Front matter lang: ru-RU title: Презентация лабораторной работы № 7 author: |Макухина Анастасия institute: | RUDN University, Moscow, Russian Federation

Formatting toc: false slide_level: 4 theme: metropolis header-includes: - - ‘’ - ‘’ - ‘’ aspectratio: 43 section-titles: true

ЛАБОРАТОРНАЯ РАБОТА №7

Цель работы

Освоить на практике применение режима однократного гаммирования.

Однократное гаммирование

Гаммирование – это наложение (снятие) на открытые (зашифрованные) данные криптографической гаммы, то есть последовательности элементов данных, вырабатываемых с помощью некоторого криптографического алгоритма, для получения зашифрованных (открытых) данных.

Однократное гаммирование – это когда каждый символ попарно с символом ключа складываются по модулю 2 (XOR).

Алгоритм

При однократном гаммирование используется попарное сложение по модулю 2.

Такой метод шифрования является симметричным, так как двойное прибавление одной и той же величины по модулю 2 восстанавливает исходное значение, а шифрование и расшифрование выполняется одной и той же программой.

Программа

В данной работе мы создаём соответствующий алгоритм, позволяющий при двух известных компонентах (исходный текст, шифр, ключ) найти третий. У меня получилась следующая функция в pyton:

def gammirovanie(x, y):

```
    x_kod = [ord(i) for i in x]

    y_kod = [ord(i) for i in y]

    return ''.join(chr(x_i ^ y_i) for x_i, y_i in
    zip(x_kod, y_kod))
```

Вывод

В ходе выполнения лабораторной работы я изучила теорию и освоила на практике применение режима однократного гаммирования.