Отчет по лабораторной работе 8

Дисциплина: Информационная безопасность

Савченков Дмитрий Андреевич, НПИбд-02-18

Содержание

[Цель работы 1](#_Toc90731779)

[Выполнение лабораторной работы 1](#_Toc90731780)

[Выводы 2](#_Toc90731781)

[Список литературы 3](#_Toc90731782)

# Цель работы

Освоить на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.

# Выполнение лабораторной работы

1. Для выполнения данной лабораторной работы использовал язык программирования Python. Написал функции для последующей работы. (рис. -fig. 1)
   * Функция generate\_key берет на вход размер строки (size) в виде целового числа и строку символов с помощью которых мы будем генерировать ключ (в нашем случае мы будем использовать буквы английского алфавита и числа). А возвращает сгенерированный ключ в строковом формате (string).
   * Функция hex\_form берет на вход строку и возвращает её 16-ный вид данной строки.
   * Функция gamming берет на вход строку и сгенерированный ключ. А возвращает зашифрованную строку методом однократного гаммирования.



Figure 1: Функции

1. Использовал функции выше для определения новых переменных для дальнейшей работы. (рис. -fig. 2)
   * Переменная P\_1 - это исходная строка (телеграмма) из лабораторной работы “НаВашисходящийот1204”
   * Переменная P\_2 - это исходная строка (телеграмма) из лабораторной работы “ВСеверныйфилиалБанка”
   * Переменная gen\_key - это сгенерированный ключ, который мы получили из функции generate\_key.
   * Переменная hex\_key - это 16-ная форма сгенерированного ключа.
   * Переменная C\_1 - это шифротекст для первой телеграммы P\_1.
   * Переменная C\_2 - это шифротекст для второй телеграммы P\_2.
   * Переменная sum\_C - это сумма шифротекстов по модулю 2.

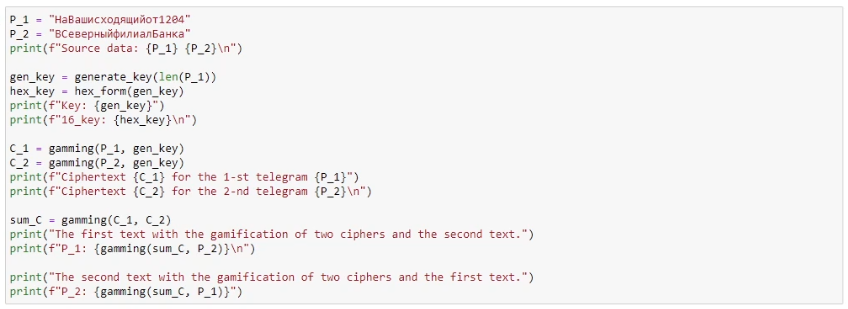


Figure 2: Переменные

1. Давайте изучим вывод программы. Вначале выводяться исходные телеграммы, ключ и его 16-ная форма. Затем выводиться шифротекст для двух исходных телеграмм, которые получены с помощью этой формулы C12 = P12 (+) K. В конце нам выводятся уже исходные телеграммы, которые получены с помощью суммирования C\_1 и C\_2 по модулю 2 и исходных телеграмм. (рис. -fig. 3)

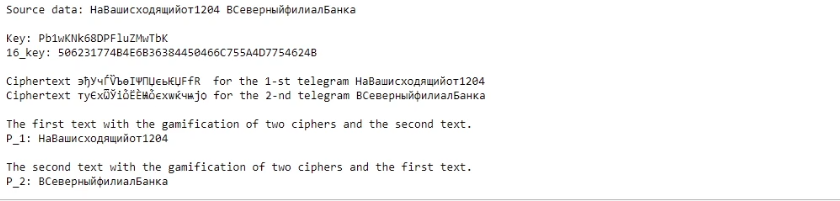


Figure 3: Вывод программы

# Выводы

Освоил на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.

# Список литературы

1. Кулябов Д. С., Королькова А. В., Геворкян М. Н. Информационная безопасность компьютерных сетей. Лабораторная работа № 5. Дискреционное разграничение прав в Linux. Исследование влияния дополнительных атрибутов