Отчёт по лабораторной работе №7

Серегин Денис Алексеевич

Содержание

# 1 Цель работы

Освоить на практике применение режима однократного гаммирования.

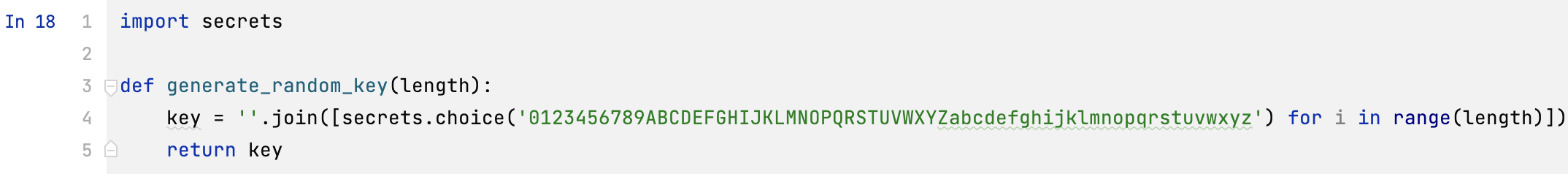
# 2 Задание

Нужно подобрать ключ, чтобы получить сообщение **«С Новым Годом, друзья!»**. Требуется разработать приложение, позволяющее шифровать и дешифровать данные в режиме однократного гаммирования. Приложение должно:

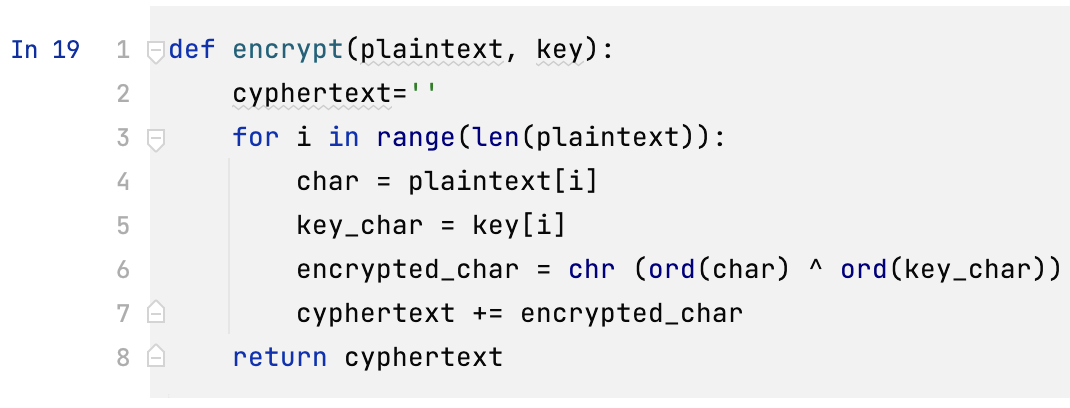
1. Определить вид шифротекста при известном ключе и известном открытом тексте.
2. Определить ключ, с помощью которого шифротекст может быть преобразован в некоторый фрагмент текста, представляющий собой один из возможных вариантов прочтения открытого текста.

# 3 Выполнение лабораторной работы

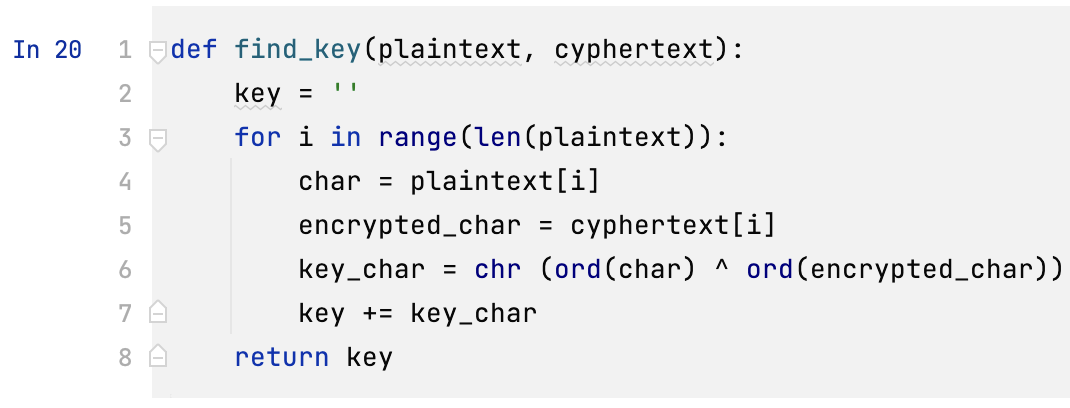
1. Изучил указания к лабораторной работе
2. Написал функцию генерации случайного ключа. (рис. ??)

* 
* Функция генерации ключа

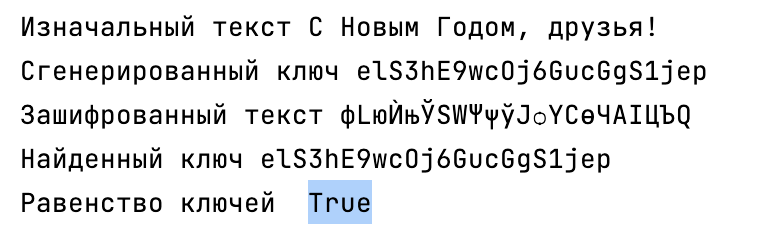
1. Написал функцию шифрования текста основываюсь на однократном гаммировании. (рис. ??)

* 
* Функция шифрования

1. Написал функцию нахождения ключа при наличии исходного текста и зашифрованного текста. (рис. ??)

* 
* Функция нахождения ключа

1. Проверил работу своих методов на фразе «С Новым Годом, друзья!» (рис. ??)

* 
* Вывод работы программы

# 4 Выводы

В результате выполнения работы я смог освоить метод однократного гаммирования и написать на его основе шифруюшее приложение.