Лабораторная работа №8

Дисциплина: Основы информационной безопасности

Коновалова Татьяна Борисовна

Содержание

# 1 Цель работы

Цель лабораторной работы — Освоить на практике применение однократного гаммирования при работе с различными текстами на одном ключе.

# 2 Теоретические данные

Гаммирование представляет собой наложение (снятие) на открытые (зашифрованные) данные последовательности элементов других данных, полученной с помощью некоторого криптографического алгоритма, для получения зашифрованных (открытых) данных. Иными словами, наложение гаммы — это сложение её элементов с элементами открытого (закрытого) текста по некоторому фиксированному модулю, значение которого представляет собой известную часть алгоритма шифрования.

В соответствии с теорией криптоанализа, если в методе шифрования используется однократная вероятностная гамма (однократное гаммирование) той же длины, что и подлежащий сокрытию текст, то текст нельзя раскрыть. Даже при раскрытии части последовательности гаммы нельзя получить информацию о всём скрываемом тексте. Наложение гаммы по сути представляет собой выполнение операции сложения по модулю 2 (XOR) (обозначаемая знаком ⊕) между элементами гаммы и элементами подлежащего сокрытию текста.

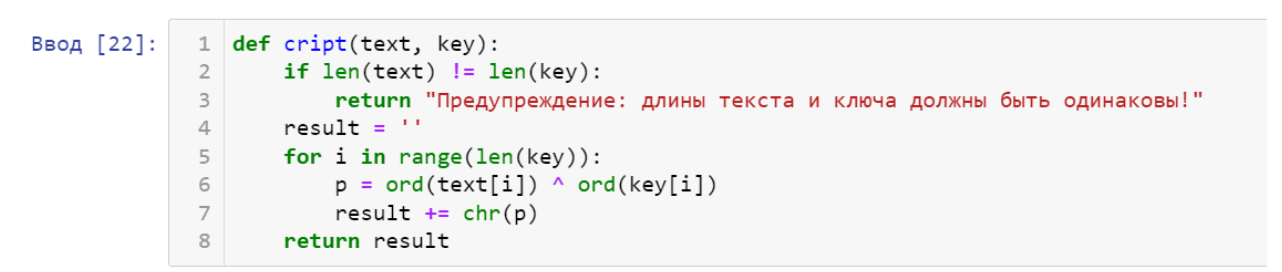
# 3 Задание

1.Не зная ключа и не стремясь его определить, прочитать оба исходных текста; 2.Разработать приложение, позволяющее шифровать и дешифровать тексты в режиме однократного гаммирования; 3.Определить и выразить аналитически способ, при котором злоумышленник может прочитать оба текста, не зная ключа и не стремясь его определить.

# 4 Выполнение лабораторной работы

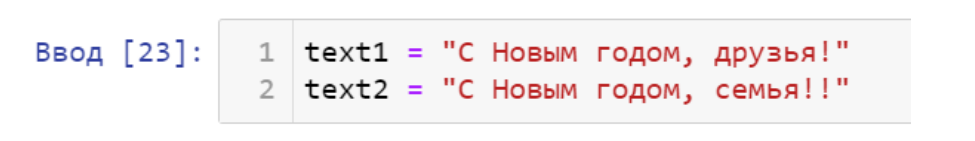
Лабораторную работу выполнила на языке Pythin 3 в среде Jupiter Notebook.

1.Cоздала функцию, которая осуществляет однократное гаммирование посредством побитового XOR (рис. [??]).

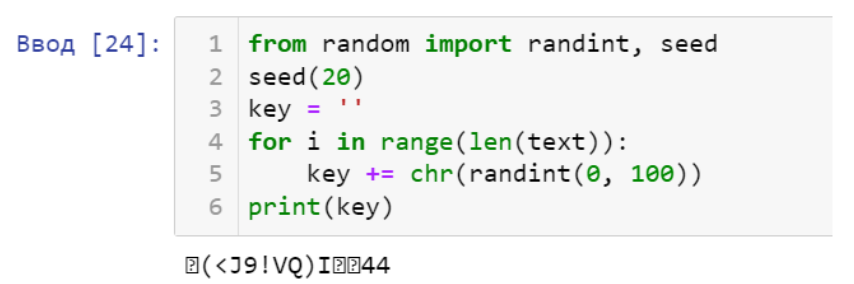


Функция шифрования

2.Задала две равные по длине текстовые строки и создала случайный символьный ключ такой же длины (рис. [??]) и (рис. [??]).

