Защита лабораторной работы №6

Информационная безопасность

Данзанова С. З.

2024

Российский университет дружбы народов, Москва, Россия

Информация

Докладчик

- Данзанова Саяна Зоригтоевна
- Студентка группы НПИбд-01-21
- Студ. билет 1032217624
- Российский университет дружбы народов

Цель лабораторной работы

- Освоить на практике применение режима однократного гаммирования

Теоретическая справка (1)

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.

Теоретическая справка (2)

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.

Теоретическая справка (3)

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 про- граммой.

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:

```
# Импорт необходимых библиотек
import random
from random import seed
import string
```

```
[18] # Функция сложения 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
```

```
[14] # Вывод исходного текста
text = "С Новым Годом, друзья!"
text
```

```
'С Новым Годом, друзья!'
```

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

Решение задачи лабораторной работы

```
[20] # Создание ключа
     key = ''
     seed(22)
     for i in range(len(text)):
       key += random.choice(string.ascii_letters + string.digits)
     key
```

```
'96ipbNClShVP4wY4for9du'
```

```
[19] # Получене шифротекста
     xor_text = xor_text_f(text,key)
     xor_text
```

```
'И\x16VюёSЩLpiЪЗJ[уЁЦЬxvЫГ'
```

```
[24] # Полученик открытого текста
     xor_text_f(xor_text,key)
```

```
'С Новым Годом, друзья!'
```

```
     # Получение ключа
     xor_text_f(text,xor_text)
```

```
'96ipbNClShVP4wY4for9du'
```

Рис. 2: 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