Презентация по лабораторной работе №7

Информационная безопасность

Чекалова Л. Р.

19 октября 2023

Российский университет дружбы народов, Москва, Россия

Информация

Докладчик

- Чекалова Лилия Руслановна
- студент 4 курса группы НФИбд-02-20
- ст. б. 1032201654
- Российский университет дружбы народов
- 1032201654@pfur.ru

Вводная часть

Цели и задачи

- Освоение на практике применение режима однократного гаммирования
- Написание программы для шифрования сообщений

Материалы и методы

- Веб-сервис `GitHub` для работы с репозиториями
- Интерактивный блокнот `Jupyter` для работы на языке `Python`
- Процессор `pandoc` для входного формата Markdown
- Результирующие форматы
  - `pdf`
  - `docx`
- Автоматизация процесса создания: `Makefile`

Ход работы

Программа, 1

```
import string
import random
import sys
```

```
def gen_key(size):
    res = ''
    for i in range(size):
        res += random.choice(string.ascii_letters)
    return res

def to_hex(text):
    res = ''
    for i in text:
        res += hex(ord(i))[2:] + ' '
    return res

def encrypt(text, key):
    res = ''
    for (t, k) in zip(text, key):
        res += chr(t^k)
    return res
```

Программа, 2

```
message = 'С Новым Годом, друзья!'
message16 = to_hex(message)
key = gen_key(len(message))
k = to_hex(key)
encr_m = encrypt([ord(i) for i in message], [ord(i) for i in key])
encr_m16 = to_hex(encr_m)
decr_m = encrypt([ord(i) for i in encr_m], [ord(i) for i in key])
key_new = encrypt([ord(i) for i in message], [ord(i) for i in encr_m])

print('open text:', message, '\nopen text in 16:', message16, '\nkey:', key, '\nkey in 16:', k)
print('encrypted text:', encr_m, '\nencrypted text in 16:', encr_m16, '\ndecrypted message:', decr_m, '\nfound key:', key_new)
```

Результат работы программы

```
open text: С Новым Годом, друзья!
open text in 16: 421 20 41d 43e 432 44b 43c 20 413 43e 434 43e 43c 2c 20 434 440 443 437 44c 44f 21
key: yrUoagIfelIRXuENBgXdDi
key in 16: 79 72 55 6f 61 67 49 66 65 6c 49 52 58 75 45 4e 42 67 58 64 44 69
encrypted text: јRшёѓЬѵFѶђѽѬѤYeѺЂФѯШЋH
encrypted text in 16: 458 52 448 451 453 42c 475 46 476 452 47d 46c 464 59 65 47a 402 424 46f 428 40b 48
decrypted message: С Новым Годом, друзья!
found key: yrUoagIfelIRXuENBgXdDi
```

Результаты

Результаты работы

- Рассмотрены основные элементы криптографии
- Получены базовые навыки применения однократного гаммирования