Отчёт по лабораторной работе №8

Серегин Денис Алексеевич

Содержание

# 1 Цель работы

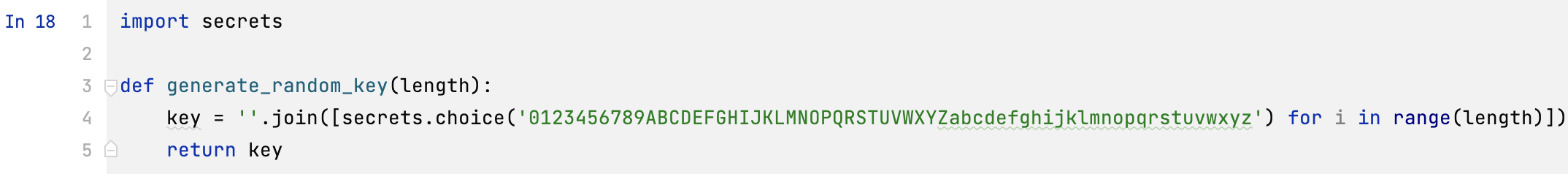
Освоить на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.

# 2 Задание

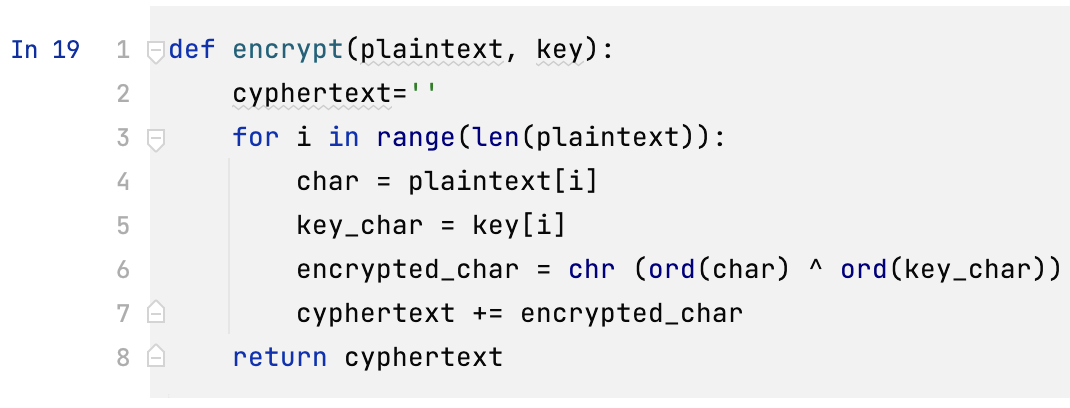
1. Два текста кодируются одним ключом (однократное гаммирование). Требуется не зная ключа и не стремясь его определить, прочитать оба текста. Необходимо разработать приложение, позволяющее шифровать и дешифровать тексты P1 и P2 в режиме однократного гаммирования. Приложение должно определить вид шифротекстов C1 и C2 обоих текстов P1 и P2 при известном ключе ; Необходимо определить и выразить аналитически способ, при котором злоумышленник может прочитать оба текста, не зная ключа и не стремясь его определить.

# 3 Выполнение лабораторной работы

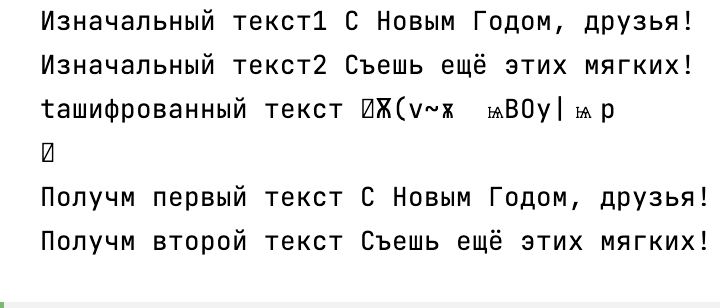
1. Изучил указания к лабораторной работе
2. Написал функцию генерации случайного ключа. (рис. ??)

* 
* Функция генерации ключа

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

* 
* Функция шифрования

1. Взял два текста и зашифровал их друг другом (рис. ??)
2. Попробовал расшифровать полученный текст используя изначальные тексты. Как итог расшифровывая одним текстом я получал другой исходный. (рис. ??)

* 
* Вывод работы программы

# 4 Выводы

В результате выполнения работы я смог освоить метод однократного гаммирования и написать на его основе шифруюшее приложение, чтобы зашифровать два текста.