Лабораторная работа №8

Царитова Нина, НПМбд-01-19

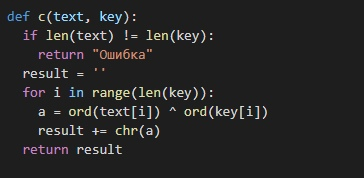
Содержание

# Цель работы

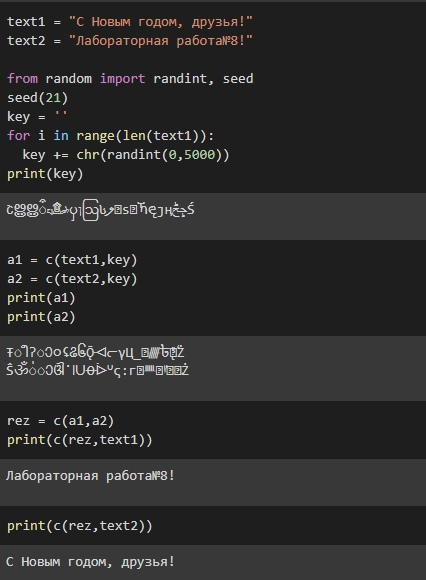
Освоить на практике применение однократного гаммирования при работе с различными текстами на одном ключе.

# Выполнение лабораторной работы

Cоздаём функцию, которая осуществляет однократное гаммирование посредством побитового XOR



Задаём две равные по длине текстовые строки и создаём случайный символьный ключ такой же длины и осуществляем шифрование двух текстов по ключу с помощью написанной функции. Создаём переменную, которая, прогнав два шифрованных текста через побитовый XOR, поможет злоумышленнику получить один текст, зная другой, без ключа.



# Выводы

Я освоила на практике применение режима однократного гаммирования при работе с несколькими текстами.

# Список литературы

* Медведовский И.Д., Семьянов П.В., Платонов В.В. Атака через Internet. — НПО “Мир и семья-95”, 1997. — URL: http://bugtraq.ru/library/books/attack1/index.html
* Медведовский И.Д., Семьянов П.В., Леонов Д.Г. Атака на Internet. — Издательство ДМК, 1999. — URL: http://bugtraq.ru/library/books/attack/index.html
* Запечников С. В. и др. Информационн~пасность открытых систем. Том 1. — М.: Горячаая линия -Телеком, 2006.