Презентация по лабораторной работе №8

Режим однократного гармонирования

Вактайпа М.

30 мая 2025

Российский университет дружбы народов, Москва, Россия

Информация

Докладчик

- Вакутайпа Милдред
- НКА 02-23
- Факультет физико-математических и естественных наук
- Российский университет дружбы народов
- 1032239009@rudn.ru
- https://wakutaipa.github.io

Цель работы

Цель работы

Освоить на практике применение режим однократного гаммирования на примере кодирования различных исходных текстов одним ключом.

Выполнение лабораторной работы

Расшифрированные тексты

В данной работе два текста кодируются одним ключом. Требуется почитать оба текста не зная ключа.

[1]:
```
import string
import random
```

[2]:
```
def generate_key(text):
    return ''.join(random.choice(string.ascii_letters + string.digits) for _ in text)
```

[3]:
```
def crypt(text, key):
    return ''.join(chr(ord(c) ^ ord(k)) for c, k in zip(text, key))
```

[4]:
```
def find_keys(cipher, fragment):
    return [''.join(chr(ord(cipher[i+j])^ord(f)))
            for i in range(len(cipher)-len(fragment)+1)
            for j, f in enumerate(fragment)]
```

[6]:
```
bland1 = 'НаВашисходящийот1204'
key1 = generate_key(bland1)
ciphered1 = crypt(bland1, key1)
decrypted1 = crypt(ciphered1, key1)

bland2 = 'ВСеверныйфилиалБанка'
ciphered2 = crypt(bland2, key1)
decrypted2 = crypt(ciphered2, key1)

print(f"orig:{bland1}, \nkey:{key1}, \nciphered:{ciphered1}")
print(f"orig:{bland2}, \nkey:{key1}, \nciphered:{ciphered2}")

unknown = crypt(ciphered1, ciphered2)
print(f"decrypt with unknown key: {crypt(bland1, unknown)}")
print(f"decrypt with unknown key: {crypt(bland2, unknown)}")
```

```
orig:НаВашисходящийот1204
```

Листинг программы 1

```
bland1 = 'НаВашисходящийот1204'
key1 = generate_key(bland1)
ciphered1 = crypt(bland1, key1)
decrypted1 = crypt(ciphered1, key1)

bland2 = 'ВСеверныйфилиалБанка'
ciphered2 = crypt(bland2, key1)
decrypted2 = crypt(ciphered2, key1)

print(f"orig:{bland1}, \nkey:{key1}, \nciphered:{ciphered1}")
print(f"orig:{bland2}, \nkey:{key1}, \nciphered:{ciphered2}")
```

Выводы

Выводы

При выполнение данной работыб я освоила на практике применение режим однократного гаммирования на примере кодирования различных исходных текстов одним ключом.