Лабораторная работа № 7

Элементы криптографии. Однократное гаммирование

Алибаева Данагуль НБибд-01-18

Содержание

List of Tables

List of Figures

1 Цель работы

Освоить на практике применение режима однократного гаммирования

2 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

3 Теоретическое введение

Простейшей и в то же время наиболее надёжной из всех схем шифрования является так называемая схема однократного использования (см. рисунок 1), изобретение, которое чаще всего связывают с именем Г.С. Вернама [1].

Гаммирование – это наложение (снятие) на открытые (зашифрованные) данные криптографической гаммы, т.е. последовательности элементов данных, вырабатываемых с помощью некоторого криптографического алгоритма, для получения зашифрованных (открытых) данных. С точки зрения теории криптоанализа, метод шифрования случайной однократной равновероятной гаммой той же длины, что и открытый текст, является невскрываемым (далее для краткости будем употреблять термин “однократное гаммирование”, держа в уме всё сказанное выше). Кроме того, даже раскрыв часть сообщения, дешифровщик не сможет хоть сколько-нибудь поправить положение – информация о вскрытом участке гаммы не даёт информации об остальных её частях [1].

Допустим, в тайной деловой переписке используется метод однократного наложения гаммы на открытый текст. “Наложение” гаммы – не что иное, как выполнение операции сложения по модулю 2 (xor) её элементов с элементами открытого текста. Эта операция в языке программирования C++ обозначается знаком , а в математике – знаком [1].

Гаммирование является симметричным алгоритмом. Поскольку двойное прибавление одной и той же величины по модулю 2 восстанавливает исходное значение, шифрование и дешифрование выполняется одной и той же программой [1].

4 Выполнение лабораторной работы

1.Лабораторная работа выполнялась дома со следующими характеристиками техники:

– Intel(R) Core(TM) i5-8300H CPU @ 2.30GHz, 2304 МГц, ядер: 4, логических процессоров: 8

– ОС Майкрософт Windows 10 Pro

– VirtualBox верс. 6.1.26

2. Подобрала ключ, чтобы получить сообщение «С Новым Годом, друзья!». Разработала приложение, позволяющее шифровать и дешифровать данные в режиме однократного гаммирования. Приложение:

1) Определяет вид шифротекста при известном ключе и известном открытом тексте.

2) Определяет ключ, с помощью которого шифротекст может быть преобразован в некоторый фрагмент текста, представляющий собой один из возможных вариантов прочтения открытого текста (рис 1.1).

```python
from operator import xor
string = input("Open text: ")
key = input("Key: ")

def gamming(a,b):
    c = []
    for a,b in zip(a,b):
        c.append(chr(xor(ord(a), ord(b))))
    text = ''.join(c)
    return text

d = gamming(string, key)
print(" ")
print("Encrypted message: ", bytes(d, "UTF-8").hex())
```

```
Open text: С Новым годом, друзья!
Key: Желаю большого счастья

Encrypted message:  37d095260e7cd1ab0dd09e08727c000fd09200750773760e03d1ae
```

Figure 4.1: 1.1. Разработка приложения

5 Выводы

Освоила на практике применение режима однократного гаммирования.

6 Список литературы

1. Гаммирование. Моделирование работы скремблера// URL: https://ami.nstu.ru/~gultyaeva/ps (дата обращения: 10.12.2021).