Презентация по лабораторной работе №7

Информационная безопасность

Байрамгельдыев Довлетмурат

21 октября 2023

Российский университет дружбы народов, Москва, Россия

Информация

Докладчик

- Байрамгельдыев Довлетмурат
- студент 4 курса группы НФИбд-01-20
- ст. б. 1032207470
- Российский университет дружбы народов
- 1032207470@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

```
[1]  import string
     import random
     import sys
```

```
     def hex_16(txt):
         return ' '.join(hex(ord(i))[2:] for i in txt)

     def cypher(size):
         return ''.join(random.choice(string.ascii_letters + string.digits) for _ in range(size))

     def decypher(txt, key):
         return ''.join(chr(a^b) for a, b in zip(txt, key))
```

Программа, 2

0 сек.

```
message = "С новым годом, друзья!"
key = cypher(len(message))
hex_key = hex_16(key)
print("Ключ: ", key)
print("Ключ в 16-ричном виде: ", hex_key)
encr = decypher([ord(i) for i in message], [ord(i) for i in key])
hex_encr = hex_16(encr)
print("Зашифр. сообщение:", hex_encr)
decr = decypher([ord(i) for i in encr], [ord(i) for i in key])
print("Расшифр. сообщение:", decr)

decr1=decypher ([ord(i) for i in encr], [ord(i) for i in key])
print("Ключ: ", key)
print("Вариант прочтения откр. текста: ", decr1)
```

Результат работы программы

```
Ключ:  rqvTz9i50Kf7dcfEnCdihY
Ключ в 16-ричном виде:  72 71 76 54 7a 39 69 35 30 4b 66 37 64 63 66 45 6e 43 64 69 68 59
Зашифр. сообщение: 453 51 44b 46a 448 472 455 15 403 475 452 409 458 4f 46 471 42e 400 453 425 427 78
Расшифр. сообщение: С новым годом, друзья!
Ключ:  rqvTz9i50Kf7dcfEnCdihY
Вариант прочтения откр. текста:  С новым годом, друзья!
```

Результаты

Результаты работы

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