

Отчет по лабораторной работе №7

Информационная безопасность

Чекалова Лилия Руслановна

Содержание

1	Цель работы	5
2	Задание	6
3	Теоретическое введение	7
4	Выполнение лабораторной работы	8
5	Выводы	10
	Список литературы	11

Список таблиц

Список иллюстраций

4.1	Программа, 1	8
4.2	Программа, 2	9
4.3	Результат запуска программы	9

1 Цель работы

- Освоить на практике применение режима однократного гаммирования.

2 Задание

- Написание программы
- Зашифровка текста по открытому тексту и известному ключу
- Определение ключа по открытому и зашифрованному тексту

3 Теоретическое введение

Гаммирование представляет собой наложение (снятие) на открытые (зашифрованные) данные последовательности элементов других данных, полученной с помощью некоторого криптографического алгоритма, для получения зашифрованных (открытых) данных. Иными словами, наложение гаммы — это сложение её элементов с элементами открытого (закрытого) текста по некоторому фиксированному модулю, значение которого представляет собой известную часть алгоритма шифрования.

Наложение гаммы по сути представляет собой выполнение операции сложения по модулю 2 (XOR) между элементами гаммы и элементами подлежащего сокрытию текста. Такой метод шифрования является симметричным, так как двойное прибавление одной и той же величины по модулю 2 восстанавливает исходное значение, а шифрование и расшифрование выполняется одной и той же программой.

Более подробно о см. в [1].

4 Выполнение лабораторной работы

Для выполнения лабораторной работы я написала программу для зашифрования и расшифровки текста. Импортировав необходимые библиотеки, я задала три функции — для генерации ключа по размеру сообщения (выбор случайных букв в кодировке ASCII), для перевода сообщения и ключей в 16-ричную систему (получение кода символа и перевод его в 16-ричную систему) и для шифрования (поэлементный XOR) (рис. 4.1).

```
import string
import random
import sys

def gen_key(size):
    res = ''
    for i in range(size):
        res += random.choice(string.ascii_letters)
    return res

def to_hex(text):
    res = ''
    for i in text:
        res += hex(ord(i))[2:] + ' '
    return res

def encrypt(text, key):
    res = ''
    for (t, k) in zip(text, key):
        res += chr(t^k)
    return res
```

Рис. 4.1: Программа, 1

Далее я задала изначальное открытое сообщение, сгенерировала ключ, закодировала со-

общение с помощью этого ключа, а также перевела все в 16-ричную систему. После этого я раскодировала закодированное сообщение, чтобы проверить правильность работы программы, и определила используемый ключ по открытому сообщению и закодированному сообщению (рис. 4.2).

```
message = 'С Новым Годом, друзья!'
message16 = to_hex(message)
key = gen_key(len(message))
k = to_hex(key)
encr_m = encrypt([ord(i) for i in message], [ord(i) for i in key])
encr_m16 = to_hex(encr_m)
decr_m = encrypt([ord(i) for i in encr_m], [ord(i) for i in key])
key_new = encrypt([ord(i) for i in message], [ord(i) for i in encr_m])

print('open text:', message, '\nopen text in 16:', message16, '\nkey:', key, '\nkey in 16:', k)
print('encrypted text:', encr_m, '\nencrypted text in 16:', encr_m16, '\ndecrypted message:', decr_m, '\nfound key:', key_new)
```

Рис. 4.2: Программа, 2

Полученные сообщения и ключи я вывела на экран (рис. 4.3). Сообщение было успешно закодировано и раскодировано, а найденный ключ совпадает с тем, который был сгенерирован для кодирования.

```
open text: С Новым Годом, друзья!
open text in 16: 421 20 41d 43e 432 44b 43c 20 413 43e 434 43e 43c 2c 20 434 440 443 437 44c 44f 21
key: yrUoagIfelIRXuENBgXdDi
key in 16: 79 72 55 6f 61 67 49 66 65 6c 49 52 58 75 45 4e 42 67 58 64 44 69
encrypted text: jRшёгьvFVл0мкУе0ь0зшн
encrypted text in 16: 458 52 448 451 453 42c 475 46 476 452 47d 46c 464 59 65 47a 402 424 46f 428 40b 48
decrypted message: С Новым Годом, друзья!
found key: yrUoagIfelIRXuENBgXdDi
```

Рис. 4.3: Результат запуска программы

5 Выводы

В результате лабораторной работы я получила представление о базовых элементах криптографии и освоила на практике применение режима однократного гаммирования, написав программу, позволяющую зашифровывать и расшифровывать тексты и определять использованные для этого ключи.

Список литературы

1. Элементы криптографии. Однократное гаммирование [Электронный ресурс]. URL: https://esystem.rudn.ru/pluginfile.php/2090284/mod_resource/content/2/007-lab_crypto-gamma.pdf.