

Элементы криптографии. Однократное гаммирование

Гебриал Ибрам¹

2021 Moscow, Russia

¹RUDN University, Moscow, Russian Federation

Цель работы

Освоить на практике применение режима однократного гаммирования.

Результаты

1. Написал блок функции для расчетов. (рис. 1)

```
In [8]: import string
import random

In [9]: #перевод в шестнадцатичную систему.
def hexx(text):
    return ''.join(hex(ord(i))[2:] for i in text)
#генерирует рандомный ключ.
def gen_key(size):
    return ''.join(random.choice(string.ascii_letters + string.digits) for _ in range(size))
#шифрует и дешифрует текст.
def encrypted(text, key):
    return ''.join(chr(a^b) for a, b in zip(text, key))
#создает ключ на основе текста и шифротекста.
def compute_key(text, encrypt):
    return ''.join(chr(a^b) for a, b in zip(text, encrypt))
```

Figure 1: Блок функции для расчетов

Определил вид шифротекста при известном ключе и известном открытом тексте. (рис. 2)

```
In [10]: message= 'С Новым Годом, друзья!'

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

print("Используемый ключ: ", key)

print("Ключ в шестнадцатичном 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:  ALToUvnEtStJ6tGq19NzXT
Ключ в шестнадцатичном виде:  41 4c 54 6f 55 76 6e 45 74 53 54 4a 36 74 47 71 6c 39 4e 7a 78 54
Зашифрованное сообщение:  460 6c 449 451 467 43d 452 65 467 46d 460 474 40a 58 67 445 42c 47a 479 436 437 75
Расшифрованное сообщение:  С Новым Годом, друзья!
```

Figure 2: Задание 1. Получение шифротекста

Определил ключ, с помощью которого шифротекст может быть преобразован в некоторый фрагмент текста, представляющий собой один из возможных вариантов прочтения открытого текста. (рис. 3)

```
In [27]: 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("Исходный ключ",key)
print("Вариант прочтения лткрытого текста: ", decrypt_compute_key)

Исходный ключ F1WNONILU6hvcP92va4XlUC
Вариант прочтения лткрытого текста: С Новым Годом, друзья!
```

Figure 3: Один из вариантов прочтения открытого текста:

Освоил на практике применение режима однократного гаммирования.

Спасибо за внимание