
Front matter

lang: ru-RU title: Отчёт по лабораторной работе №7 author: Георгес
Геден institute: РУДН, Москва, Россия

date: 19 Октября 2024

Formatting

toc: false slide_level: 2 theme: metropolis header-includes:

- `\metroset{progressbar=frametitle,sectionpage=progressbar,numbering=fraction}`
- `'\makeatletter'`
- `'\beamer@ignorenonframefalse'`
- `'\makeatother' aspectratio: 43 section-titles: true`

Отчет по лабораторной работе №7

Цель работы: Освоить на практике применение режима однократного гаммирования.

Теоретическое введение

Гаммирование - наложение (снятие) на открытые (зашифрованные) данные последовательности элементов других данных, полученной с помощью некоторого криптографического алгоритма, для получения зашифрованных (открытых) данных. Основная формула, необходимая для реализации однократного гаммирования: $C_i = P_i \text{ XOR } K_i$, где C_i - i -й символ зашифрованного текста, P_i - i -й символ открытого текста, K_i - i -й символ ключа. Аналогичным образом можно найти ключ: $K_i = C_i \text{ XOR } P_i$. Необходимые и достаточные условия абсолютной стойкости шифра:

- длина открытого текста равна длине ключа
- ключ должен использоваться однократно
- ключ должен быть полностью случаен

Более подробно см. в [1].

```
In [1]: import random
        from random import seed
        import string

In [2]: def cipher_text_function(text, key):
        if len(key) != len(text):
            return "Ключ и текст должны быть одной длины!"
        cipher_text = ''
        for i in range(len(key)):
            cipher_text_symbol = ord(text[i]) ^ ord(key[i])
            cipher_text += chr(cipher_text_symbol)
        return cipher_text

In [38]: text = "С НОВЫМ ГОДОМ, ДРУЗЬЯ!"

In [27]: key = ''
          seed(21)
          for i in range(len(text)):
              key += random.choice(string.ascii_letters + string.digits)
          print(key)

kASAOsE1nYEZ9G1GHpYaax

In [30]: cipher_text = cipher_text_function(text, key)
          print('Шифротекст:', cipher_text)

Шифротекст: ЪаЗѡиИЙиЩKSKLøJгЭЮУ

In [48]: print('Открытый текст:', cipher_text_function(cipher_text, key))

Открытый текст: С Новым годом, друзья!

In [49]: print('Ключ:', cipher_text_function(text, cipher_text))

Ключ: kASAOsE1nYEZ9G1GHpYaax
```

Выводы

- В ходе выполнения данной лабораторной работы я освоил на практике применение режима однократного гаммирования.