Элементы криптографии. Однократное гаммирование

Каримов Зуфар 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 [18]:
```
import string
import random
```

Ввод [19]:
```
def function1(text):
    return ' '.join(hex(ord(i))[2:] for i in text)

def function2(size):
    return ''.join(random.choice(string.ascii_letters+string.digits) for _ in range(size))

def function3(text,key):
    return ''.join(chr(a^b) for a,b in zip (text,key))

def function4(text,encrypt):
    return ''.join(chr(a^b) for a,b in zip (text, encrypt))
```

Figure 1: Блок функции для расчетов

Получение шифротекста

Результат

Ввод [20]:
```
message = 'С новым Годом, друзья!'
key = function2(len(message))
hex_key = function1(key)
print("Используем ключ: ", key)
print("Ключ в шестнадцатиричном виде: ", hex_key)
encrypt = function3([ord(i) for i in message], [ord(i) for i in key])
hex_encrypt = function1(encrypt)
print("Зашифрованное сообщение: ", hex_encrypt)
decrypt = function3([ord(i) for i in encrypt], [ord(i) for i in key])
print("Расшифрованное сообщение: ", decrypt)
```

```
Используем ключ:  zDgLWqM1zyRg6zxGNuveI9
Ключ в шестнадцатиричном виде:  7a 44 67 4c 57 71 4d 31 7a 79 52 67 36 7a 78 47 4e 75 76 65 49 39
Зашифрованное сообщение:  45b 64 45a 472 465 43a 471 11 469 447 466 459 40a 56 58 473 40e 436 441 429 406 18
Расшифрованное сообщение:  С новым Годом, друзья!
```

Figure 2: Получение шифротекста

Вариант прочтения открытого текста

Ввод [23]:
```
compute_key = function4([ord(i) for i in message], [ord(i) for i in encrypt])
decrypt_compute_key = function3([ord(i) for i in encrypt], [ord(i) for i in key])
print("Исходный ключ: ", key)
print("Вариант прочтения открытого текста: ", decrypt_compute_key)
```

```
Исходный ключ:  zDgLWqM1zyRg6zxGNuveI9
Вариант прочтения открытого текста:  С новым Годом, друзья!
```

Figure 3: Прочтение открытого текста

Выводы

Выводы

Освоил на практике применение режима однократного гаммирования.