Презентация по лабораторной работе №8

Информационная безопасность

Чекалова Л. Р.

26 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 применения режима однократного гаммирования на примере кодирования различных текстов одним ключом
- 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 encrypt(text, key):
    res = ''
    for (t, k) in zip(text, key):
        res += chr(t^k)
    return res
```

Программа, 2

```
message1 = 'С Новым Годом, друзья!'
message2 = 'Счастливого рождества!'
key = gen_key(len(message1))
encr_m1 = encrypt([ord(i) for i in message1], [ord(i) for i in key])
encr_m2 = encrypt([ord(i) for i in message2], [ord(i) for i in key])
temp = encrypt([ord(i) for i in encr_m1], [ord(i) for i in encr_m2])
open1 = encrypt([ord(i) for i in temp], [ord(i) for i in message2])
open2 = encrypt([ord(i) for i in temp], [ord(i) for i in open1])

print('open text1:', message1, '\nopen text2:', message2, '\nkey:', key)
print('encrypted text1:', encr_m1, '\nencrypted text2:', encr_m2)
print('decrypted text1:', open1, '\ndecrypted text2:', open2)
```

Результат работы программы

```
open text1: С Новым Годом, друзья!
open text2: Счастливого рождества!
key: FiVePMeBSsTEGunnuETpsA
encrypted text1: ѧIыћЂIљbрэѠѻоYNњeIѢмм`
encrypted text2: ѧЮѦФВѶйѰѫрѪeЇыjњрЄЖту`
decrypted text1: С Новым Годом, друзья!
decrypted text2: Счастливого рождества!
```

Результаты

Результаты работы

- Закреплены знания об основных элементах криптографии
- Отработаны навыки применения однократного гаммирования
- Написана программа для расшифровки текстов без использования ключа