Лабораторная работа №7

Элементы криптографии. Однократное гаммирование

Хамдамова А. А.

9 мая 2024

Российский университет дружбы народов, Москва, Россия

Информация

Докладчик

- Хамдамова Айжана Абдукаримовна
- студент Факультета Физико-математических и естественных наук
- Российский университет дружбы народов
- 1032225989@pfur.ru
- https://github.com/AizhanaKhamdamova/study_2023-2024_infosec

Вводная часть

Предложенная Г. С. Вернамом так называемая «схема однократного использования (гаммирования)» (рис. 7.1) является простой, но надёжной схемой шифрования данных. 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. В соответствии с теорией криптоанализа, если в методе шифрования используется однократная вероятностная гамма (однократное гаммирование) той же длины, что и подлежащий сокрытию текст, то текст нельзя раскрыть. Даже при раскрытии части последовательности гаммы нельзя получить информацию о всём скрываемом тексте. Наложение гаммы по сути представляет собой выполнение операции сложения по модулю 2 (XOR) (обозначаемая знаком ⊕) между элементами гаммы и элементами подлежащего сокрытию текста. Напомним, как работает операция XOR над

Цели и задачи

- Освоить на практике применение режима однократного гаммирования

Выполнение лабораторной работы

Нужно подобрать ключ, чтобы получить сообщение «С Новым Годом, друзья!». Требуется разработать приложение, позволяющее шифровать и дешифровать данные в режиме однократного гаммирования. Приложение должно: 1. Определить вид шифротекста при известном ключе и известном открытом тексте. 2. Определить ключ, с помощью которого шифротекст может быть преобразован в некоторый фрагмент текста, представляющий собой один из возможных вариантов прочтения открытого текста.

```
In [7]: import random
        from random import seed
        import string

In [8]: def xor_text_f(text,key):
            if len(key) != len(text): return "Ошибка. Ключ и текст разной длины"
            xor_text = ''
            for i in range(len(key)):
                xor_text_symbol = ord(text[i]) ^ ord(key[i])
                xor_text += chr(xor_text_symbol)
            return xor_text

In [9]: text = 'С Новым годом, друзья!'

In [10]: key = ''
         seed(22)
         for i in range(len(text)):
             key += random.choice(string.ascii_letters + string.digits)
         key

Out[10]: '96ipbNClShVP4wY4for9du'

In [11]: xor_text = xor_text_f(text,key)
         xor_text

Out[11]: 'И\x16VюèSw̄LωiЂ3̌J[yÈЦьxvЫT'

In [12]: xor_text_f(xor_text,key)

Out[12]: 'С Новым годом, друзья!'

In [13]: xor_text_f(text,xor_text)

Out[13]: '96ipbNClShVP4wY4for9du'
```

Выводы

Выводы

Я освоила на практике применение режима однократного гаммирования