Отчёт по лабораторной работе №7 по предмету Информационная безопасность

Элементы криптографии. Однократное гаммирование

Саттарова Вита Викторовна

Содержание

Список иллюстраций

Список таблиц

1 Цели и задачи работы

Цели:

- Изучить основы криптографии.
- Освоить на практике применение режима однократного гаммирования.

Задачи:

- Выполнить все пункты, указанные в методических рекомендациях к лабораторной работе.
- Выполняя задания, познакомиться с основами криптографии.
- Выполняя задания, изучить однократное гаммирование.
- Написать отчёт, проанализировав результаты, полученные в ходе выполнения лабораторной работы.

2 Объект и предмет исследования

Объект исследования: основы шифрования.

Предмет исследования: однократное гаммирование.

3 Условные обозначения и термины

Условные обозначения

Отсутствуют

Термины

- шифрование
- однократное гаммирование

4 Задание

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.

Более подробно о работе см. в [1].

5 Теоретическое введение

5.1 Однократное гаммирование

Предложенная Г. С. Вернамом так называемая «схема однократного использования (гаммирования)» 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) 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.

Если известны ключ и открытый текст, то задача нахождения шифротекста заключается в применении к каждому символу открытого текста и ключа операции XOR. Размерности открытого текста и ключа должны совпадать, и полученный шифротекст будет такой же длины.

Если известны шифротекст и открытый текст, то задача нахождения ключа решается также, а именно, обе части равенства необходимо применить посимвольно операцию XOR к шифротексту и открытому тексту.

Необходимые и достаточные условия абсолютной стойкости шифра:

- полная случайность ключа;
- равенство длин ключа и открытого текста;
- однократное использование ключа.

Более подробно о работе см. в [1].

6 Техническое оснащение и выбранные методы проведения работы

Техническое оснащение

- Ноутбук
- Python 3
- Jupyter Notebook
- Интернет

Методы проведения работы

- Изучение методической информации
- Выполнение заданий в соответствии с указаниями
- Анализ результатов
- Обобщение проведённой деятельности

7 Выполнение лабораторной работы и полученные результаты

1. Скачала и ознакомилась с методическими указаниями к лабораторной работе (рис. 7.1).

Лабораторная работа № 7. Элементы криптографии. Однократное гаммирование

7.1. Цель работы

Освоить на практике применение режима однократного гаммирования[1].

7.2. Указание к работе

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)

Рис. 7.1: Лабораторная работа 7

2. Создала сообщение и написала основные функции для приложения с однократным гаммированием (рис. 7.2).

Ввод [16]:
```
import random as rd
```

Ввод [17]:
```
# строка
message = "С Новым Годом, друзья!"
```

Ввод [18]:
```
# перевод в 16
def hex_string(mes):
    return " ".join([hex(ord(elem))[2:] for elem in mes])
```

Ввод [19]:
```
# ключ
def make_key(mes):
    base = "abcdefghijklmnopqrstuvwxyzабвгдеёжзийклмнопрстуфхцчшщъыьэюя0123456789"
    return "".join([rd.choice(base) for i in range(len(mes))])
```

Ввод [20]:
```
# кодирование
def coding(mes, key):
    return "".join(chr(ord(mes[i]) ^ ord(key[i])) for i in range(len(mes)))
```

Рис. 7.2: Функции

3. Использовала созданные функции, создав ключ для кодирования сообщения, закодировав сообщение и получив шифротекст, а затем раскодировав шифротекст в исходное сообщение тем же ключом. После этого показала, что использование другого ключа даёт иное прочтение текста (не даёт исходное сообщение), а также то, что применение функции кодирования к исходному тексту и шифротексту возвращает значение ключа (рис. 7.3).

```
Ввод [30]: main_key = make_key(message)
           encoded = coding(message, main_key)
           decoded = coding(encoded, main_key)
```

```
Ввод [31]: print(message)
           print(main_key)
           print(encoded)
           print(decoded)
```

```
С Новым Годом, друзья!
хлbвтарk0хбоьбвqа5вi8ы
dЛ₩р{|КУц□ёрНВхрЎ□ХўЖ
С Новым Годом, друзья!
```

```
Ввод [36]: # пример с неверным ключом
           new_key = make_key(message)
           coding(encoded, new_key)
```

```
Out[36]: 'ёƷ0еькы9ы\x0cиЊ\x1aV]VoЌ0\x18@T'
```

```
Ввод [37]: coding(message, encoded)
```

```
Out[37]: 'хлbвтарk0хбоьбвqа5вi8ы'
```

Рис. 7.3: Применение функций

8 Анализ результатов

Таким образом, были выаолнены задания по изучению однократного гаммирования: было зашифровано сообщение, расшифровано сгенерированным случайно ключом, а также получен ключ для исходного текста по закодированному.

9 Заключение и выводы

Таким образом, в ходе выполнения лабораторной работы было сделано следующее:

- Изучены основы криптографии.
- Освоено на практике применение режима однократного гаммирования.
- Написан отчёт к лабораторной работе.

10 Список литературы

[1]

1. Информационная безопасность [Электронный ресурс]. Российский университет дружбы народов, 2023. URL: https://esystem.rudn.ru/pluginfile.php/2090284/mod_resource/content/2/007-lab_crypto-gamma.pdf.