Front matter lang: ru-RU title: Презентация лабораторной работы № 8 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 №8

Цель работы

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

Однократное гаммирование одним ключом двух видов открытого текста

Режим шифрования однократного гаммирования одним ключом двух видов открытого текста реализуется следующим образом

$C1 = P1 \oplus K$

$C2 = P2 \oplus K$

Расшифровка

Открытый текст можно найти, зная шифротекст двух телеграмм, зашифрованных одним ключом. Для это оба равенства получаем:

$C1 \oplus C2 = P1 \oplus K \oplus P2 \oplus K = P1 \oplus P2.$

Тогда зная P1 можно найти P2

$C1 \oplus C2 \oplus P1 = P1 \oplus P2 \oplus P1 = P2.$

Программа

В данной работе мы создаём соответствующий алгоритм, позволяющий при трёх известных компонентах (2 исходных текста и ключ) найти шифры. У меня получилась следующая функция в pyton:

def gammirovanie(x, y, k):

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

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

    k_kod = [ord(i) for i in k]

    c1 = ''.join(chr(x_i ^ k_i) for x_i, k_i in zip(x_kod, k_kod))

    c2 = ''.join(chr(y_i ^ k_i) for y_i, k_i in zip(y_kod, k_kod))

    return c1, c2
```

Вывод

В ходе выполнения лабораторной работы я на практике изучила применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.