Лабораторная работа № 8

Элементы криптографии. Шифрование (кодирование) различных исходных текстов одним ключом

Алибаева Данагуль НБибд-01-18

Содержание

List of Tables

List of Figures

1 Цель работы

Освоить на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.

2 Задание

Два текста кодируются одним ключом (однократное гаммирование). Требуется, не зная ключа и не стремясь его определить, прочитать оба текста. Необходимо разработать приложение, позволяющее шифровать и дешифровать тексты P1 и P2 в режиме однократного гаммирования. Приложение должно определить вид шифротекстов C1 и C2 обоих текстов P1 и P2 при известном ключе; Необходимо определить и выразить аналитически способ, при котором злоумышленник может прочитать оба текста, не зная ключа и не стремясь его определить.

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. Не зная ключа и не стремясь его определить, прочитала оба текста. Разработала приложение, позволяющее шифровать и дешифровать тексты P1 и P2 в режиме однократного гаммирования. Приложение определяет вид шифротекстов C1 и C2 обоих текстов P1 и P2 при известном ключе (рис 1.1).

```python
import random
import string
P1 = " НаВашисходящийот1204"
P2 = " ВСеверныйфилиалБанка"

def hex1(a):
    return ' '.join(hex(ord(i))[2:] for i in a)

def key1(lenn):
    return ''.join(random.choice(string.ascii_letters + string.digits) for _ in range(lenn))

def gamming(first, second):
    first = [ord(i) for i in first]
    second = [ord(i) for i in second]
    return ''.join(chr (a^b) for a,b in zip(first, second))

key = key1(len(P1))
print("Ключ: ", key)
hex_key = hex1(key)
print("Шеснадцатиричный ключ: ", hex_key)
C1 = gamming(P1, key)
C2 = gamming(P2, key)
gamming2 = gamming(C1,C2)
print("Открый 1 текст: ", gamming(gamming2,P1))
print("Открый 2 текст: ", gamming(gamming2,P2))
print("Зашифрованное 1 послание: ", C1)
print("Зашифрованное 2 послание: ", C2)
```

```
Ключ:  y70Zts2kcnTksBzubtAH2
Шеснадцатиричный ключ:  79 37 30 5a 74 73 32 6b 63 6e 54 6b 73 42 7a 75 62 74 41 48 32
Открый 1 текст:   ВСеверныйфилиалБанка
Открый 2 текст:   НаВашисходящийот1204
Зашифрованное 1 послание:  YЬЁшфлЊЬЦёЮФкОуыPEsx
Зашифрованное 2 послание:  YXБ҂ццθiШЇAґшОъюефЎθЂ
```

Figure 4.1: 1.1. Разработка приложения

5 Выводы

Освоила на практике применение режима однократного гаммирования на примере кодирования различных исходных текстов одним ключом.

6 Список литературы

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