Отчёт по лабораторной работе 7

Невзоров Дмитрий Сергеевич

2021

Цель работы

- Освоить на практике применение режима однократного гаммирования

Ход работы

- Нужно подобрать ключ, чтобы получить сообщение «С Новым Годом, друзья!». Разработаем приложение, позволяющее шифровать и дешифровать данные в режиме однократного гаммирования

Выполнение лабораторной работы

```
In [73]: import random
         import string
         vvod = input("Введите строку: ")

         Введите строку: С Новым Годом, друзья!

In [74]: def key_gener(size = 6, chars = string.ascii_letters + string.digits):
             return ''.join(random.choice(chars) for _ in range(size))
         def chan(s):
             return ":".join("{:02x}".format(ord(c)) for c in s)

In [75]: key = key_gener(len(vvod))

In [76]: print(f'Ключ в виде строки: {key}')

         Ключ в виде строки: uOssSwjTvvlb4bR31CiU1N
```

Рис.1 Начало выполнения работы

Выполнение лабораторной работы

- Продолжим выполнение работы (рис.2)

In [77]:
```
def gammirovanie(vvod, key):
    vvod_ascii = [ord(i) for i in vvod]
    key_ascii = [ord(i) for i in key]
    enc_str = ''.join(chr(s ^ k) for s, k in zip(vvod_ascii, key_ascii))
    return enc_str
def find_truekey(vvod, enc_str):
    sm_ascii = [ord(i) for i in vvod]
    enc_str_ascii = [ord(i) for i in enc_str]
    true_key = ''.join(chr(s ^ k) for s, k in zip(enc_str_ascii, sm_ascii))
    return true_key
def unencrypt(enc_str, key):
    enc_str_ascii = [ord(i) for i in enc_str]
    key_ascii = [ord(i) for i in key]
    true_str = ''.join(chr(s ^ k) for s, k in zip(enc_str_ascii, key_ascii))
    return true_str
```

In [78]:
```
enc_str = gammirovanie(vvod, key)
```

Рис.2

Выполнение лабораторной работы

- Завершение выполнения работы (рис.3)

```
In [79]: new_key = key_gener(len(enc_str))
         unencrypted_new_key = unencrypt(enc_str, new_key)
         true_key = find_truekey(vvod, enc_str)
         unencrypted_true_key = unencrypt(enc_str, true_key)

In [80]: print(f'Закодированная строка: {enc_str}')
         print(f'В шестнадцатеричной системе: {chan(enc_str)}')

         Закодированная строка: ЄoѮэѡміtѥшјќЈNrЇѱЀўЙѾo
         В шестнадцатеричной системе: 454:6f:46e:44d:461:43c:456:74:465:448:458:45c:408:4e:72:407:471:400:45e:419:47e:6f

In [81]: print(f'Подобранный ключ: {new_key}')
         print(f'Строка, расшифрованная ключом: {unencrypted_new_key}')
         print(f'Настоящий ключ: {true_key}')
         print(f'Декодированная строка: {unencrypted_true_key}')

         Подобранный ключ: sErOua2O2ndKsjCVgKkdWQ
         Строка, расшифрованная ключом: Ч*MЂДИЄ;ЇЦм3ҫ$1ёЖыеӢЩ>
         Настоящий ключ: uOssSwjTvvlb4bR31CiU1N
         Декодированная строка: С Новым Годом, друзья!
```

рис.3

Вывод

- В ходе выполнения лабораторной работы я изучил теорию и освоил на практике применение режима однократного гаммирования

Спасибо за внимание!