

Защита лабораторной работы №7

Информационная безопасность

Малашенко М. В.

2023

Российский университет дружбы народов, Москва, Россия

- Малашенко Марина Владимировна
- Студентка группы НФИбд-01-20
- Студ. билет 1032202459
- Российский университет дружбы народов



Цель лабораторной работы

- Освоить на практике применение режима однократного гаммирования

Предложенная Г. С. Вернамом так называемая «схема однократного использования (гаммирования)» является простой, но надёжной схемой шифрования данных. [0]

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 \boxtimes) 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.

Ход выполнения лабораторной работы

Задача 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.

Решение задачи лабораторной работы

Для решения задачи написан программный код:

```
In [1]: import random

In [2]: from random import seed

In [3]: import string

In [4]: # сложение двух строк по модулю
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 [5]: # ввод исходного текста
text = "С Новым Годом, друзья!"

In [6]: # создание ключа
key = ""
seed(22)
for i in range(len(text)):
    key += random.choice(string.ascii_letters + string.digits)
key

Out[6]: '96ipbNC1SHVP4wY4for9du'

In [7]: # получение шифротекста
xor_text = xor_text_f(text, key)
xor_text

Out[7]: 'И\х10Vee5\p1t53[уёЦххыт'

In [8]: # открытый текст
xor_text_f(xor_text, key)

Out[8]: 'С Новым Годом, друзья!'

In [9]: # получение ключа
xor_text_f(text, xor_text)

Out[9]: '96ipbNC1SHVP4wY4for9du'
```

Рис. 1: (рис. 1. Программный код приложения, реализующего режим однократного гаммирования)

Вывод

В ходе выполнения данной лабораторной работы было освоено на практике применение режима однократного гаммирования

Список литературы. Библиография

0] Методические материалы курса