Презентация к лабораторной работе 8

Элементы криптографии. Шифрование (кодирование) различных исходных текстов одним ключом

Саттарова В.В.

28 октября 2023

Российский университет дружбы народов, Москва, Россия

Информация

Докладчик

- Саттарова Вита Викторовна
- студент НФИбд-02-20, 1032201655
- Российский университет дружбы народов

Вводная часть

Актуальность и прагматика

- Практические навыки применения шифрования позволяют обеспечить лучшую безопасность информации в системе

Цели

- Изучить основы криптографии.
- Освоить на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.

Задачи

- Выполнить все пункты, указанные в методических рекомендациях к лабораторной работе.
- Выполняя задания, познакомиться с основами криптографии.
- Выполняя задания, использовать режим однократного гаммирования для кодирования различных исходных текстов одним ключом.
- Написать отчёт, проанализировав результаты, полученные в ходе выполнения лабораторной работы.

Функции для однократного гаммирования

Ввод [16]:
```
import random as rd
```

Ввод [17]:
```
# строка
message = "С Новым Годом, друзья!"
```

Ввод [18]:
```
# перевод в 16
def hex_string(mes):
    return " ".join([hex(ord(elem))[2:] for elem in mes])
```

Ввод [19]:
```
# ключ
def make_key(mes):
    base = "abcdefghijklmnopqrstuvwxyzабвгдеёжзийклмнопрстуфхцчшщъыьэюя0123456789"
    return "".join([rd.choice(base) for i in range(len(mes))])
```

Ввод [20]:
```
# кодирование
def coding(mes, key):
    return "".join(chr(ord(mes[i]) ^ ord(key[i])) for i in range(len(mes)))
```

Рис. 1: Функции

Создание сообщений и применение функций

Ввод [6]:
```
P1 = "Странное и непонятное сообщение для работы"
P2 = "Просто сообщение для кодирования в работе2"
key = make_key(P1)
hex_key = hex_string(key)
C1 = coding(P1, key)
C2 = coding(P2, key)
```

Ввод [11]:
```
print("P1: ", P1)
print("P2: ", P2)
print("key: ", key)
print("hex_key: ", hex_key)
print("C1: ")
print(C1)
print("C2: ")
print(C2)
```

```
P1:  Странное и непонятное сообщение для работы
P2:  Просто сообщение для кодирования в работе2
key:  0уо8faыфх0эгюуiчiгшъvвhе7яуедэеюuоес7ро4h
hex_key:  30 79 6f 38 66 430 44b 444 78 30 44d 433 44e 6f 443 69 447 69 72 448 44a 76 432 68 65 37 44
f 443 435 434 44d 435 44e 75 6f 65 441 37 70 6f 34 68
C1:
uqXJжЗ{è}Ыяv VsiЋIЗxEzюPEЗЇсёЎУ
C2:
ЯйёэуФЗхЗцЎ|z{ђ{ќаіщЗЂьќйЎqqЗ     uzЗчOXqIюЭЁZ
```

Исследование возможностей получения информации

```
Ввод [12]: try1 = coding(C1, C2)
           try1

Out[12]: '>\x02~q\x7f\x03OtO\x06Бt\x00\x02\x06\x08ƺv\x06qEK\x7f\n\x06qw\x07\r\x05\rƷД\tƷΩp\x01\x0f|wy'

Ввод [13]: coding(try1, P1)

Out[13]: 'Просто сообщение для кодирования в работе2'

Ввод [14]: coding(try1, P2)

Out[14]: 'Странное и непонятное сообщение для работы'

Ввод [15]: try2 = coding(C1, P2)
           try2

Out[15]: '\x0e{\x11I\x19rUaA6\\чютха(\x1ftй_ЯэbcFифибpZZ|ЁS66\x7f\x13СБ'

Ввод [16]: try3 = coding(C1, P1)
           try3

Out[16]: 'Θуо8faыфx0эгюуiчiгшъvвhe7яуедэекuоес7ро4h'

Ввод [17]: coding(C2, P2)

Out[17]: 'Θуо8faыфx0эгюуiчiгшъvвhe7яуедэекuоес7ро4h'

Ввод [18]: coding(C2, P1)

Out[18]: '\x0e{\x11I\x19rUaA6\\чютха(\x1ftй_ЯэbcFифибpZZ|ЁS66\x7f\x13СБ'

Ввод [19]: coding(try2, C1)

Out[19]: 'Просто сообщение для кодирования в работе2'

Ввод [20]: coding(try2, C2)

Out[20]: 'Странное и непонятное сообщение для работы'

Ввод [21]: coding(try3, C1)

Out[21]: 'Странное и непонятное сообщение для работы'
```

Результаты

Результаты

- Изучены основы криптографии.
- Освоено на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.
- Написан отчёт к лабораторной работе.