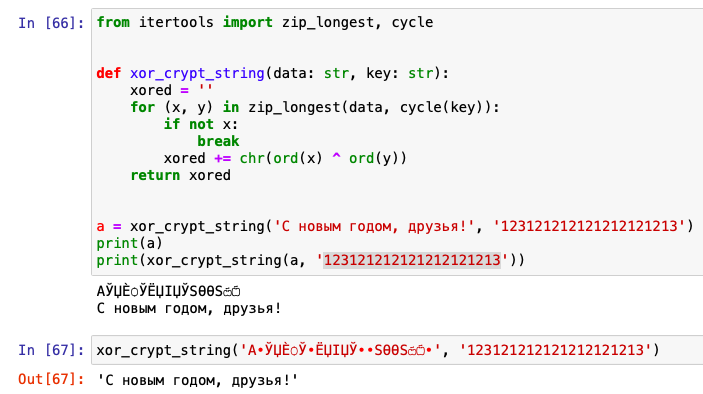
Освоить на практике применение режима однократного гаммирования.

# Задание

Лабораторная работа подразумевает подобрать ключ, чтобы получить сообщение «С Новым Годом, друзья!». Требуется разработать приложение, позволяющее шифровать и дешифровать данные в режиме однократного гаммирования.

# Выполнение лабораторной работы

1. Разработаем приложение, позволяющее шифровать и дешифровать данные в режиме однократного гаммирования. (рис.1).

* 
* Figure 1: рис.1. Программа.

1. Подоберём ключ, чтобы получить сообщение «С Новым Годом Вас!». После ключа текст становится неизменным. (рис.2).

* 
* Figure 2: рис.2. Определение ключа.

1. Контрольные вопросы
2. Поясните смысл однократного гаммирования. Каждый символ попарно с символом ключа складываются по модулю.
3. Перечислите недостатки однократного гаммирования. Ключ нельзя переиспользовать. Размер ключа должен быть такой же, как и размер текста.
4. Перечислите преимущества однократного гаммирования. Основные преимущества однократного гаммирования – это симметричность и криптостойкость.
5. Почему длина открытого текста должна совпадать с длиной ключа? Потому что каждый символ открытого текста должен складываться символом ключа попарно.
6. Какая операция используется в режиме однократного гаммирования, назовите её особенности? В режиме однократного гаммирования используется сложение по модулю 2. Её особенность состоит в том, что при сложении чисел с другим получается исходное.Например, 0+0 = 0, 0+1=1, 1+0=1, 1+1=0.
7. Как по открытому тексту и ключу получить шифротекст? Нужно сложить попарно символы текста с ключом по модулю 2.
8. Как по открытому тексту и шифротексту получить ключ? Нужно сложить попарно символы открытого текста с символами шифротекста по модулю 2.
9. В чем заключаются необходимые и достаточные условия абсолютной стойкости шифра? Необходимые и достаточные условия абсолютной стойкости шифра: а) полная случайность ключа; б) равенство длин ключа и открытого текста; в) использование ключа однкратно.

# Выводы

Я приобрела практические навыки применения режима однократного гаммирования.