Элементы криптографии. Однократное гаммирование

Ханина Ирина Владимировна НБИбд-02-18

9 декабря, 2021, Москва, Россия

Российский Университет Дружбы Народов

Теоретическое введение

Гаммирование или Шифр XOR - это наложение (снятие) на открытые (зашифрованные) данные последовательности элементов других данных, полученной с помощью некоторого криптографического алгоритма, для получения зашифрованных (открытых) данных. С точки зрения теории криптоанализа метод шифрования однократной вероятностной гаммой (однократного гаммирования) той же длины, что и открытый текст, является невскрываемым. Наложение гаммы представляет собой выполнение операции сложения по модулю 2 (XOR) между элементами гаммы и элементами подлежащего сокрытию текста. Данный метод шифрования - симметричный, т.к. двойное прибавление одной и той же величины по модулю 2 восстанавливает исходное значение, а шифрование и расшифрование выполняется одной и той же программой.

Цель лабораторной работы

Цель - освоить на практике применение режима однократного гаммирования.

Задачи лабораторной работы

Подобрать ключ, чтобы получить сообщение «С Новым Годом, друзья!». Далее 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.

Результаты выполнения лабораторной работы

Я освоила на практике применение режима однократного гаммирования. Код программы:

```
from operator import xor

string = 'С Новым годом, друзья!'
key = 'Счастливого Рождества!'

def gamming(x, y):
    text = []
    for x, y in zip(x, y):
        text.append(chr(xor(ord(x), ord(y))))
    t = ''.join(text)
    return t

s = gamming(string, key)
print("Зашифрованное послание: ", bytes(s, "UTF-8").hex())
print("Ключ: ", gamming(string, s))
print("Открытый текст: ", gamming(s, key))
```

```
Зашифрованное послание:  00d1a72d7f707004d0920d0d0ad09e1cd092d096007502757e7f00
Ключ:  Счастливого Рождества!
Открытый текст:  С Новым годом, друзья!
```

Figure 1: Рис 1. Код приложения