Отчёт

по лабораторной работе 7

Лекомцева Алёна

Содержание

[Цель работы 1](#_Toc95003533)

[Задание 1](#_Toc95003534)

[Выполнение лабораторной работы 1](#_Toc95003535)

[Выводы 3](#_Toc95003536)

# Цель работы

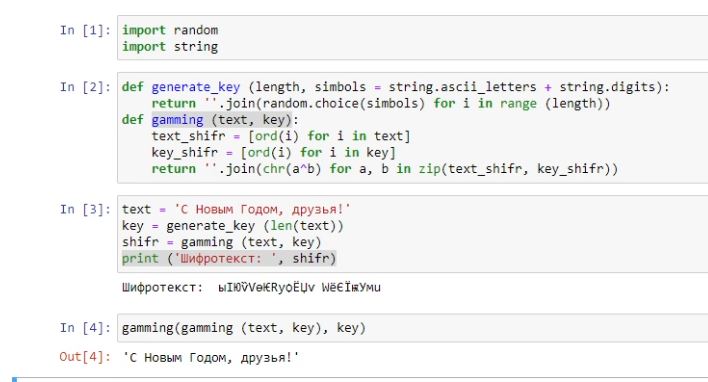
Освоить на практике применение режима однократного гаммирования.

# Задание

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).

* 
* рис.1. Программа.

1. Подоберём ключ, чтобы получить один из вариантов прочтения открытого текста. (рис.2).

* 
* рис.2. Определение ключа.

1. Контрольные вопросы:
2. Поясните смысл однократного гаммирования. Каждый символ открытого текста попарно по модулю 2 складывается с символом ключа.
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. Также простота использования.
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 она симметрична, то есть при повторном применении дает исходное значение. Например, если мы применим к открытому тексту гаммирование, а затем к получившемуся зашифрованному тексту применим гаммирование еще раз с темже ключом, то получим изначальный открытый текст.
7. Как по открытому тексту и ключу получить шифротекст? Нужно попарно сложить по модулю 2 символы текста с символами ключа.
8. Как по открытому тексту и шифротексту получить ключ? Нужно попарно сложить по модулю 2 символы открытого текста с символами шифротекста.
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.