Лабораторная работа 8

Элементы криптографии. Шифрование (кодирование) различных исходных текстов одним ключом

Илья Валерьевич Фирстов

Содержание

Список иллюстраций

Список таблиц

Цель работы

Освоить на практике применение гаммирования нескольких текстов.

Задание

Развить навыки администрирования ОС Linux

Теоретическое введение

Предложенная Г. С. Вернамом так называемая «схема однократного использования (гаммирования)» (рис. 7.1) является простой, но надёжной схемой шифрования данных.

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.

Выполнение лабораторной работы

Взял из предыдущей работы функцию гаммирования (рис. [-@fig:001])

```
def gamma(istr,key):
    output = ""
    for i in range(0,len(istr)):
        output += chr(ord(istr[i]) ^ ord(key[i]))
    return output
```

Рис. 1: Функция наложения гаммы

Написал программу, которая шифрует оба текста одним ключом, выводит шифротексты, затем выводит их расшифровку, после этого выводит результат гаммирования двух шифротекстов и одного из исходных текстов. Таким образом удалось получить второй исходный текст, не находя ключ.(рис. [-@fig:002])

Рис. 2: Листинг программы

Протестировал работоспособность программы(рис. [-@fig:003])

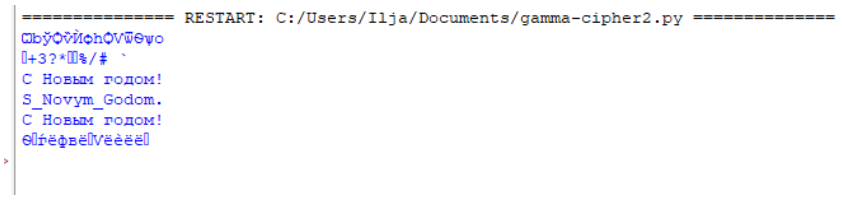

Рис. 3: Работа программы

Выводы

Я освоил на практике применение гаммирования нескольких текстов.

Список литературы