Лабораторная работа №7. Элементы криптографии. Однократное гаммирование.

Alexander S. Baklashov

18 October, 2022

RUDN University, Moscow, Russian Federation

Цель работы

Цель работы

Освоить на практике применение режима однократного гаммирования.

Выполнение лабораторной работы

Выполнение

Создадим функции для перевода в 16-ричный вид, шифрования и дешифрования, а также импортируем необх. библиотеки.

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

In [2]: def hex_16(txt):
            return ' '.join(hex(ord(i))[2:] for i in txt)
        def cypher(size):
            return ''.join(random.choice(string.ascii_letters+string.digits) for _ in range(size))
        def decypher (txt, key):
            return ''.join(chr(a^b) for a,b in zip (txt,key))
```

Figure 1: Функции

Выполнение

Создадим код для получения шифротекста.

In [3]:
```
msg = "С Новым Годом, друзья!"
key = cypher (len(msg))
hex_key = hex_16(key)
print ("Ключ:", key)
print ("Ключ в 16-ричном виде:", hex_key)
encr = decypher ([ord(i) for i in msg], [ord(i) for i in key])
hex_encr = hex_16 (encr)
print ("Зашифр. сообщение:", hex_encr)
decr=decypher ([ord(i) for i in encr], [ord(i) for i in key])
print ("Расшифр. сообщ.:", decr)
```

```
Ключ: Cjy9C184jA8QkVWihuKrmr
Ключ в 16-ричном виде: 43 6a 79 39 43 31 38 34 6a 41 38 51 6b 56 57 69 68 75 4b 72 6d 72
Зашифр. сообщение: 462 4a 464 407 471 47a 404 14 479 47f 40c 46f 457 7a 77 45d 428 436 47c 43e 422 53
Расшифр. сообщ.: С Новым Годом, друзья!
```

Figure 2: Шифротекст

Выполнение

Создадим код для получения варианта прочтения открытого текста.

```
In [4]: decr1=decypher ([ord(i) for i in encr], [ord(i) for i in key])
        print ("Ключ:", key)
        print ("Вариант прочтения откр. текста:", decr1)

        Ключ: Cjy9C184jA8QkVWihuKrmr
        Вариант прочтения откр. текста: С Новым Годом, друзья!
```

Figure 3: Открытый текст

Выводы

Выводы

В результате выполнения работы я освоил на практике применение режима однократного гаммирования.