Презентация по лабораторной работе №7

Информационная безопасность

Нгуен Фыок Дат

21 октября 2023

Российский университет дружбы народов, Москва, Россия

Информация

Докладчик

- Нгуен Фыок Дат
- студент 4 курса группы НФИбд-01-20
- ст.б.1032195855
- Российский университет дружбы народов
- 1032195855@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

```
msg ="С Новым Годом, друзья!"
msg16 = to_hex(msg)
key = gen_key(len(msg))
k = to_hex(key)
encr_m = encrypt([ord(i) for i in msg], [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 msg], [ord(i) for i in encr_m])

print("open text:", msg, "\nopen text in 16:", msg16, "\nkey:", key, "\nkey in 16:", k)
print("encrypted text:", encr_m, "\nencrypted text in 16", encr_m16, "\ndecrypted msg:", 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: hyvCGKJYdNeNvobNPQQuWq
key in 16: 68 79 76 43 47 4b 4a 59 64 4e 65 4e 76 6f 62 4e 50 51 51 75 57 71
encrypted text: щУжЎvЁЎуЎЎЁЎъСВQАВАЙИР
encrypted text in 16 449 59 46b 47d 475 400 476 79 477 470 451 470 44a 43 42 47a 410 412 466 439 418 50
decrypted msg: С Новым Годом, друзья!
found key: hyvCGKJYdNeNvobNPQQuWq
```

Результаты

Результаты работы

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