Лабораторная работа 7

Элементы криптографии. Однократное гаммирование

Илья Валерьевич Фирстов

Содержание

Цель работы 5

Задание 6

Теоретическое введение 7

Выполнение лабораторной работы 8

Выводы 10

Список литературы 11

Список иллюстраций

1 Функция наложения гаммы 8
2 Листинг программы 8
3 Работа программы 9

Список таблиц

Цель работы

Освоить на практике применение режима однократного гаммирования

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

Создал на языке python функцию для наложения гаммы (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 для шифровки, расшифровки текста и поиска ключа (рис. [-@fig:002])

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

text = "С Новым годом!"
key =  "ABCDEFGHIJKLMN"
cipher = gamma(text,key)
print(text)
print(key)
print(cipher)
print(" ")
print(gamma(cipher,key))
print(gamma(cipher,text))
```

Рис. 2: Листинг программы

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

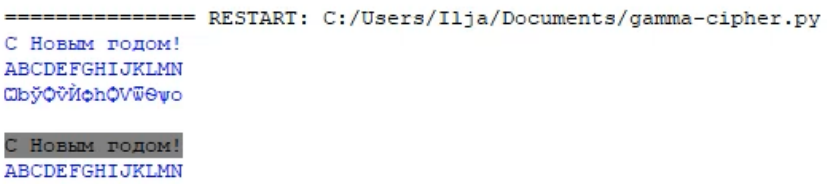

Рис. 3: Работа программы

Выводы

Я освоил на практике применение режима однократного гаммирования

Список литературы