Элементы криптографии. Однократное гаммирование

Гаджиев Нурсултан НПИ-01-18

Информационная безопасность, 11 декабря, 2021, Москва, Россия

RUDN University

Цель лабораторной работы

Цель лабораторной работы

Освоить на практике применение режима однократного гаммирования

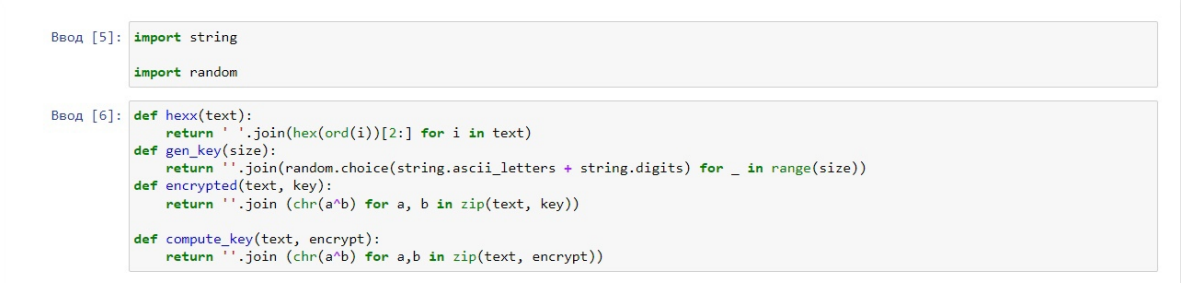
Процесс выполнения лабораторной работы

Выполнение работы

1. Блок функции для расчетов
2. Получение шифротекста
3. Вариант прочтения открытого текста

Блок функции для расчетов

Результат



Ввод [5]:
```
import string

import random
```

Ввод [6]:
```
def hexx(text):
    return ' '.join(hex(ord(i))[2:] for i in text)
def gen_key(size):
    return ''.join(random.choice(string.ascii_letters + string.digits) for _ in range(size))
def encrypted(text, key):
    return ''.join (chr(a^b) for a, b in zip(text, key))

def compute_key(text, encrypt):
    return ''.join (chr(a^b) for a,b in zip(text, encrypt))
```

Figure 1: Блок функции для расчетов

Получение шифротекста

Результат

Ввод [7]:
```
message= 'С Новым Годом, друзья!'

key=gen_key(len(message))
hex_key=hexx(key)

print("Используемый ключ: ", key)

print("Ключ в шестнадцатиричном виде: ", hex_key)

encrypt = encrypted([ord(i) for i in message], [ord(i) for i in key])
hex_encrypt=hexx(encrypt)

print("Зашифрованное сообщение:", hex_encrypt)

decryptt = encrypted([ord(i) for i in encrypt], [ord(i) for i in key])

print("Расшифрованное сообщение:", decryptt)
```

```
Используемый ключ:  a22rPGn2s8ziZkHxX8inhI
Ключ в шестнадцатиричном виде:  61 32 32 72 50 47 6e 32 73 38 7a 69 5a 6b 48 78 58 38 69 6e 68 49
Зашифрованное сообщение: 440 12 42f 44c 462 40c 452 12 460 406 44e 457 466 47 68 44c 418 47b 45e 422 427 68
Расшифрованное сообщение: С Новым Годом, друзья!
```

Figure 2: Получение шифротекста

Вариант прочтения открытого текста

```
Ввод [8]: compute_key = compute_key([ord(i) for i in message], [ord(i) for i in encrypt])

          decrypt_compute_key= encrypted([ord(i) for i in encrypt], [ord(i) for i in key])

          print("Вариант прочтения открытого текста", decrypt_compute_key)

          Вариант прочтения открытого текста С Новым Годом, друзья!
```

Figure 3: Прочтение открытого текста

Выводы

Выводы

Освоил на практике применение режима однократного гаммирования.