

Отчёт по лабораторной работе № 7

Информационная безопасность

Кинсиклунон Доря Флора

Содержание

0.1	Цель работы	4
0.2	Теоретическое введение	4
0.3	Выполнение лабораторной работы	4
0.4	Выводы	5
1	Список литературы	6

Список иллюстраций

1	Рис. 7.1: Приложение, реализующее режим однократного гаммирования	5
---	---	---

Список таблиц

0.1 Цель работы

Освоить на практике применение режима одноразового гаммирования.

0.2 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 одноразового 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. Аналогичным образом можно найти ключ: $K_i = C_i \text{ XOR } P_i$. Необходимые и достаточные условия абсолютной стойкости шифра: • длина открытого текста равна длине ключа • ключ должен использоваться однократно • ключ должен быть полностью случаен

0.3 Выполнение лабораторной работы

Код программы(рис. 7.1).

```

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

In [5]: 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 [6]: text = "С новым годом, друзья"

In [7]: key = ''
        seed(23)
        for i in range(len(text)):
            key += random.choice(string.ascii_letters + string.digits)
        print(key)

        7X8s51fbltByHwiUmrCao

In [8]: cipher_text = cipher_text_function(text, key)
        print('Шифротекст:', cipher_text)

        Шифротекст: ЖксЭIQыВwъVчV[IwЭ6VЭР

In [11]: print('Открытый текст:', cipher_text_function(cipher_text, key))

        Открытый текст: С новым годом, друзья

In [13]: print('ключ:', cipher_text_function(text, cipher_text))

        ключ: 7X8s51fbltByHwiUmrCao

```

Рис. 1: Рис. 7.1: Приложение, реализующее режим однократного гаммирования

- In[21]: импорт необходимых библиотек
- In[22]: функция, реализующая сложение по модулю два двух строк
- In[23]: открытый/исходный текст
- In[24]: создание ключа той же длины, что и открытый текст
- In[25]: получение шифротекста с помощью функции, созданной ранее, при условии, что известны открытый текст и ключ
- In[26]: получение открытого текста с помощью функции, созданной ранее, при условии, что известны шифротекст и ключ
- In[27]: получение ключа с помощью функции, созданной ранее, при условии, что известны открытый текст и шифротекст

0.4 Выводы

В ходе выполнения данной лабораторной работы я освоила на практике применение режима однократного гаммирования.

1 Список литературы

Однократное гаммирование [Электронный ресурс]. URL: https://esystem.rudn.ru/pluginfile.php/1651639/mod_resource/content/2/007-lab_cryptogamma.pdf.