Лабораторная работа 7

Элементы криптографии. Однократное гаммирование

Илья Валерьевич Фирстов

Содержание

# Цель работы

Освоить на практике применение режима однократного гаммирования

# Задание

Развить навыки администрирования ОС Linux

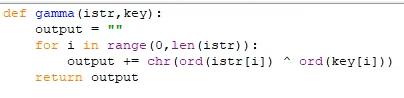
# Теоретическое введение

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.

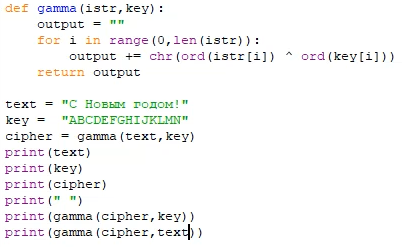
# Выполнение лабораторной работы

Создал на языке python функцию для наложения гаммы (рис. [-@fig:001])



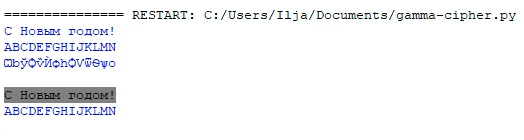
Функция наложения гаммы

Написал программу для шифровки, расшифровки текста и поиска ключа (рис. [-@fig:002])



Листинг программы

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



Работа программы

# Выводы

Я освоил на практике применение режима однократного гаммирования

# Список литературы