

Лабораторная работа №8

Информационная безопасность

Леонтьева Ксения Андреевна | НПМбд-01-19

Содержание

1	Цель работы	4
2	Теоретическое введение	5
3	Выполнение лабораторной работы	6
4	Выводы	8
	Список литературы	9

Список иллюстраций

3.1	Приложение, реализующее режим однократного гаммирования для двух текстов одним ключом, Часть 1	6
3.2	Приложение, реализующее режим однократного гаммирования для двух текстов одним ключом, Часть 2	7

1 Цель работы

Освоить на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.

2 Теоретическое введение

Гаммирование - наложение (снятие) на открытые (зашифрованные) данные последовательности элементов других данных, полученной с помощью некоторого криптографического алгоритма, для получения зашифрованных (открытых) данных.

Основная формула, необходимая для реализации однократного гаммирования: $C_i = P_i \text{ XOR } K_i$, где C_i - i -й символ зашифрованного текста, P_i - i -й символ открытого текста, K_i - i -й символ ключа.

В данном случае для двух шифротекстов будет две формулы: $C_1 = P_1 \text{ xor } K$ и $C_2 = P_2 \text{ xor } K$, где индексы обозначают первый и второй шифротексты соответственно.

Если нам известны оба шифротекста и один открытый текст, то мы можем найти другой открытый текст, это следует из следующих формул: $C_1 \text{ xor } C_2 = P_1 \text{ xor } K \text{ xor } P_2 \text{ xor } K = P_1 \text{ xor } P_2$, $C_1 \text{ xor } C_2 \text{ xor } P_1 = P_1 \text{ xor } P_2 \text{ xor } P_1 = P_2$.

Более подробно см. в [1].

3 Выполнение лабораторной работы

Код программы (рис. 3.1).

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

In [2]: def cipher_text_function(text, key):
        if len(key) != len(text):
            return "Ключ и текст должны быть одной длины!"
        cipher_text = ''
        for i in range(len(key)):
            cipher_text_symbol = ord(text[i]) ^ ord(key[i])
            cipher_text += chr(cipher_text_symbol)
        return cipher_text

In [3]: text_1 = "С Новым годом, друзья!"
        text_2 = "Поздравляем с 8 марта!"

In [5]: key = ''
        seed(23)
        for i in range(len(text_1)):
            key += random.choice(string.ascii_letters + string.digits)
        print(key)

        7X8s51fbLtByHwiUmrCaoN

In [7]: cipher_text_1 = cipher_text_function(text_1, key)
        cipher_text_2 = cipher_text_function(text_2, key)
        print('Первый шифротекст:', cipher_text_1)
        print('Второй шифротекст:', cipher_text_2)

        Первый шифротекст: ЖхХэЇФъВѡъŸчV[IwЭ6VЭРо
        Второй шифротекст: ШАЦчvЁельГсŸYьWQuётГУуо

In [8]: print('Первый открытый текст:', cipher_text_function(cipher_text_1, key))
        print('Второй открытый текст:', cipher_text_function(cipher_text_2, key))

        Первый открытый текст: С Новым годом, друзья!
        Второй открытый текст: Поздравляем с 8 марта!
```

Рис. 3.1: Приложение, реализующее режим одноразового гаммирования для двух текстов одним ключом, Часть 1

- In[1]: импорт необходимых библиотек

- In[2]: функция, реализующая сложение по модулю два двух строк
- In[3]: открытые/исходные тексты (одинаковой длины)
- In[5]: создание ключа той же длины, что и открытые тексты
- In[7]: получение шифротекстов с помощью функции, созданной ранее, при условии, что известны открытые тексты и ключ
- In[8]: получение открытых текстов с помощью функции, созданной ранее, при условии, что известны шифротексты и ключ

```
In [9]: cipher_text_xor = cipher_text_function(cipher_text_1, cipher_text_2)
print('Первый шифротекст XOR Второй шифротекст:', cipher_text_xor)

Первый шифротекст XOR Второй шифротекст: >0*
r{0|0}0Д|sw00

In [10]: print('Первый открытый текст:', cipher_text_function(cipher_text_xor, text_2))
print('Второй открытый текст:', cipher_text_function(cipher_text_xor, text_1))

Первый открытый текст: С Новым годом, друзья!
Второй открытый текст: Поздравляем с 8 марта!

In [12]: text_1_ = text_1[3:6]
print('Часть первого открытого текста:', text_1_)

Часть первого открытого текста: овы

In [14]: cipher_text_xor = cipher_text_function(cipher_text_1[3:6], cipher_text_2[3:6])
print('Часть второго открытого текста:', cipher_text_function(cipher_text_xor, text_1_))

Часть второго открытого текста: дра
```

Рис. 3.2: Приложение, реализующее режим однократного гаммирования для двух текстов одним ключом, Часть 2

- In[9]: сложение по модулю два двух шифротекстов с помощью функции, созданной ранее
- In[10]: получение открытых текстов с помощью функции, созданной ранее, при условии, что известны оба шифротекста и один из открытых текстов
- In[12]: получение части первого открытого текста (срез)
- In[14]: получение части второго текста (на тех позициях, на которых расположены символы части первого открытого текста) с помощью функции, созданной ранее, при условии, что известны оба шифротекста и часть первого открытого текста

4 Выводы

В ходе выполнения данной лабораторной работы я освоила на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.

Список литературы

1. Однократное гаммирование [Электронный ресурс]. URL: https://esystem.rudn.ru/pluginfile.php/1651641/mod_resource/content/2/008-lab_crypto-key.pdf.