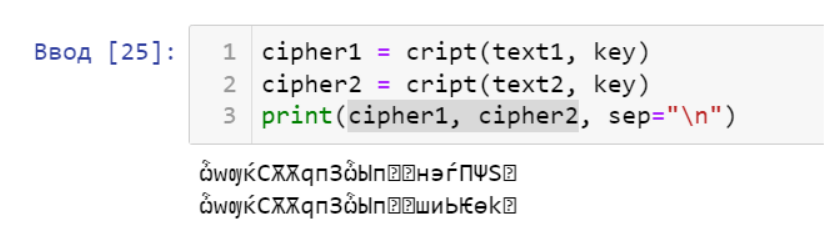


Исходные данные



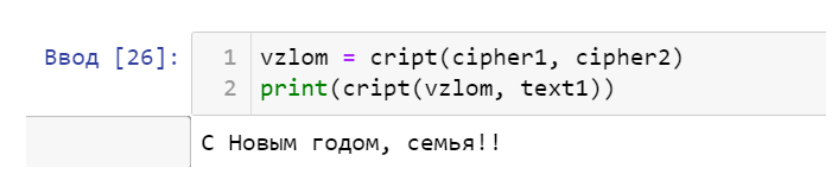
Случайный символьный ключ

3.Осуществила шифрование двух текстов по ключу с помощью написанной функции (рис. [??])

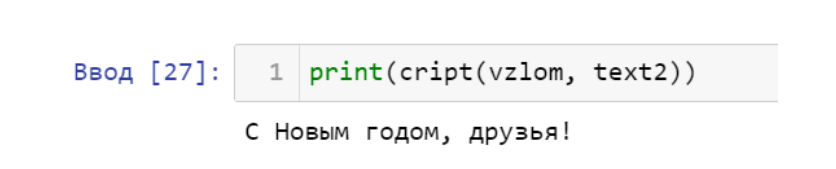


Шифрование данных

4.Создала переменную, которая, прогнав два шифрованных текста через побитовый XOR, поможет злоумышленнику получить один текст, зная другой, без ключа (рис. [??]) и (рис. [??]).

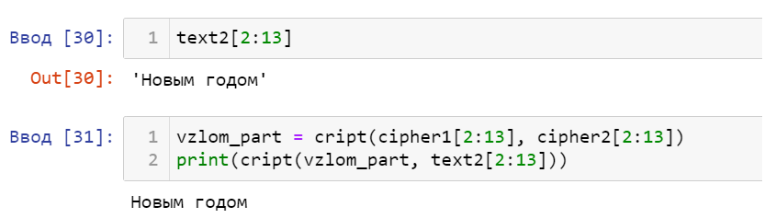


Получение данных без ключа



Получение данных без ключа

5.Таким же способом я получила часть данных из исходных предложений (рис. [??])



Получение части данных

# 5 Выводы

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

# 6 Библиография

СПИСОК ЛИТЕРАТУРЫ

1.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

2.Теоретические знания, приведённые в Лабораторной работе №8 - https://esystem.rudn.ru/pluginfile.php/2090135/mod\_resource/content/2/008-lab\_crypto-key.pdf

3.Запечников С. В. и др. Информационн~пасность открытых систем. Том 1. — М.: Горячаая линия -Телеком, 2006.

СПИСОК ИНТЕРНЕТ-ИСТОЧНИКОВ

1.[Электронный ресурс] - доступ: https://codeby.school/blog/informacionnaya-bezopasnost/razgranichenie-dostupa-v-linux-znakomstvo-s-astra-linux

2.[Электронный ресурс] - доступ: https://debianinstall.ru/diskretsionnoe-razgranichenie-dostupa-linux/