Перезнтация по лабораторной работе 7

Элементы криптографии. Однократное гаммирование

Неустроева И.Н.

19.05.25

Российский университет дружбы народов, Москва, Россия

Информация

Докладчик

- Неустроева Ирина Николаевна
- студентка группы НБИ 02-23
- Российский университет дружбы народов
- https://inneustroeva.github.io/ru/

Вводная часть

Актуальность

Умение решать задачи шифрования является ключевым навыком для специалистов в области информационной безопасности.

Цели и задачи

Освоить практическое использование режима однократного гаммирования.

Необходимо подобрать ключ для получения сообщения: “С Новым Годом, друзья!”. Нужно разработать приложение, которое будет обеспечивать шифрование и дешифрование данных в режиме однократного гаммирования. Приложение должно:

1. Определять вид шифротекста при известном ключе и открытом тексте.
2. Определять ключ, который позволяет преобразовать шифротекст в один из возможных вариантов открытого текста.

Материалы и методы

- Процессор `pandoc` для входного формата Markdown
- Результирующие форматы
  - `pdf`
  - `html`
- Автоматизация процесса создания: `Makefile`

Создание презентации

Программный код

In [1]:
```
import random
```

In [2]:
```
from random import seed
```

In [3]:
```
import string
```

In [7]:
```
# сложение двух строк по модулю (xor)
def xor_text_f(text, key):
    if len(key) != len(text):
        return "Ошибка: ключ и  текст разной длины!"
    xor_text = ''
    for i in range(len(key)):
        # функция ord возвращает целое число – номер из таблицы символов Unicode, представляющий позицию данного символа
        xor_text_symbol = ord(text[i]) ^ ord(key[i])
        xor_text += chr(xor_text_symbol)
    return xor_text
```

In [12]:
```
# ввод исходного текста
text = 'С Новым Годом, друзья!'
```

In [13]:
```
# создание ключа
key = ''
seed(22)
for i in range(len(text)):
    key += random.choice(string.ascii_letters + string.digits)
key
```

Out[13]:
```
'96ipbNClShVP4wY4for9du'
```

In [14]:
```
# получение шифротекста
xor_text = xor_text_f(text, key)
xor_text
```

Out[14]:
```
'И\x16VoèS¤Lpitƀ]J[yÈЦbxvЫT'
```

In [15]:
```
# открытый текст
xor_text_f(xor_text, key)
```

Out[15]:
```
'С Новым Годом, друзья!'
```

In [16]:
```
# получение ключа
xor_text_f(text, xor_text)
```

Out[16]:
```
'96ipbNClShVP4wY4for9du'
```

функция xortextf

Ключевым элементом этой программы является функция xortextf, которая принимает две строки для сложения. Эти строки должны иметь одинаковую длину, и программа проверяет это условие. Если длины строк различаются, выводится сообщение об ошибке. В случае успешной проверки мы поочередно применяем операцию сложения по модулю к символам строк, в результате чего получаем сумму двух строк.

Итог работы

В процессе выполнения лабораторной работы я овладела навыками шифрования и дешифрования сообщений с использованием однократного гаммирования и познакомилась с этим методом в криптографии.

:::